NOTICE OF FILING

This document was lodged electronically in the FEDERAL COURT OF AUSTRALIA (FCA) on 24/09/2019 12:16:00 PM AEST and has been accepted for filing under the Court's Rules. Details of filing follow and important additional information about these are set out below.

Details of Filing

Document Lodged: Statement of Agreed Facts

File Number: NSD989/2019

File Title: AUSTRALIAN BROADCASTING CORPORATION v MARTIN KANE &

ORS

Registry: NEW SOUTH WALES REGISTRY - FEDERAL COURT OF

AUSTRALIA



Dated: 24/09/2019 2:19:45 PM AEST Registrar

Important Information

Wound Soden

As required by the Court's Rules, this Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date and time of lodgment also shown above are the date and time that the document was received by the Court. Under the Court's Rules the date of filing of the document is the day it was lodged (if that is a business day for the Registry which accepts it and the document was received by 4.30 pm local time at that Registry) or otherwise the next working day for that Registry.



STATEMENT OF AGREED FACTS AND ISSUES

FEDERAL COURT OF AUSTRALIA

DISTRICT REGISTRY: NEW SOUTH WALES

Division: General No NSD 989 of 2019

AUSTRALIAN BROADCASTING CORPORATION

Applicant

MARTIN KANE

and others named in the Schedule Respondents

PART I INTRODUCTION

- 1. The documents annexed to this Statement of Agreed Facts and Issues form part of the Statement of Agreed Facts and Issues. The Applicant and the Second and Third Respondents rely on the documents annexed for their full meaning and effect. The explanations of those documents contained in this Statement of Agreed Facts and Issues are for ease of reference only and in no way limit or affect the meaning and effect of those documents.
- 2. The agreement of the Applicant and the Second and Third Respondents to the facts and documents set out in this Statement of Agreed Facts and Issues is not an agreement that those facts and documents are relevant to the issues before the Court.

PART II FACTS

A. PARTIES

- 3. The Applicant (ABC) is and was at all material times:
 - 3.1. a body corporate continued in existence by s 5 of the *Australian Broadcasting Corporation Act 1983* (Cth) (**ABC Act**);
 - 3.2. able to sue; and
 - 3.3. the publisher of a website called www.abc.net.au/news.

Filed on behalf of the Second and Third Respondents

Prepared by: Kristy Alexander

AGS lawyer within the meaning of s 55I of the *Judiciary Act*

1903

Address for Service: The Australian Government Solicitor, Level 42, MLC Centre, 19 Martin Place, Sydney, NSW 2000 Kristy.Alexander@ags.gov.au 33877130 Telephone: 02 9581 7640 Lawyer's Email: Kristy.Alexander@ags.gov.au Facsimile: 02 9581 7732

File ref: 19004307

- 4. The First Respondent (Registrar Kane) is and was at all material times:
 - 4.1. employed under Part 4 of the *Government Sector Employment Act 2013* (NSW) in the Local Court of New South Wales;
 - 4.2. a registrar for the purposes of s 18 of the Local Court Act 2007 (NSW);
 - 4.3. an 'authorised officer' for the purposes of s 3 of the *Law Enforcement (Powers and Responsibilities) Act 2002* (NSW); and
 - 4.4. an 'issuing officer' within the meaning of ss 3C and 3E of the *Crimes Act 1914* (Cth) (**Crimes Act**).
- 5. The Second Respondent (**Commissioner**) is and was at all material times:
 - 5.1. the Commissioner of Police appointed under s 17(1) of the *Australian Federal Police Act 1979* (Cth) (**AFP Act**);
 - 5.2. an officer of the Commonwealth; and
 - 5.3. in accordance with s 37(1) of the AFP Act, subject to that Act, the officeholder responsible for the general administration of, and the control of the operations of, the Australian Federal Police (**AFP**).
- 6. The Third Respondent (**FA Brumby**) is and was at all material times:
 - 6.1. a member of the AFP, pursuant to s 40B of the AFP Act; and
 - 6.2. a 'constable' within the meaning of ss 3, 3C and 3E of the Crimes Act.

B. DEFENCE

The Australian Defence Organisation

- 7. The Australian Defence Organisation (**Defence**) consists of the Department of Defence (**Department**) and the Australian Defence Force (**ADF**).
- 8. The Department is established as a Department of State. This is done by the Governor-General of Australia through an Administrative Arrangements Order, most recently on 29 May 2019.
- 9. The Department's staff comprise persons employed under the *Public Service Act* 1999 (Cth) (**Public Service Act**) and ADF members who are appointed as an officer of, or who are enlisted in, the Royal Australian Navy, the Australian Army or the Royal Australian Air Force under the *Defence Regulation 2016* (Cth).
- 10. The Department is administered by the Secretary of the Department (**Secretary**). The Secretary is appointed under s 58 of the Public Service Act.

- 11. The ADF is the military arm of Defence. It is constituted under s 17 of the *Defence Act* 1903 (Cth) (**Defence Act**) and consists of the Royal Australian Navy, the Australian Army and the Royal Australian Air Force.
- 12. Under s 8 of the Defence Act, the Minister for Defence has general control and administration of the ADF.
- 13. Under s 9(1) of the Defence Act, the ADF is commanded by the Chief of the Defence Force. The Chief of the Defence Force is appointed by the Governor-General under s 12(1) of the Defence Act.
- 14. Under s 10(1) of the Defence Act, the Secretary and the Chief of the Defence Force have joint administration of the ADF. The administration of the ADF does not include any matter falling within the command of the ADF.
- 15. Defence prepares and publishes Corporate Plans under s 35 of the *Public Governance, Performance and Accountability Act 2013* (Cth) (**PGPA Act**). A Defence Corporate Plan was published for each of 2016-17, 2017-18, 2018-19, and 2019-2020.

Document: Annexed to this Statement of Agreed Facts and Issues at p 27 and marked 'Annexure 1' is a copy of the Defence 2016-17 Corporate Plan dated 23 August 2016.

Document: Annexed to this Statement of Agreed Facts and Issues at p 45 and marked 'Annexure 2' is a copy of the Defence 2017-18 Corporate Plan dated 7 June 2017.

Document: Annexed to this Statement of Agreed Facts and Issues at p 63 and marked 'Annexure 3' is a copy of the Defence 2018-19 Corporate Plan dated 28 June 2018.

Document: Annexed to this Statement of Agreed Facts and Issues at p 85 and marked 'Annexure 4' is a copy of the Defence 2019-20 Corporate Plan dated 13 July 2019.

- 16. Defence's Corporate Plans set out Defence's role, objectives and functions, referred to as 'purposes' in the PGPA Act, and describe how Defence will measure its performance in achieving those purposes. [Defence Corporate Plans 2016-17 (p 2), 2017-18 (p 2), 2018-19 (p 2), 2019-20 (p 5)]
- 17. Defence's Corporate Plans for each of 2016-17, 2017-18 and 2018-19 state that:
 - 17.1. the mission of Defence is to defend Australia and its national interests [Defence Corporate Plans 2016-17 (p 3), 2017-18 (p 3) and 2018-19 (p 3)]; and
 - 17.2. the primary role of Defence is to protect and advance Australia's strategic interests through the promotion of security and stability, the provision of military capabilities to defend Australia and its national interests, and the provision of support for the Australian community and civilian authorities as directed by Government [Defence Corporate Plans 2017-18 (p 3) and 2018-19 (p 3); the Defence Corporate Plan 2016-17 (p 3) is in slightly (but immaterially) different terms].
- 18. Defence's Corporate Plan for 2019-20 states that:
 - 18.1. Defence plans for, develops and maintains the capability to deter and defeat armed attacks on Australia or on Australian interests. This includes planning for,

- conducting, controlling and evaluating Defence and/ or coalition contributions to Government-directed operations [Defence Corporate Plan 2019-2020, p 16];
- 18.2. Defence must provide high-quality, relevant and timely advice to Government on Defence strategy, capability and resourcing [Defence Corporate Plan 2019-2020, p 16]; and
- 18.3. The Government expects Defence to play an active role in contributing to regional security and stability, and to coalition operations around the world where our interests are engaged [Defence Corporate Plan 2019-2020, p 16].
- 19. On 25 February 2016, the Commonwealth released a Defence White Paper setting out its defence policy (**Defence White Paper**). The Defence White Paper identified three strategic defence interests. For each strategic defence interest, the Defence White Paper also identified an associated defence objective setting out the activities the government expected Defence to be able to conduct if it decided to use military power in support of the strategic defence interests.

Document: Annexed to this Statement of Agreed Facts and Issues at p 109 and marked 'Annexure 5' is a copy of extracts from the Defence White Paper dated 25 February 2016.

- 20. The three strategic defence interests identified in the Defence White Paper are [Defence White Paper p 17, Ch 3]:
 - 20.1. a secure, resilient Australia;
 - 20.2. a secure nearer region, encompassing maritime South East Asia and the South Pacific; and
 - 20.3. a stable Indo-Pacific region and rules-based global order.
- 21. The three strategic defence objectives identified in the Defence White Paper are, respectively [Defence White Paper pp 17-18]:
 - 21.1. to deter, deny and defeat any attempt by a hostile country or non-state actor to attack, threaten or coerce Australia;
 - 21.2. to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor-Leste and of Pacific Island Countries to build and strengthen their security; and
 - 21.3. to provide meaningful contributions to global responses to address threats to the rules-based global order which threaten Australia and its interests.
- 22. The delivery of the capability required by the Defence White Paper was identified as a key Defence activity or objective in the Defence Corporate Plans for each of 2016-17 (p 12), 2017-18 (p 15), 2018-19 (p 15, activity 2.1(c)) and 2019-20 (pp 9, 16).
- 23. The ADF defends Australia and its national interests through both its presence and posture in Australia and through the conduct of activities and operations overseas.

ADF deployment in Afghanistan

- 24. The ADF gives effect to the third strategic defence interest and third strategic defence objective (as identified in the Defence White Paper and outlined at [20.3] and [21.3] above) through a number of means, including by involvement in the mission known as Resolute Support. Resolute Support is the mission in Afghanistan led by the North Atlantic Treaty Organisation (NATO). Resolute Support launched on 1 January 2015, following the conclusion of the previous NATO-led International Security Assistance Force mission.
- 25. Resolute Support is an active, ongoing mission. Its purpose is to:
 - 25.1. train, advise and assist the Afghan National Defense and Security Forces; and
 - 25.2. help the Afghan security forces and institutions:
 - 25.2.1. develop the capacity to defend Afghanistan; and
 - 25.2.2. protect its citizens in a sustainable manner.

Document: Annexed to this Statement of Agreed Facts and Issues at p 148 and marked 'Annexure 6' is a copy of the NATO webpage located at https://rs.nato.int/about-us/mission.aspx extracted 5 September 2019.

26. Operation HIGHROAD, which began on 1 January 2015, is the ADF's commitment to Resolute Support.

Document: Annexed to this Statement of Agreed Facts and Issues at p 154 and marked 'Annexure 7' is an extract of Chapter 4, Volume 1 from the Defence Annual Report 2014-15 dated 9 October 2015.

- 27. Approximately 300 Australian personnel, comprising ADF members from the Royal Australian Navy, the Australian Army and the Royal Australian Air Force and Defence civilians, are currently deployed in Afghanistan as part of Operation HIGHROAD.
- 28. The ADF's Afghanistan headquarters for Operation HIGHROAD are at Kabul's Hamid Karzai International Airport and comprise a command element of about 40 ADF personnel. The command element coordinates administration, communications and logistics support for all ADF members deployed to Afghanistan.

Document: Annexed to this Statement of Agreed Facts and Issues at p 165 and marked 'Annexure 8' is a copy of the Defence webpage located at http://www.defence.gov.au/Operations/Afghanistan/ extracted 5 September 2019.

29. Prior to Operation HIGHROAD, Australia's military contribution to the International Security Assistance Force Mission in Afghanistan and the International Coalition Against Terrorism mission across Afghanistan and the Middle East was called Operation SLIPPER. That operation began in October 2001 and ended at the end of 2014.

C. THE ABC

30. The ABC is a national Australian public broadcaster and a news organisation.

- 31. Under s 27 of the ABC Act, the ABC is required to develop and maintain an independent service for the broadcasting of news and information and, subject to s 27(5), to broadcast daily from each broadcasting service regular sessions of news and information relating to current events within and outside Australia.
- 32. The ABC currently employs more than 800 journalists, and undertakes investigative journalism to produce stories for its news and current affairs programs, including programs dedicated to investigative journalism such as *Four Corners*.
- 33. The ABC prepares and publishes Corporate Plans under s 35 of the PGPA Act. A Corporate Plan was published for each of 2016-17, 2017-18, 2018-19, and 2019-20.

Document: Annexed to this Statement of Agreed Facts and Issues at p 166 and marked 'Annexure 9' is a copy of the ABC 2019-20 Corporate Plan dated 30 August 2019.

- 34. Among other things, the ABC's Corporate Plans include statements as to the ABC's purpose, vision and strategy [ABC Corporate Plan for 2019-2020, pp 4-5].
- 35. The ABC's Corporate Plan for 2019-20 states that part of the ABC's purpose is to support democracy through civic journalism that helps to keep industries and institutions accountable [ABC Corporate Plan for 2019-20, p 4].
- 36. The ABC is governed by the Board of Directors of the ABC (**Board**), established under s 7 of the ABC Act.
- 37. Under s 8(1)(c) of the ABC Act, it is a duty of the Board to ensure that the gathering and presentation by the ABC of news and information is accurate and impartial according to the recognised standards of objective journalism.
- 38. Under s 8(1)(e) of the ABC Act, it is a duty of the Board to develop codes of practice relating to programming matters, and to notify those codes of practice to the Australian Communications and Media Authority (**ACMA**).
- 39. At all relevant times, in fulfilment of the duty under s 8(1)(e) of the ABC Act, the ABC has had a Code of Practice developed by the Board. The Code of Practice sets out principles and standards for the ABC.

Document: Annexed to this Statement of Agreed Facts and Issues at p 192 and marked 'Annexure 10' is a copy of the Code of Practice issued on 1 March 2016.

Document: Annexed to this Statement of Agreed Facts and Issues at p 212 and marked 'Annexure 11' is a copy of the Code of Practice issued on 15 January 2019.

- 40. A failure to comply with the Code of Practice may result in the ABC being investigated by ACMA and in ACMA recommending that the ABC take action under s 152 of the *Broadcasting Services Act 1992* (Cth).
- 41. At all relevant times, the ABC has had Editorial Policies adopted by the Board.

Document: Annexed to this Statement of Agreed Facts and Issues at p 231 and marked 'Annexure 12' is a copy of the Editorial Policies issued on 15 January 2019.

42. The ABC Values & Standards of Workplace Behaviour states that a failure to comply with the Editorial Policies may constitute misconduct and may lead to disciplinary action being taken against an ABC employee.

Document: Annexed to this Statement of Agreed Facts and Issues at p 265 and marked 'Annexure 13' is a copy of the ABC Values & Standards of Workplace Behaviour as at 23 September 2019.

43. As at July 2017, one of the applicable Editorial Policies was Editorial Policy 5, titled 'Fair and honest dealing'.

Document: Annexed to this Statement of Agreed Facts and Issues at p 267 and marked 'Annexure 14' is a copy of the Editorial Policy titled 'Fair and honest dealing' as at July 2017.

- 44. From time to time, the Managing Director of the ABC authorises guidance notes to assist in the interpretation of the Editorial Policies.
- 45. On or about 11 April 2011, the Managing Director of the ABC authorised a guidance note titled 'Attribution / Anonymity of Sources' (**Guidance Note**). The Guidance Note has not been withdrawn.

Document: Annexed to this Statement of Agreed Facts and Issues at p 271 and marked 'Annexure 15' is a copy of the Guidance Note authorised on or about 11 April 2011.

- 46. In the course of their work, journalists employed by the ABC may obtain or receive documents and information from time to time from sources in circumstances where the journalist has promised the source not to disclose, directly or indirectly, the source's identity or to disclose documents from which the source's identity may be able to be ascertained. Journalists rely on information provided to them by sources who have provided that information on condition that their identity will be kept confidential.
- 47. In some circumstances, if the identity of a source of significant information were to be revealed, the source may be at risk of various types of harm to reputation, livelihood, property or person. Those close to the source, such as family members, may also be at risk. If sources who reveal information that serves a significant public interest face ramifications of those or other kinds, they and other actual or potential sources may be deterred from providing information in future.
- 48. Among other things, the Guidance Note:
 - 48.1. states that a basic rule of journalism is to protect the identity of sources when committed to do so:
 - 48.2. states that any failure to uphold the rule can result in serious potential costs in loss of trust and reduced information flow, both from the source affected and from other potential sources who may be deterred; and
 - 48.3. sets out ways in which journalists employed by the ABC must strive to maintain the protection of confidential sources.

- 49. The obligations of journalists relating to the protection of confidential sources are also reflected in like policies of other news organisations and associations of journalists, and the journalist's privilege in s 126K of the *Evidence Act 1995* (Cth) and cognate legislation.
- 50. In 1944, the Media, Entertainment and Arts Alliance (**MEAA**) adopted a Journalist Code of Ethics. The Journalist Code of Ethics was updated in 1984 and 1999. The version of the Journalist Code of Ethics adopted in 1999 has not been withdrawn.

Document: Annexed to this Statement of Agreed Facts and Issues at p 284 and marked 'Annexure 16' is a copy of the Journalist Code of Ethics adopted in February 1999.

- 51. Among other things, the current version of the Journalist Code of Ethics:
 - 51.1. requires journalists who are members of the MEAA to apply the following standard: 'Aim to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source. Where confidences are accepted, respect them in all circumstances'; and
 - 51.2. contains a 'Guidance Clause', which states: 'Basic values often need interpretation and sometimes come into conflict. Ethical journalism requires conscientious decision-making in context. Only substantial advancement of the public interest or risk of substantial harm to people allows any standard to be overridden.'
- 52. The MEAA has Rules.

Document: Annexed to this Statement of Agreed Facts and Issues at p 286 and marked 'Annexure 17' is a copy of the Rules of the MEAA current as at July 2017.

Document: Annexed to this Statement of Agreed Facts and Issues at p 353 and marked 'Annexure 18' is a copy of the current version of the Rules of the MEAA.

- 53. Journalism, and the publication of journalists' work, is one means by which public malfeasance, abuse of power, neglect and corruption may be brought to the attention of electors. The information that electors obtain as a result of journalistic work can be relevant to the decisions they make at Commonwealth, State, Territory and other elections.
- 54. There have been a number of occasions when the publication by the ABC of investigative journalism has brought public malfeasance, abuse of power, neglect and corruption to the attention of electors. Examples of ABC reporting on allegations of malfeasance, abuse of power, neglect and corruption include the following.
 - 54.1. On 17 and 24 September 2018, the ABC's *Four Corners* program broadcast episodes titled 'Who Cares?'. The episodes concerned allegations of abuse and mistreatment in aged care homes.
 - 54.2. On 9 April 2018, the ABC's *Four Corners* program broadcast an episode titled 'Mongrel bunch of bastards'. The episode concerned a joint ABC/Fairfax investigation into the Australian Taxation Office (**ATO**) and (among other things) the manner in which it used its powers.

- 54.3. On 25 July 2016, the ABC's *Four Corners* program broadcast an episode titled 'Australia's Shame'. The episode concerned the treatment of children in detention in the Northern Territory.
- 54.4. On 4 April 2016, the ABC's *Four Corners* program broadcast an episode titled 'The Panama Papers'. The episode concerned documents leaked to the International Consortium of Investigative Journalists known as the 'Panama Papers', which related to international tax avoidance, among other things.
- 54.5. On 16 February 2015, the ABC's *Four Corners* program broadcast an episode titled 'Making a Killing'. The episode concerned practices in the greyhound racing industry.
- 54.6. On 30 May 2011, the ABC's *Four Corners* program broadcast an episode titled 'A Bloody Business'. The episode concerned the treatment of Australian cattle exported to Indonesia.
- 54.7. On 11 May 1987, the ABC's *Four Corners* program broadcast an episode titled 'The Moonlight State'. The episode concerned corruption in Queensland Police.
- 55. Events subsequent to the reporting described at [54] above included the following:
 - 55.1. On 18 September 2018, the Prime Minister announced the Royal Commission into Aged Care Quality and Safety.
 - 55.2. On 10 April 2018, the Australian Government announced that the Treasury would conduct an inquiry into the ATO.
 - 55.3. On 26 July 2016, the Prime Minister announced the Royal Commission into the Protection and Detention of Children in the Northern Territory.
 - 55.4. As at 31 December 2017, the ATO had commenced or completed 557 investigations as a result of information obtained from the Panama Papers.
 - 55.5. In February 2015, the New South Wales Government established a Special Commission of Inquiry into the Greyhound Racing Industry in New South Wales. On 7 July 2016, the Commission delivered its report. That day, the New South Wales Government announced that it would shut down greyhound racing in New South Wales.
 - 55.6. On 7 June 2011, the Agriculture Minister announced that live cattle exports to Indonesia would be suspended.
 - 55.7. On 12 May 1987, the Deputy Premier of Queensland announced the Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct. On 3 July 1989, the Commission delivered its report. Subsequently, criminal charges were brought against the Queensland Police Commissioner and several Queensland politicians.

D. THE PUBLICATIONS

- 56. Daniel Michael Oakes (**Oakes**) and Sam Clark (**Clark**) were at all relevant times employed by the ABC in Victoria. Oakes was at all relevant times employed by the ABC as a journalist.
- 57. Oakes and Clark are, and were at all relevant times, members of the MEAA.
- 58. On 11 July 2017 at approximately 6.02 am, the ABC published a series of online stories by Oakes and Clark titled 'The Afghan Files' (**Afghan Files Stories**) on its website at www.abc.net.au/news. On 11 July 2017, the ABC updated the contents of each of those online stories. On 14 and 15 July 2017, the ABC further updated the contents of one of those online stories. The Afghan Files Stories reported on, inter alia, the operations of the ADF in Afghanistan.

Document: Annexed to this Statement of Agreed Facts and Issues at p 422 and marked 'Annexure 19' are copies of the updated versions of the Afghan Files Stories.

A playable version of the video embedded in the online story at the ABC webpage https://www.abc.net.au/news/2017-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642 will be tendered as part of this Statement of Agreed Facts and Issues as Exhibit A.

Document: A playable version of the video embedded in the webpage at https://www.facebook.com/abcnews.au/videos/inside-the-afghanfiles/10156950722999988/, which is the same video as that embedded in the online story at the ABC webpage described immediately above, will be tendered as part of this Statement of Agreed Facts and Issues as Exhibit B.

59. On 10 July 2017, the ABC broadcast an episode of its program 7.30 titled 'Afghan veteran raises disturbing allegations over the killing of civilians in Afghanistan' (7.30 Episode). Oakes and Clark were the authors of the 7.30 Episode. For the purposes of the balance of this Statement of Agreed Facts and issues, the abbreviation Afghan Files Stories includes a reference to the 7.30 Episode.

Document: Annexed to this Statement of Agreed Facts and Issues at p 466 and marked 'Annexure 20' is a copy of the ABC webpage located at https://www.abc.net.au/7.30/afghan-veteran-raises-disturbing-allegations-over/8695400 extracted 21 September 2019.

A playable version of the 7.30 Episode will be tendered as part of this Statement of Agreed Facts and Issues as Exhibit C.

- 60. The content of the Afghan Files Stories was capable of affecting the choice of electors at federal elections or referenda.
- 61. The Afghan Files Stories made reference to documents described as 'The Afghan Files' (**Afghan Files**). The Afghan Files are described in the Afghan Files Stories as being '[h]undreds of pages of secret defence force documents leaked to the ABC'.
- 62. The Afghan Files were described in the Afghan Files Stories as including documents marked with the following protective markings:

62.1. the security classification: 'SECRET'; and

- 62.2. the caveat 'AUSTEO'.
- 63. The meanings of those protective markings are described at [104.3] and [106.2], below.
- 64. In preparing the Afghan Files Stories, Oakes and Clark relied on information provided to Oakes by informants in circumstances where Oakes had promised the informants not to disclose the informants' identity. The Afghan Files Stories stated that they were based upon information provided by such sources.

E. THE MCBRIDE PROCEEDING

- 65. David William McBride (**McBride**):
 - 65.1. was between 2005 and 2009 a commissioned officer of the Australian Army Reserve holding the rank of Captain;
 - 65.2. was between 2005 and 2017 a Specialist Service Officer in the Australian Army Legal Corps;
 - 65.3. was between 2009 and 2017 a commissioned officer in the Australian Regular Army holding the rank of Major; and
 - 65.4. at all times between 20 June 2008 and 25 May 2016, held a security clearance that permitted him to access documents classified as SECRET (see further [104] and [108.4], below).
- 66. On 5 September 2018, McBride was charged with Theft contrary to s 131.1.01 of the Schedule to the *Criminal Code Act 1995* (Cth) (**Criminal Code**).

Document: Annexed to this Statement of Agreed Facts and Issues at p 473 and marked 'Annexure 21' is the Bench Sheet for the charges laid against McBride on 5 September 2018.

- 67. McBride entered a plea of not guilty in respect of this charge on 30 October 2018.
- 68. On 7 March 2019, McBride was further charged with:
 - 68.1. unlawfully giving information as to defences, contrary to s 73A(1) of the Defence Act: and
 - 68.2. unlawfully disclosing a Commonwealth document contrary to s 70(1) of the Crimes Act.

Document: Annexed to this Statement of Agreed Facts and Issues at p 474 and marked 'Annexure 22' is the Bench Sheet for the charges laid against McBride on 7 March 2019.

- 69. McBride entered a plea of not guilty in respect of these charges on 30 May 2019.
- 70. The charges described in paragraphs [66] and [68] are described below as the **alleged McBride offences**.

- 71. On 18 July 2019, McBride was committed to stand trial in respect of the alleged McBride offences pursuant to s 88B of the *Magistrates Court Act 1930* (ACT), on his application and with the prosecutor's consent (**McBride proceeding**).
- 72. On 8 August 2019, the Commonwealth Director of Public Prosecutions filed an indictment in the McBride proceeding specifying five counts in respect of the alleged McBride offences.

Document: Annexed to this Statement of Agreed Facts and Issues at p 478 and marked 'Annexure 23' is the indictment filed against McBride in the Supreme Court of the Australian Capital Territory on 8 August 2019

73. In March, May, June and July 2019, various media outlets reported that McBride made public statements concerning the allegations against him.

Document: Annexed to this Statement of Agreed Facts and Issues at p 481 and marked 'Annexure 24' is an article published by The Canberra Times dated 7 March 2019 titled 'I'm not afraid of going to jail': Ex-Defence lawyer charged over document leak'.

Document: Annexed to this Statement of Agreed Facts and Issues at p 483 and marked 'Annexure 25' is an article published by The Canberra Times dated 31 May 2019 titled 'Ex-Defence whistleblower charged over leak to journalists committed to stand trial'.

Document: Annexed to this Statement of Agreed Facts and Issues at p 485 and marked 'Annexure 26' is an article published by The Guardian dated 13 June 2019 titled 'Afghan Files whistleblower David McBride's trial delayed to protect state secrets'.

Document: Annexed to this Statement of Agreed Facts and Issues at p 487 and marked 'Annexure 27' is the transcript of a video uploaded to the website of the Gold Coast Bulletin dated 18 July 2019, located at https://www.goldcoastbulletin.com.au/news/national/rawwhistleblower-david-mcbride-speaks-outsidecourt/video/1cc9e8e46602db9e9b322e7263989491

F. THE INVESTIGATION

74. On 13 September 2018, each of Oakes and Clark received, via their respective ABC email addresses, a letter from the AFP.

Document: Annexed to this Statement of Agreed Facts and Issues at p 488 and marked 'Annexure 28' are copies of the 13 September 2018 letters addressed to each of Oakes and Clark (with sensitive and irrelevant information redacted by agreement of the Applicant and the Second and Third Respondents).

75. Also on 13 September 2018, Mr Gaven Morris, Director of News, Analysis and Investigations at the ABC, received, via his ABC email address, a letter from the AFP.

Document: Annexed to this Statement of Agreed Facts and Issues at p 490 and marked 'Annexure 29' is a copy of that letter (with sensitive and irrelevant information redacted by agreement of the Applicant and the Second and Third Respondents).

76. On 4 October 2018, the AFP received a letter from the ABC.

Document: Annexed to this Statement of Agreed Facts and Issues at p 491 and marked 'Annexure 30' is a copy of that letter (with sensitive and irrelevant information redacted by agreement of the Applicant and the Second and Third Respondents).

77. On 24 January 2019, Mr Michael Rippon (**Rippon**), Senior Lawyer, Disputes-Legal, received an email from FA Brumby.

Document: Annexed to this Statement of Agreed Facts and Issues at p 492 and marked 'Annexure 31' is a copy of that email (with sensitive and irrelevant information redacted by agreement of the Applicant and the Second and Third Respondents).

78. On 1 April 2019, Rippon received an email from FA Brumby, attaching two letters, one of which was addressed to Oakes, and the other addressed to Clark.

Document: Annexed to this Statement of Agreed Facts and Issues at p 494 and marked 'Annexure 32' is a copy of that email and its attachments (with sensitive and irrelevant information redacted by agreement of the Applicant and the Second and Third Respondents).

G. THE WARRANT

- 79. On 3 June 2019, Registrar Kane issued the search warrant at issue in this proceeding (Warrant). The Warrant purported to authorise FA Brumby or a constable assisting him to enter the ABC's premises in order to search for specified classes of things that there were reasonable grounds for suspecting would afford evidence as to whether:
 - 79.1. between 14 April 2016 and 1 October 2016, McBride gave Oakes military information, contrary to s 73A(1) of the Defence Act;
 - 79.2. between 14 April 2016 and 1 October 2016, Oakes unlawfully obtained military information, contrary to s 73A(2) of the Defence Act;
 - 79.3. between 1 March 2013 and 20 December 2014, McBride stole property belonging to the Commonwealth, contrary to s 131.1(1) of the *Criminal Code Act 1995* (Cth);
 - 79.4. between 14 April 2016 and 1 October 2016, Oakes dishonestly received stolen property from McBride, knowing or believing that the property was stolen, contrary to s 132.1 of the *Criminal Code Act 1995* (Cth); and
 - 79.5. about 1 May 2016, McBride unlawfully disclosed a fact or document which came into his knowledge by virtue of him being a Commonwealth officer, contrary to s 70(1) of the Crimes Act.

Document: Annexed to this Statement of Agreed Facts and Issues at p 499 and marked 'Annexure 33' is a copy of the Warrant dated 3 June 2019.

- 80. On 5 June 2019, FA Brumby executed the Warrant on the ABC's premises. FA Brumby and the constables assisting him seized documents and things purportedly pursuant to the Warrant (**Seized Material**).
- 81. On 6 June 2019, the ABC broadcast on its ABC News channel a live press conference by the then Acting Commissioner of the AFP, Neil Gaughan, concerning, among other things, the execution of the search warrant at the premises of the ABC on 5 June 2019.

Document: Annexed to this Statement of Agreed Facts and Issues at p 507 and marked 'Annexure 34' is a copy of a transcript of the press conference on 6 June 2019.

H. THE MINISTERIAL DIRECTION

82. On 8 August 2019, the Minister for Home Affairs issued a Ministerial Direction under s 37(2) of the AFP Act.

Document: Annexed to this Statement of Agreed Facts and Issues at p 517 and marked 'Annexure 35' is a copy of the Ministerial Direction issued on 8 August 2019.

I. THE PROTECTION OF SENSITIVE DEFENCE INFORMATION

83. The effective functioning of national governments in relation to national security, international relations and economic interests of the State, including in its relationships with foreign governments and international organisations, requires some information to be kept secret from the public. This extends to governments of representative democracies. To that end, western democracies including the United Kingdom, the United States of America, Canada and New Zealand have legal frameworks that are designed to identify information that needs to be kept secret and then to require that information to be kept secret.

Protection of sensitive defence information under colonial and early UK legislation

- 84. Prior to Federation, the Imperial Parliament had enacted the *Official Secrets Act 1889* (52 & 53 Vict. c. 52) (**Official Secrets Act 1889**), which extended to the colonies by virtue of s 6(1) of the Act, except where its operation was suspended pursuant to an order made under s 5.
- 85. Section 1 of the Official Secrets Act 1889 made it an offence (amongst other things) for certain persons in certain circumstances to communicate information relating to a 'fortress, arsenal, factory, dockyard, camp, ship, office, or other like place belonging to Her Majesty', or information relating to 'the naval or military affairs of her Majesty' which it was not 'in the interest of the State' to communicate.
- 86. In addition to the Official Secrets Act 1889, the Australian colonies enacted laws which regulated the disclosure of official information, either of specific kinds or more generally, including:
 - 86.1. the Safety of Defences Act 1890 (Qld) s 6, which made it an offence for an officer or member of the Defence Force or officer of the Civil Service to communicate, otherwise than in the course of official duty, 'any plans, documents, or other information relating to any battery, field-work, or fortification in Queensland, or to any other defences of the Colony';
 - 86.2. the Safety of Defences Act 1890 (SA) s 5, which made it an offence for an officer or member of the Defence Forces or officer of the Civil Service to communicate, otherwise than in the course of official duty, 'any plans, documents, or other information relating to any fort, battery, field-work, or fortification or other work of military defence, or to any other defences of the province';
 - 86.3. the Safety of Defences Act 1891 (Tas) s 6, which made it an offence for an officer or member of the Defence Force or officer of the Civil Service to communicate, otherwise than in the course of official duty, 'any plans, documents, or other information relating to any battery, field-work, or fortification in Tasmania, or to any other defences of the Colony';
 - 86.4. the Safety of Defences Act 1892 (WA) s 5, which made it an offence for an officer or member of the Defence Forces or officer of the Civil Service to communicate,

otherwise than in the course of official duty, 'any plans, documents, or other information relating to any fort, battery, fieldwork, fortification, or other work of military defence in Western Australia, or to any other defences of the Colony'; and

86.5. the Criminal Code Act 1899 (Qld), which:

- 86.5.1. by s 84, made it an offence for a person employed in the Public Service to communicate, otherwise in the course of official duty, 'any plans, documents, or other information, relating to any battery, field work, or fortification, in Queensland, or relating to any other defence of Queensland'; and
- 86.5.2. by s 85, made it an offence for any person to procure a person employed in the Public Service to make a communication falling within s 84, or to obtain information as to any matter falling within s 84 without lawful authority.
- 87. The Official Secrets Act 1889 was repealed and replaced by the Official Secrets Act 1911 (UK) (Official Secrets Act 1911). Section 1(1)(c) of that Act contained an offence of obtaining or communicating 'any sketch, plan, model, article, or note, or other document or information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy' 'for any purpose prejudicial to the safety or interests of the State'.

Document: Annexed to this Statement of Agreed Facts and Issues at p 519 and marked 'Annexure 36' is a copy of extracts of colonial and early UK legislation described at [84]-[87] above.

Protection of sensitive defence information under the Defence Act

- 88. In 1903, the Commonwealth Parliament enacted the Defence Act. At that time, s 73(4) of that Act made it an offence for any member of the Defence Force or officer in the Public Service of the Commonwealth to communicate, otherwise than in the course of official duty, 'any plan document or information relating to any fort battery fieldwork fortification or defence work or to any of the defences of the Commonwealth'. Section 73(5) of that Act made it an offence for a person to unlawfully obtain 'any plan document or information relating to any fort battery fieldwork fortification or defence work or to any of the defences of the Commonwealth'.
- 89. In 1917, s 73(4) and (5) of the Defence Act were repealed and replaced by the *Defence Act 1917* (Cth), which relevantly inserted s 73A.
- 90. In 2001, cl 8 of Sch 1 to the *Defence Legislation Amendment (Application of Criminal Code) Act 2001* (Cth) repealed and replaced s 73A.

Document: Annexed to this Statement of Agreed Facts and Issues at p 542 and marked 'Annexure 37' is a copy of extracts of the historical Defence Act legislation described at [88]-[90] above.

91. At all relevant times, s 73A(2) of the Defence Act has made persons less likely to communicate to electors material to which that provision applies.

92. At all relevant times, s 73A(2) of the Defence Act has effectively burdened the implied freedom of political communication.

Commonwealth policies, instructions and rules governing the protection of sensitive defence information

- 93. Since at least 1944, the Commonwealth government has promulgated policies, instructions and rules in relation to the protection of sensitive government information, including information relating to defence. These included:
 - 93.1. a document published by the Prime Minister's Department on 19 October 1948 entitled 'Instructions for the Security of Official Documents and Information'. The foreword to that document, written by Prime Minister Chifley, said that it contained 'instructions for the security of official documents and information within Commonwealth Departments and Instrumentalities';
 - 93.2. a document published by the Attorney-General's Department in May 1954 entitled 'Security of Classified Matter in Government Departments and Instrumentalities'. The foreword to that document, written by Prime Minister Menzies, said that it was the 'duty' of all members of the Commonwealth Government Service to 'safeguard the official information which is entrusted to [them]' and that the 'rules laid down in this booklet are designed to help [the members of the Commonwealth Government Service] fulfil this duty, and it is essential that they should be faithfully observed'; and
 - 93.3. a re-print of the document referred to in 93.2 published by the Attorney-General's Department in June 1960.

Documents: Annexed to this Statement of Agreed Facts and Issues at p 551 and marked 'Annexure 38' are copies of the historical policies referred to at [93].

- 94. Since 2010, the Commonwealth government has had in place a 'Protective Security Policy Framework' (**PSPF**) which is made up of a collection of documents organised into a hierarchy (the base level of which is agency-specific).
- 95. Immediately prior to October 2018 (at which time the PSPF was materially amended), and at all relevant times for the purposes of this proceeding, the PSPF comprised the following 'hierarchy' of instruments:
 - 95.1. a 'Directive on the Security of Government Business' (**Directive**), issued by the Attorney-General Senator the Hon George Brandis QC on 21 October 2014;
 - 95.2. three Core Policies (including an Information Security Core Policy) and mandatory requirements;
 - 95.3. a number of protocols, standards and guidelines; and
 - 95.4. agency-specific security policies and procedures.
- 96. An overview of the PSPF as it applied at all relevant times, and a copy of the Directive, is contained in a document entitled 'Securing Government Business Protective security

guidance for executives (v 2.1)' (**Guidance**). The Attorney-General Senator the Hon George Brandis QC caused the Guidance to be published in or about April 2015.

Document: Annexed to the statement of agreed facts at p 668 and marked 'Annexure 39' is a copy of the Guidance dated April 2015.

Defence-specific information security policies and procedures

97. On 21 May 2010, the Defence Instruction (General) ADMIN 20-29 – Defence Security Manual was issued.

Document: Annexed to the statement of agreed facts at p 685 and marked 'Annexure 40' is a copy of Defence Instruction (General) ADMIN 20-29 – Defence Security Manual dated 21 May 2010.

98. On 9 July 2015, the Defence Security Manual v 5 (**DSM**) was issued in accordance with Defence Instruction (General) ADMIN 20-29.

Document: Annexed to the statement of agreed facts at p 690 and marked 'Annexure 41' is a copy of extracts of the Defence Security Manual v 5 as at 9 July 2015 (minus some annexes and attachments).

- 99. The DSM was issued with the authority of the Chief of the Defence Force and the Secretary:
 - 99.1.1. under s 9A of the Defence Act (as continued in force by schedule 1, clause 65(1) of the *Defence Legislation Amendment (First Principles) Act 2015* (Cth)) for members of the ADF; and
 - 99.1.2. with the authority of the Secretary pursuant to s 20 of the Public Service Act for Department employees.
- 100. The mandatory requirements of the DSM:
 - 100.1. constituted a general order to Defence Members for the purposes of the *Defence Force Discipline Act* 1982 (Cth) (**Defence Discipline Act**); and
 - 100.2. had effect as a direction to Defence employees by the Secretary for the purpose of s 13(5) of the Public Service Act.
- 101. The DSM implemented the requirements of the PSPF and contained additional requirements addressing the particular security requirements of the ADF and the Department. It was replaced by the Defence Security Principles Framework on 2 July 2018.
- 102. The portions of the DSM described at [103]-[109] below, and annexed at Annexure 19, applied from 9 July 2015 and at all relevant times thereafter until 2 July 2018.
- 103. Part 2:30 of the DSM:
 - 103.1. required Australian Government employees to have agency authorisation to release any information to members of the public ([11]);

- 103.2. required Defence personnel or external service providers generating official information to assess the potential damage that could be caused by the compromise of the information, identify any legal, regulatory or Cabinet requirements applicable to the information, and assign any required protective marking(s) to the information ([16]); and
- 103.3. required Defence personnel and external service providers to ensure that official information is protected from unauthorised access as indicated by the protective markings ([107]).
- 104. One of the categories of protective markings under Part 2:30 of the DSM consisted of security classifications ([15]). There were four levels of security classification, which were said to reflect the consequences of the compromise of information ([28]):
 - 104.1. The PROTECTED security classification was to be used when the compromise of the confidentiality of information could be expected to cause minor damage to national security, damage to the national interest more broadly, or damage to organisations or individuals.
 - 104.2. The CONFIDENTIAL security classification was to be used when the compromise of the confidentiality of information could be expected to cause damage to national security, significant damage to the national interest more broadly, or significant damage to organisations or individuals.
 - 104.3. The SECRET security classification was to be used when compromise of the confidentiality of information could be expected to cause serious damage to national security, the national interest more broadly, or serious damage to organisations or individuals.
 - 104.4. The TOP SECRET security classification was to be used for information that required the highest degree of protection, in cases when compromise of the confidentiality of information could be expected to cause exceptionally grave damage to national security or to the national interest more broadly.
- 105. Part 2:30 of the DSM stated that information was only to be protectively marked when the results of compromise warranted the expense of increased protection or if there was a legislative or regulatory basis for the information to be protected ([24]). It noted that inappropriate over-classification had many seriously harmful effects ([25]), and that the Australian Government expected that Defence personnel and external service providers will only protectively mark information and preserve that marking where there is a clear and justifiable need to do so ([26]).
- 106. Part 2:30 of the DSM stated that certain information classified as PROTECTED or above may bear a 'caveat' in addition to a security classification ([71]–[72]). A caveat was stated to be a warning that the information had special requirements in addition to those indicated by the protective marking relating to the security classification ([71]). Several categories of security caveat were specified, including:

- 106.1. 'codewords', which were words indicating that the information covered was in a special need-to-know compartment, used to identify the source of certain information without revealing it to those who do not have a need-to-know ([75]); and
- 106.2. 'eyes only' 'releasibility indicators', which indicated that access to information was restricted to certain nationalities or coalitions of nations ([85], [87]). For example, the 'eyes only' caveat 'AUSTEO' indicated that access to information was limited to 'Australian Eyes Only' (meaning that only Australian citizens who hold the appropriate clearance were to be permitted access to that information) ([87], [90]-[92]).
- 107. Part 2:30 of the DSM required Defence personnel and external service providers to ensure that access to official information was limited to those who had the level of security clearance required and who needed to know the information for their official duties ([112]-[113]).
- 108. Part 2:20 of the DSM stated that Defence personnel and external service providers were to be security cleared to the level commensurate with the level of classified information or assets they are required to access, or the responsibilities they hold ([4]). The security clearance levels were as follows ([5]):
 - 108.1. Baseline, permitting ongoing access to Australian Government information and assets that are security classified up to and including PROTECTED;
 - 108.2. Negative Vetting Level 1 (NV1), permitting ongoing access to Australian Government information and assets that are security classified up to and including SECRET;
 - 108.3. Negative Vetting Level 2 (NV2), permitting ongoing access to Australian Government information and assets that are security classified up to and including TOP SECRET; and
 - 108.4. Positive Vetting (PV), permitting access to information and assets at all classification levels.
- 109. Part 2:30 of the DSM imposed requirements on the storage and secure destruction of security classified material ([107]-[129]).

Sensitive defence information generally

- 110. Members of the ADF and persons appointed or engaged under the Public Service Act may have access to information about:
 - 110.1. the nature and status of the physical resources of the ADF; and
 - 110.2. the intangible resources of the ADF including intelligence and operational information such as orders, directions, rules of engagement (see at [115]-[116],

below), reports, and information related to the ADF's activities or interactions with partner or allied forces.

- 111. Unauthorised disclosure of defence information contrary to the requirements of the information security framework established by the Commonwealth under the PSPF and Defence under the DSM (defence information disclosures) may undermine the ADF's ability to respond to threats and conduct successful missions. Disclosing defence information such as operational plans, techniques, tactics and procedures may diminish the effectiveness of those resources. Disclosure of such information may also expose Defence personnel to an elevated risk of harm.
- 112. Defence information disclosures may also harm Australia's relationships with allies and coalition members. A demonstrated inability to maintain the secrecy of certain types of defence information may reduce the willingness of those countries to share information with Australia.
- 113. A reduction in information-sharing by Australia's military partners may hinder the ADF's ability to plan for and respond to threats to Australia's national security, to defend Australia from armed attacks, and / or to participate effectively in joint operations.
- 114. In determining whether a defence information disclosure may have the effects described at [111] to [113] above, it is relevant to consider the nature of the information and the circumstances of disclosure.

Rules of Engagement

115. Rules of Engagement (ROEs) are directives issued to the ADF by the Chief of the Defence Force, in consultation with the Australian Government. ROEs regulate the use of force and activities connected with the use of force by the ADF. They are issued for operations across the full spectrum of military force, from armed conflict through to peacetime operations. ROEs constitute a general order to Defence Members for the purposes of the Defence Discipline Act.

Document: Annexed to the statement of agreed facts at p 745 and marked 'Annexure 42' is a copy of extracts from the Australian Defence Doctrine Publication (ADDP) 06.1 – *Rules of Engagement* edition 3, issued by the Chief of the Defence Force on 6 August 2019.

- 116. Unauthorised disclosure of ROEs for operations in which Australia has a current involvement or ROEs for concluded operations which current ROEs substantially replicate, contrary to the requirements of the information security framework established by the Commonwealth under the PSPF and Defence under the DSM (ROE disclosures), may increase the likelihood that the ADF's adversaries will ascertain the precise terms of current ROEs. If information about how ADF forces will operate during a mission is available to an adversary, that adversary may be more effective in combat with the ADF, as it may be able to adjust its strategy and operations in light of that information. For these reasons, ROE disclosures may:
 - 116.1. diminish the effectiveness of ADF tactics, techniques and operations;
 - 116.2. impede the success of ADF missions;

- 116.3. undermine the ADF's defensive capacity, both abroad and in Australian territory; and / or
- 116.4. physically endanger ADF members, increasing their risk of injury and death.
- 117. In determining whether an ROE disclosure may have the effects described at [116] above, it is relevant to consider the nature of the information and the circumstances of the disclosure.
- 118. The Second and Third respondents' agreement to [116] above should not be interpreted as an agreement that the disclosure of only the ROEs described in that paragraph may lead to the consequences described in that paragraph.

PART III ISSUES

- 119. The Applicant and the Second and Third Respondents agree that the following issues fall for determination by the Court:
 - (1) Is the First Respondent's decision to issue the Warrant invalid on any or all of the following grounds:
 - (a) the decision was not authorised by s 3E of the Crimes Act on its proper construction;
 - (b) the three conditions of the Warrant did not provide a real and meaningful perimeter to the evidential matters the Warrant purportedly authorised to be searched for and seized;
 - (c) the suspected offences specified in the third condition of the Warrant were expressed in a conclusionary, vague and uncertain manner;
 - (d) the Warrant purported to authorise the search and seizure of material that could not afford evidence as to the commission of the offences in sub-ss 73A(1) and (2) of the Defence Act that were specified in the third condition of the Warrant;
 - (e) the decision was legally unreasonable?
 - (2) Was the decision of the Second and Third Respondents to seek the Warrant legally unreasonable?
 - (3) Should the Court find that it is unnecessary to decide whether s 73A(2) of the Defence Act is invalid on the ground that it infringed the implied freedom of political communication, and decline to make a declaration that s 73A(2) is invalid:
 - (a) on the basis that the Applicant is not entitled to such relief because any error arising from the invalidity of s 73A(2) could not have affected the decisions to issue and execute the Warrant; or

(b) on the ground that such relief would lack utility and should be refused as a matter of discretion?

(4) If it is necessary to decide the issue, is s 73A(2) of the Defence Act invalid on the ground that it infringed the implied freedom of political communication?

(5) If the answer to any of questions (1)-(2) is 'yes', is the Applicant entitled to any of the following relief:

(a) a declaration that the Warrant is invalid;

(b) a declaration that the search of and seizure of materials from the Applicant's

premises in purported execution of the Warrant was unlawful;

(c) a declaration that the Second and Third Respondents, and all members, employees and agents of the AFP, are not entitled to examine the Seized

Material;

(d) an order that the Seized Material, any copies of the Seized Material, and

any related lists or schedules in the possession of the Second Respondent,

Third Respondent or the AFP, be returned immediately to the Applicant;

(e) an injunction permanently restraining the Second and Third Respondents,

and all members, employees and agents of the AFP, from viewing, accessing, copying or disseminating, or causing to be viewed, accessed,

copied or disseminated, the Seized Material, any copies of the Seized

Material, and any related lists or schedules?

(6) If the answer to question (4) is 'yes', is the Applicant entitled to a declaration that

s 73A(2) is invalid?

(7) Who should pay the costs of and incidental to this proceeding?

Date: 23 September 2019

Kristy Alexander

AGS lawyer

for and on behalf of the Australian Government Solicitor

Lawyer for the Second and Third Respondents

Michael Rippon

Lawyer for the Applicant

Date: 24 September 2019

Schedule

FEDERAL COURT OF AUSTRALIA DISTRICT REGISTRY: NEW SOUTH WALES

Division: General No NSD 989 of 2019

Respondents

Second Respondent Commissioner of the Australian Federal Police

Third Respondent Agent Ian Brumby of the Australian Federal Police

Date: 23 September 2019

FEDERAL COURT OF AUSTRALIA DISTRICT REGISTRY: NEW SOUTH WALES

Division: General No NSD 989 of 2019

AUSTRALIAN BROADCASTING CORPORATION

Applicant

MARTIN KANE

and others named in the Schedule Respondents

INDEX TO ANNEXURES TO STATEMENT OF AGREED FACTS AND ISSUES

No.	Description	Date	Page
1.	Defence 2016-17 Corporate Plan	23 August 2016	27
2.	Defence 2017-18 Corporate Plan	7 June 2017	45
3.	Defence 2018-19 Corporate Plan	28 June 2018	63
4.	Defence 2019-20 Corporate Plan	13 July 2019	85
5.	Extracts from the Defence White Paper	25 February 2016	109
6.	NATO webpage located at https://rs.nato.int/about-us/mission.aspx	5 September 2019	148
7.	Chapter 4, Volume 1 of the Defence Annual Report 2014-15	9 October 2015	154
8.	Defence webpage located at http://www.defence.gov.au/Operations/Afghanistan/	5 September 2019	165
9.	ABC 2019-20 Corporate Plan	30 August 2019	166
10.	Code of Practice	1 March 2016	192
11.	Code of Practice	15 January 2019	212
12.	Editorial Policies	15 January 2019	231
13.	ABC Values & Standards of Workplace Behaviour	as at 23 September 2019	265
14.	Editorial Policy titled 'Fair and honest dealing'	as at July 2017	267
15.	Guidance Note titled 'Attribution / Anonymity of Sources'	11 April 2011	271
16.	MEAA Journalist Code of Ethics	February 1999	284
17.	MEAA Rules	as at July 2017	286

18.	MEAA Rules	5 March 2019	353
19.	Afghan Files Stories:		
	A. The Afghan Files: Defence Leak Exposes Deadly Secrets of Australia's Special Forces	11 July 2017	422
	B. The Afghan Files: An Interrogation, a Shooting and No Witnesses	11 July 2017	432
	C. The Afghan Files: What the Documents Reveal About Killings of Unarmed Afghans	11 July 2017	435
	D. The Afghan Files: The Spy and the SAS Soldier with a Loaded Glock	11 July 2017	447
	E. The Afghan Files: Who is the Enemy? Australia's Secretive Rules of Engagement	15 July 2017	451
	F. The Afghan Files: What the F*** Are You Doing'. Chaos Over Severed Hands	11 July 2017	456
	G. The Afghan Files: Relations Between Australia's Special Forces Units on 'A Perilous Knife Edge'	11 July 2017	462
20.	ABC webpage located at https://www.abc.net.au/7.30/afghan-veteran-raises-disturbing-allegations-over/8695400	21 September 2019	466
21.	Bench Sheet for charges laid against McBride	5 September 2018	473
22.	Bench Sheet for charges laid against McBride	7 March 2019	474
23.	Indictment filed against McBride in the Supreme Court of the ACT	8 August 2019	478
24.	Canberra Times article titled 'I'm not afraid of going to jail': Ex-Defence lawyer charged over document leak'	7 March 2019	481
25.	Canberra Times article titled "Ex-Defence whistleblower charged over leak to journalists committed to stand trial"	31 May 2019	483
26.	Guardian article titled 'Afghan Files whistleblower David McBride's trial delayed to protect state secrets'	13 June 2019	485
27.	Transcript of a video uploaded to the website of the Gold Coast Bulletin	18 July 2019	487
28.	Letters from the AFP to Oakes and Clark of the ABC	13 September 2018	488
29.	Letter from the AFP to Gaven Morris of the ABC	13 September 2018	490
30.	Letter from the ABC to the AFP	4 October 2018	491
31.	Email from FA Brumby to Rippon of the ABC	24 January 2019	492
32.	Email from FA Brumby to Rippon attaching letters addressed to Oakes and Clark	1 April 2019	494
33.	Warrant	3 June 2019	499

34.	Transcript of Press Conference given by Acting Commissioner of the AFP Neil Gaughan	6 June 2019	507
35.	Ministerial Direction	8 August 2019	517
36.	Extracts of colonial and early UK legislation		
	A. Extracts from Official Secrets Act 1889	-	519
	B. Extracts from Safety of Defences Act 1890 (Qld)	-	523
	C. Extracts from Safety of Defences Act 1890 (SA)	-	527
	D. Extracts from Safety of Defences Act 1891 (Tas)	-	529
	E. Extracts from Safety of Defences Act 1892 (WA)	-	532
	F. Extracts from Criminal Code Act 1899 (Qld)	-	535
	G. Extracts from Official Secrets Act 1911	-	537
37.	Extracts of historical Defence Act legislation		
	A. Extracts from Defence Act 1903	-	542
	B. Extracts from Defence Act 1917	-	545
	C. Defence Legislation Amendment (Application of Criminal Code) Act 2001 (Cth)	-	549
38.	Historical policies		
	A. Document published by the Prime Minister's Department entitled 'Instructions for the Security of Official Documents and Information'	19 October 1948	551
	B. Document published by the Attorney-General's Department entitled 'Security of Classified Matter in Government Departments and Instrumentalities'	May 1954	560
	C. Document published by the Attorney-General's Department entitled 'Security of Classified Matter in Government Departments and Instrumentalities' (June 1960 reprint)	June 1960	631
39.	Guidance	April 2015	668
40.	Defence Instruction (General) ADMIN 20-29 – Defence Security Manual	21 May 2010	685
41.	Extracts from DSM	9 July 2015	690
42.	Extracts from the Australian Defence Doctrine Publication (ADDP) 06.1 – Rules of Engagement edition 3	6 August 2019	758



2016-2017 Defence Corporate Plan



Statement of Preparation

Denin Richard

I, as the accountable authority of Defence, present the 2016-17 Defence Corporate Plan, which covers the periods of 2016-20, as required under paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

Dennis Richardson AO Secretary of Defence

23 August 2016

© Commonwealth of Australia 2015

ISSN 2205-5282 (online)

ISBN 978-0-9944235-6-6

This publication is available for your use under a UCreative Commons BY Attribution 3.0 AustraliaU licence, with the exception of the Commonwealth Coat of Arms and the Department of Defence logo, signatures and where otherwise stated. The full licence terms are available from http://creativecommons.org/licenses/by/3.0/au/legalcode.



Use of the Department of Defence's material under a UCreative Commons BY Attribution 3.0 AustraliaU licence requires you to attribute the work (but not in any way that suggests that the Department of Defence endorses you or your use of the work).

Department of Defence material used 'as supplied'

Provided you have not modified or transformed the Department of Defence material in any way including, for example, by changing the Department of Defence text, the Department of Defence prefers the following attribution:

Source: The Australian Government Department of Defence

Derivative material

If you have modified or transformed the Department of Defence 's material, or derived new material from those of the Department of Defence in any way, then the Department of Defence prefers the following attribution:

Based on the Australian Government Department of Defence's data.

Contents

INTRODUCTION	2
PURPOSES	3
ENVIRONMENT	4
PERFORMANCE	6
CAPABILITY	13
RISK OVERSIGHT AND MANAGEMENT	15

Introduction

The 2016-17 Defence Corporate Plan sets out Defence's role, objectives and functions, referred to as Purposes in the PGPA Act,¹ and describes how we will measure our performance in achieving our Purposes. Performance against the Corporate Plan will be reported through Annual Performance Statements, to be included in the 2016-17 Defence Annual Report. The Corporate Plan is a living document and will be updated at least annually to reflect changes in our operating environment and to meet the requirements of the PGPA Act.

The Defence Purposes have been revised from the ten described in the 2015-16 Defence Corporate Plan to focus on the three core outcomes we deliver to Government:

- Provide advice to Government;
- Deliver and sustain Defence capability and conduct operations; and
- Develop the future capability Defence needs to conduct operations.

Our Purposes and Activities centre on delivering an effective defence capability for Government.² Over the life of this plan, we will continue to build capability to support our national security interests and promote them in a region that is growing more complex and dynamic, as described in the 2016 Defence White Paper.

In 2016-17 we will begin implementation of the new force structure and capabilities identified in the 2016 Defence White Paper. These changes are essential if we are to transform Defence into an organisation that can effectively deliver on our primary role: to protect and advance Australia's strategic interests through the provision of military capabilities, the promotion of security and stability, and to provide support for the Australian community and civilian authorities as directed by Government.

In delivering Defence capability to Government, Defence will continue to undertake significant organisational change resulting from the First Principles Review, *Creating One Defence*, while continuing to build on and deliver our cultural reform program, *Pathway to Change*. It is essential we continue to build our organisational capability and culture if we are to achieve our Purposes both now and into the future.

We are pleased to present the 2016-17 Defence Corporate Plan.

Dennis Richardson AO

Penin Richard

Secretary of Defence

23 August 2016

Mark Binskin AC

Air Chief Marshal

Chief of the Defence Force

23 August 2016

Purposes are defined by Part 1, Division 2—8 of the *Public Governance, Performance and Accountability Act 2013* as 'the objectives, functions or role' of an entity.

Defence Capability is the power to achieve a desired operational effect in a nominated environment within a specified time and to sustain that effect for a designated period. In a military context, capability is achieved by developing a force structure appropriately prepared for a range of military operations. Australian Defence Doctrine Publication 00.2, 'Executive Series: Preparedness and Mobilisation', 2013.

Purposes

The Defence mission is to defend Australia and its national interests.

Defence's primary role is to protect and advance Australia's strategic interests through the provision of military capabilities, the promotion of security and stability, and to provide support for the Australian community and civilian authorities as directed by Government.³ In fulfilling its mission, Defence has three Purposes:

- 1. Provide advice to Government
- 2. Deliver and sustain Defence capability and conduct operations
- 3. Develop the future capability Defence needs to conduct operations

Programs described in the Defence Portfolio Budget Statements 2016-17 contribute to the Defence Purposes, as shown in Table 1.

	Defence Purposes		
Defence Portfolio Budget Statements 2016-17 Programs	1. Provide advice to Government ⁴	2. Deliver and sustain Defence capability and conduct operations	3. Develop the future capability Defence needs to conduct operations
1.1 Strategic Policy and Intelligence	•	•	•
1.2 Navy Capabilities		•	•
1.3 Army Capabilities		•	•
1.4 Air Force Capabilities		•	•
1.5 Joint Operations Command		•	
1.6 Vice Chief of the Defence Force	•	•	•
1.7 Capability Acquisition and Sustainment		•	•
1.8 Defence Executive Support	•	•	
1.9 Estate and Infrastructure		•	
1.10 Chief Information Officer		•	
1.11 Defence People		•	•
1.12 Defence Science and Technology		•	•
1.13 Chief Finance Officer	•		
1.14 Defence Force Superannuation Benefits		•	
1.15 Defence Force Superannuation Nominal Interest		•	
1.16 Housing Assistance		•	
1.17 Other Administered		•	
2.1 Operations Contributing to the Security of the Immediate neighbourhood		•	
2.2 Operations Supporting Wider Interests		•	
3.1 Defence Contribution to National Support Tasks in Australia		•	

Table 1. Defence Portfolio Budget Statement Programs mapped to Purposes

³ This statement is drawn from the outcome statements in the Defence Portfolio Budget Statements.

⁴ Advice will be provided through the Strategic Center.

Environment

Security

Australia's security environment is changing. The role of Defence is to protect and advance Australia's strategic interests through the provision of military capabilities, the promotion of security and stability, and to provide support for the Australian community and civilian authorities as requested by Government. Defence does this through the strategies described in the 2016 Defence White Paper. Defence must be prepared to undertake a diverse range of possible operational requirements as directed by Government.

Defence has the most extensive land and property holdings in Australia, including large training areas and bases close to the coastline. Recognising the challenges posed by climate change, Defence is undertaking studies to determine the level of risk and implementing mitigation strategies to reduce the impact to bases and training areas.⁵

Organisational Capability

The First Principles Review: *Creating One Defence*, requires that Defence become a more integrated organisation, with clear accountabilities and streamlined decision-making processes. Successful implementation of the recommendations of the First Principles Review will ensure that Defence has the organisational capability it needs to deliver the 2016 Defence White Paper and to respond to a wide range of operational requirements both now and into the future.

The PGPA Act requires all entities to take a deliberate approach to corporate planning and performance management, supported by a stronger risk management framework that aligns to the Commonwealth Risk Management Policy. Improved corporate risk management, business planning and performance management will enable Defence to focus all activities on achieving Government-directed outcomes.

Risks to the achievement of the Defence mission are managed by risk stewards in accordance with the Defence Enterprise Risk Management Framework, which is described in the Risk Oversight and Management section. The risks are reviewed and updated at least annually, or when there are changes in Defence's operating environment.

Diversity

Diversity and inclusion in Defence is a critical capability issue. We must harness the broadest talents if we are to remain prepared to defend Australia. The Defence Diversity and Inclusion Strategy 2012-2017 outlines five strategic goals which will underpin successful diversity and inclusion in Defence:

- 1. Defence is a flexible, adaptable and agile organisation that is able to accommodate the diverse needs of people as they move through various life and career stages.
- 2. Defence utilises creative, targeted human resource solutions to achieve the numerous strategic capability benefits that diversity brings to all levels of the organisation.
- 3. Defence recognises and understands that true inclusiveness does not mean treating everyone exactly the same way, all the time.
- 4. Defence is viewed by all as an organisation committed to diversity and inclusion.
- 5. Defence has strategies in place to support the employment of identified diverse groups that require immediate priority attention.

Department of Environment 2015, National Climate Resilience and Adaptation Strategy p. 31, Canberra, Viewed 02 March 2016 http://www.environment.gov.au/system/files/resources/3b44e21e-2a78-4809-87c7-a1386e350c29/files/national-climate-resilience-and-adaptation-strategy.pdf

The Australian National Action Plan on Women, Peace and Security 2012-2018 is a whole-of-Government policy to implement the United Nations Security Council Resolution 1325 (UNSCR 1325) and other United Nations (UN) Security Council resolutions related to Women, Peace and Security. The Women, Peace and Security agenda is central to Defence's operational effectiveness and success and will be an essential component of future planning and conduct of operations.

Performance

Purpose 1. Provide advice to Government

Defence must provide high-quality, coherent and timely policy advice to Government on Defence strategy, capability and resourcing. As part of First Principles Review implementation, Defence has brought strategic policy functions together in order to improve the quality of advice provided to Government.

The Government expects Defence to be able to defend Australia and its national interests, to play an active role in contributing to regional security and stability, and to contribute to coalition operations across the world where our interests are engaged. Delivering on these requirements will require Australia to build on its strong network of bilateral and multilateral relationships. Through regular dialogue and practical cooperation, Defence will strengthen its engagement with partners to support shared responses to shared challenges.

The **One Defence** business model recommended by the First Principles Review requires strong alignment between strategy, funding and capability. Effective corporate planning and performance monitoring are vital to ensure the direction set in the strategic centre is effectively cascaded through the organisation and that leaders are held to account for their performance. As required by the PGPA Act, Defence continues to improve the way it plans, prioritises and manages resources to achieve Government-directed outcomes.

Performance measures

i. Government has confidence in	2016–2020	
Measured and reported	Measured bi-annually. Reported annually.	
Methodology	Bi-annual survey of the relevant Ministers and the central	al agencies.

ii. Government is assured that De	2016–2020	
Measured and reported	Measured bi-annually. Reported annually.	
Methodology	Bi-annual survey of the relevant Ministers and the central	al agencies.

Activities

Activities	Intended Results	Performance Criteria	When
Defence provides clear, accurate and timely advice to Government.	The Minister receives policy advice that supports effective decision-making.	Measure: Government has confidence in the relevance and quality of Defence advice. Target: Minister expresses high to very high confidence in Defence advice.	Ongoing
Defence ensures that the policy development process incorporates inputs from relevant stakeholders through processes that include contestability.	Defence strengthens its engagement on policy development with other national security participants and other relevant parties.	Measure: Decision-makers understand Australian defence and national security policy issues Target: Stakeholders express high confidence in Defence engagement.	Ongoing
Use data and information to support risk-informed decision-making by Defence's senior leaders.	Appropriate risk appetite is actively exercised based on all available information. Assured data is available to support the design of good performance measures. Managers across Defence have a view of performance within their work area that is based on true information, enabling them to make more robust resource decisions.	Measure: Performance information uses validated information to support decision-making. Target: All performance information is supported by a reliable and validated data source.	Ongoing

Purpose 2. Deliver and sustain Defence capability and conduct operations

Defence advances Australia's strategic interests by planning for, and developing and maintaining the capability to deter and defeat armed attacks on Australia or on Australian interests. This includes planning for, conducting, controlling and evaluating Defence and/or coalition contributions to Government-directed operations.

Defence also supports the Commonwealth and State/Territory Governments with emergency and non-emergency tasks, as well as supporting events of national significance as requested by relevant authorities and the general public.

The joint force is the standing, prepared force that provides options to Government for future joint force operations. This includes the current disposition of the ADF, force structure and posture, as well as including all elements of the fundamental inputs to capability.

As required in the 2016 Defence White Paper, Defence will increase the level of preparedness over time to meet Government-directed outcomes.

Performance measures

i. Required preparedness levels are achieved.		2016–2020
Measured and reported	Measured tri-annually. Reported annually.	
Methodology	Assessment of preparedness against the Chief of the Defence Force Preparedness Directive.	

ii. Operational outcomes meet the requirements of Government policy.		2016–2020
Measured and reported	Measured tri-annually. Reported annually.	
Methodology	Assessment of operational deployments against operational outcomes agreed with Government.	

iii. The capability delivery process maintains the integrity of the Integrated Investment Program and delivers the required capability for the force-in-being.		2016–2020
Measured and reported	Measured tri-annually. Reported annually for each year of the corporate plan.	
Methodology	Assessment of delivery against the Integrated Investment Program.	

iv. Military capability is sustained	2016–2020	
Measured and reported	easured and reported Measured tri-annually. Reported annually for each year of the corporate plan.	
Methodology	Assessment of sustainment against capability manager requirements.	

Activities

Activities	Intended Results	Performance Criteria	When
Ensure Defence's operational capabilities are available to meet Government direction.	Government is able to deploy defence capability to support Government policy objectives.	Measure: Chief of the Defence Force preparedness levels meet Government requirements. Target:	Ongoing
		Chief of the Defence Force preparedness levels are achieved as agreed with Government.	
Conduct joint, combined and interagency operations as directed by Government.	Joint forces are able to be deployed and sustained efficiently and effectively, and in accordance with Government timeframes.	Measure: Operational outcomes meet the requirements of Government policy. Target: All operational requirements are met.	Ongoing
Deliver intelligence services.	Defence intelligence services enable efficient operations across national security agencies.	Measure: Defence intelligence outputs align with Government intelligence priorities. Target: Whole-of-Government and Australian Defence Force intelligence requirements are met.	Ongoing
Deliver health and welfare services to meet the requirements of the Australian Defence Force.	Effective and efficient health support and welfare services are provided.	Measure: Quality of health and welfare services delivered to Australian Defence Force members and families. Target: Delivery meets agreed standards.	Ongoing
Implement the First Principles Review plan.	Defence develops organisational capability that ensures it can achieve Government-directed outcomes.	Measure: Implementation of the First Principles Review recommendations. Target: Implementation is achieved by 30 June 2017.	2016–17

Activities	Intended Results	Performance Criteria	When
Deliver corporate and military enabling services to enable Defence capability.	Defence has the corporate and military enabling services it needs to support preparedness and operational requirements.	Measure: Enabling services meet requirements. Target: Satisfaction with the service delivery system increases over time.	2016–17
Australian Government Security Vetting Agency to strengthen its ability to meet its Charter. Support Government capability through the provision of timely and quality security vetting services.	The Australian Government Security Vetting Agency delivers the required security vetting service.	Measure: Quality of Australian Government Security Vetting Agency services. Target: The Australian Government Security Vetting Agency meets its service charter.	2016–17

Purpose 3. Develop the future capability Defence needs to conduct operations

The capability life cycle is a core business process that enables Defence to perform its mission of defending Australia and its national interests. Defence must procure capability efficiently and effectively. As part of First Principles Review implementation, Defence is establishing a single end-to-end capability development function, which creates fewer hand-over points, reduces risk and complexity, and promotes a closer relationship between customer and purchaser. This includes development of a stronger contestability function as part of the new investment approval process for the major capital programs.

Australia's defence industry is a major partner in the Government's plans for current and future Defence capabilities. It is vital that Australia maintains a science and technology base, and defence industry capable of supporting Defence's acquisition and sustainment requirements during peacetime and operations. A highly skilled and capable Australian defence industry is necessary for Defence to achieve its strategic objectives and deliver large-scale, complex projects and sustain military capability. Defence will work with industry to reflect a shared policy agenda that supports the growth and competitiveness of Australian businesses.

In 2016–17, Defence will continue building the new levels of capability required by Government and described in the 2016 Defence White Paper and the Integrated Investment Program. Major investments will enhance Australian Defence Force capability to conduct operations to deter and defeat threats to Australia, operate over longer distances to conduct independent combat operations in our region, and make more effective contributions to international coalitions.

Performance measures

 The Integrated Investment Program is managed effectively and comprises all investment and sustainment inputs, incorporating the Fundamental Inputs to Capability. 		2016–2020
Measured and reported	Measured bi-annually. Reported annually.	
Methodology	Regular independent assurance of the Defence capability deve process by the Defence Audit and Risk Committee.	
	2. Regular reviews of the Integrated Investment Program in cons with the Minister and central agencies.	

ii. Emerging capability and technology is used to support development of best value-for-money capability.		2016–2020
Measured and reported	Measured tri-annually. Reported annually.	
Methodology	Regular assessment of how Defence's strategic research builds understanding of future Defence capability.	

iii. Defence capability development leverages industry to promote innovation.		2016–2020
Measured and reported Measured tri-annually. Reported annually.		
Methodology	Regular assessment of the value of Defence engagement with industry.	

Activities

Activities	Intended Results	Performance Criteria	When
Deliver the capability required by the 2016 Defence White Paper.	Defence develops the capability it needs to meet Government's requirements now and into the future.	Measure: Effective implementation of the 2016 Defence White Paper. Target: The 2016 Defence White Paper implementation plan activities for 2016-20 are delivered as agreed with Government.	Ongoing
Establish the Centre for Defence Industry Capability and the Defence Innovation Hub to engage with industry to enhance and sustain Defence capability.	A competitive Australian industrial base is able to support defence capability.	Measure: The intent of the Defence Industry Statement 2016 is met. Target: The Centre for Defence Industry Capability and the Defence Innovation Hub operate in accordance with the Defence Industry Statement 2016.	Ongoing

Capability

The First Principles Review: Creating One Defence, found that Defence's existing organisational model and processes were complicated, slow and inefficient. Implementation of the recommendations of the Review will make changes to accountabilities, structures, systems and processes to build organisational capability.

Defence's corporate and military enabling functions are essential to the effective and efficient delivery of capability⁶ and to support operations. The enabling functions range from supporting the Australian Defence Force in the conduct of operations through information and communication technology services and logistics and health support, to building and remediating the Defence estate. Over the life of this plan, the priority is to continue to develop a service delivery system as set out in the First Principles Review. This will involve standardising services, removing duplication of functions, professionalising the workforce and ensuring there are single, clear lines of ownership and accountability.

Workforce

An integrated Australian Defence Force and Australian Public Service workforce is the foundation for delivering the organisational capability envisaged in the First Principles Review. It is also necessary to ensure Defence is fit for purpose and able to deliver its long-term strategy as outlined in the 2016 Defence White Paper. Defence needs Australian Defence Force personnel and Australian Public Servants who have the right attitude, the right skills, and are in the right roles to achieve the Defence mission.

A key focus for 2016-17 is the development of a 10-year Strategic Workforce Plan that will set out the skills Defence needs and detail how Defence will attract, retain and develop its people. The Strategic Workforce Plan will provide workforce priorities, practical initiatives and resources for attracting, growing and retaining the people Defence needs.

Integrated Investment Program

Defence has one of the largest capital investment programs in the Australian Government, consisting primarily of acquisition, sustainment and support of Defence materiel.

Through implementation of the First Principles Review, we will undertake regular reviews of the capital program in consultation with the Minister for Defence and central agencies. The Integrated Investment Program includes all capital and related investments (such as materiel, estate and facilities, workforce, and information and communications technology). The Integrated Investment Program will be supported by a contestability function to ensure that acquisitions are aligned with strategy and resources.

Information Management

Information management is a critical enabler for Defence. In the military environment, information management must provide the war fighter with common battlespace awareness and information superiority through integrated and interoperable information. It underpins the next generation of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, and links sensors and weapons platforms. It is crucial to offset the relatively small size of the Australian Defence Force and enable a competitive war fighting advantage over Australia's adversaries.

In this context capability refers to the power to achieve a desired operational effect in a nominated environment within a specified time and to sustain that effect for a designated period. In a military context, capability is achieved by developing a force structure appropriately prepared for a range of military operations. Australian Defence Doctrine Publication 00.2, 'Executive Series: Preparedness and Mobilisation', 2013.

Information management must enable the organisation to make informed decisions, measure performance, provide timely, credible, traceable and relevant management information, and support enterprise-wide business processes. It must be underpinned by a trusted single source of enterprise-wide data, and to the extent possible, common and standardised applications and infrastructure.

Defence is undertaking a large-scale transformation program that will deliver a secure, integrated and easier to manage information and communication technology environment, and support improved information management. This will improve collaboration and productivity to support the integration of future technologies, and ensure the longevity of Defence information and communication technology capability.

Risk Oversight and Management

Risk management is undertaken in accordance with an overarching Defence Risk Management Framework which provides:

- 1. Transparency of risk management within the business units of Defence;
- 2. A structure to draw out accountabilities and responsibilities of shared risk of the business units across the Department; and
- 3. A collective frame that articulates accountabilities and responsibilities for risk shared with Commonwealth, industry and international partners.

Through this framework, Defence addresses risks at three levels:

- **Operating risks** These are risks to Defence achieving efficient and effective operating intent. They are the inward focus of how Defence undertakes the activities in this Plan.
- Enterprise-level risks These are events which may limit or compromise Defence's collective ability to meet the obligations and requirements set by Government. These risks may arise from four 'enterprise vulnerabilities', which are: integration across Defence; integration with key external partners; compliance with legislation and Government policy; and efficient and effective use of resources.
- National security risks These are risks managed as shared risks with Commonwealth, international and
 industry partners. Understanding of the national security risk environment informs the risk tolerance for enterprise
 risks.

The Secretary and Chief of the Defence Force have set out their minimum expectations for risk management in Defence in the *Joint Directive on the Management of Risk in Defence*.

Defence senior management exercises high-level oversight and assurance of risk. A Defence enterprise risk profile report providing a picture of the performance of enterprise-level risks is produced annually for senior committees. The Defence Audit and Risk Committee provides the Secretary and Chief of the Defence Force with independent advice on all aspects of Defence Governance including implications arising from Australian National Audit Office audits and Joint Committee of Public Accounts and Audit reports.

The management and oversight of risk across Defence will continue to evolve as a key component within the planning, performance and governance functions.



Defending Australia and its National Interests www.defence.gov.au



2017-2018

Defence Corporate Plan



Statement of Preparation

I, as the accountable authority of Defence, present the 2017–18 Defence Corporate Plan, which covers the periods of 2017–21, as required under paragraph 35(1)(b) of the Public Governance, Performance and Accountablity Act 2013.

Brendan Sargeant

Acting Secretary of Defence

7 June 2017

© Commonwealth of Australia 2017

ISSN 2205-5282 (online)

ISBN 978-0-6480977-0-9

This publication is available for your use under a <u>Creative Commons BY Attribution 3.0 Australia</u> licence, with the exception of the Commonwealth Coat of Arms and the Department of Defence logo, signatures and where otherwise stated. The full licence terms are available from http://creativecommons.org/licenses/by/3.0/au/legalcode.



Use of the Department of Defence's material under a <u>Creative Commons BY Attribution 3.0 Australia</u> licence requires you to attribute the work (but not in any way that suggests that the Department of Defence endorses you or your use of the work).

Department of Defence material used 'as supplied'.

Provided you have not modified or transformed the Department of Defence material in any way including, for example, by changing the Department of Defence text, the Department of Defence prefers the following attribution:

Source: The Australian Government Department of Defence.

Derivative material

If you have modified or transformed the Department of Defence's material, or derived new material from those of the Department of Defence in any way, then the Department of Defence prefers the following attribution:

Based on the Australian Government Department of Defence's data.

Contents

INTRODUCTION	2
PURPOSES	3
ENVIRONMENT	4
RISK OVERSIGHT AND MANAGEMENT	10
PLANNED PERFORMANCE	11

Introduction

The 2017–18 Defence Corporate Plan sets out Defence's role, objectives and functions, referred to as Purposes in the PGPA Act,¹ and describes how we will measure our performance in achieving our Purposes. Performance against the Corporate Plan will be reported through annual performance statements, to be included in the Defence Annual Report for 2017–18. The Corporate Plan is a living document and will be updated at least annually to reflect changes in our operating environment and to meet the requirements of the PGPA Act.

The Defence Corporate Plan focuses on the two outcomes we deliver to Government:²

- Defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction; and
- Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by Government.

We undertake activities to deliver an effective defence capability³ for Government. Over the life of this plan, we will continue to build capability to support our national security interests and promote them in a region that is growing more complex and dynamic, as described in the 2016 Defence White Paper.

In 2017–18 we will continue implementation of the new force structure and capabilities identified in the White Paper. These changes are essential as we transform Defence into an organisation that delivers on our primary role: to protect and advance Australia's strategic interests through the provision of military capabilities, the promotion of security and stability, and the provision of support for the Australian community and civilian authorities as directed by Government.

In delivering this capability to Government, Defence will work to embed the significant organisational change that resulted from the First Principles Review, *Creating One Defence*, while continuing to deliver cultural reform, building on our *Pathway to Change* program. These changes are aimed at building our organisational capability and culture so that we can achieve our Purposes both now and into the future.

We are pleased to present the 2017–18 Defence Corporate Plan.

Brendan Sargeant

Acting Secretary of Defence

7 June 2017

Mark Binskin AC

Air Chief Marshal
Chief of the Defence Force

14 June 2017

¹ Purposes are defined by Part 1, Division 2—8 of the *Public Governance, Performance and Accountability Act 2013* as 'the objectives, functions or role' of an entity.

² The Defence Outcomes are published in the Portfolio Budget Statements.

Defence Capability is the power to achieve a desired operational effect in a nominated environment within a specified time and to sustain that effect for a designated period. In a military context, capability is achieved by developing a force structure appropriately prepared for a range of military operations. Australian Defence Doctrine Publication 00.2, 'Executive Series: Preparedness and Mobilisation', 2013.

Purposes

The Defence mission is to defend Australia and its national interests.

Defence's primary role is to protect and advance Australia's strategic interests through the promotion of security and stability, the provision of military capabilities to defend Australia and its national interests, and the provision of support for the Australian community and civilian authorities as directed by Government. In fulfilling this mission, Defence has two Purposes:

1. Defend Australia and its national interests

2. Protect and advance Australia's strategic interests.

Programs contribute to the achievement of the Defence Purposes and Defence Outcomes, as shown in Table 1. NB: Budget programs have been renumbered for 2017–18.

Purpose	Outcome Statement	Budg	et Program
Purpose 1: Defend Australia and its national	Outcome 1: Defend Australia and its national	1.1	Operations Contributing to the Safety of the Immediate Neighbourhood
interests	interests through the	1.2	Operations Supporting Wider Interests
	conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction.	1.3	Defence Contribution to National Support Tasks in Australia
Purpose 2: Protect	Outcome 2: We protect	Depa	rtmental
and advance Australia's	and advance Australia's	2.1	Strategic Policy & Intelligence
strategic interests	strategic interests through the provision of strategic	2.2	Defence Executive Support
	policy, the development,	2.3	Chief Finance Officer
	delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by	2.4	Vice Chief of the Defence Force
		2.5	Navy Capabilities
		2.6	Army Capabilities
		2.7	Air Force Capabilities
	Government.	2.8	Joint Operations Command
		2.9	Capability Acquisition and Sustainment
		2.10	Estate and Infrastructure
		2.11	Chief Information Officer
		2.12	Defence People
		2.13	Defence Science and Technology
		Admi	nistered
		2.14	Defence Force Superannuation Benefits
		2.15	Defence Force Superannuation Nominal Interest
		2.16	Housing Assistance
		2.17	Other Administered

Table 1. Portfolio Budget Statement programs mapped to Defence Purposes and Outcomes for 2017–18.

Environment

Strategic Risk

The Government's Defence policy, articulated in the 2016 Defence White Paper, is to align Australia's defence strategy with capabilities and resourcing, grow our international defence partnerships and invest in the Defence–industry partnership to develop and deliver innovative, cutting-edge capabilities. Inherent in this policy is a greater focus on seizing opportunities while managing strategic risks. This will be achieved through developing Defence's ability to take a more active role in shaping regional affairs and to respond to developments that threaten our interests. Our alliance with the United States will be strengthened as will our partnerships with other countries. This is designed to ensure the Australian Defence Force is better prepared to respond to complex emerging strategic risks by providing Government with greater options and flexibility.

Emerging challenges are increasing strategic risk and uncertainty. As identified in the 2016 Defence White Paper:

We can expect greater uncertainty in Australia's strategic environment over the next two decades as a consequence of: the changes in the distribution of power in the Indo-Pacific and globally; the continuing threat of terrorism from groups like Daesh and from foreign terrorist fighters; the modernisation of regional military capabilities; the introduction of new military technologies such as cyber systems; and the proliferation of weapons of mass destruction and ballistic missile technology.⁴

The White Paper sets out a new strategic framework within which all Defence activities are undertaken. This framework identified three Strategic Defence Interests linked to three equally weighted Strategic Defence Objectives:

1. A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication.

The **Strategic Defence Objective** for this interest is: Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches. This objective relates to Defence Purpose 1.

2. A secure nearer region, encompassing maritime South East Asia and South Pacific (comprising Papua New Guinea, Timor–Leste and Pacific Island Countries).

The **Strategic Defence Objective** for this interest is: Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor–Leste and of Pacific Island Countries to build and strengthen their security. This objective relates to Defence Purpose 2.

3. A stable Indo-Pacific region and a rules-based global order.

The **Strategic Defence Objective** for this interest is: Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order. This objective relates to Defence Purpose 2.

Defence undertakes a number of programs designed to achieve these objectives and manage strategic risk. The major activities to be undertaken in 2017–18 are outlined in the section on Performance.

4 2016 Defence White Paper, p.32.

Enterprise Challenges

The First Principles Review and the 2016 Defence White Paper both identified that Defence has a number of significant challenges we must overcome to develop the organisational capability we require to meet Government expectations. In addition to internal challenges, Commonwealth legislation and policy require Defence to develop the capacity to meet specific whole-of-Government requirements.

For example, the Australian National Action Plan on Women, Peace and Security 2012–2018 is a whole-of-Government policy to implement the United Nations Security Council Resolution 1325 (UNSCR 1325) and other United Nations (UN) Security Council resolutions related to Women, Peace and Security. The Women, Peace and Security agenda is central to Defence's operational effectiveness and is an essential component of future planning and conduct of operations.

Defence has the most extensive land and property holdings in Australia, including large training areas and bases close to the coastline. Recognising the challenges posed by climate change, Defence is undertaking studies to determine the level of risk and implementing mitigation strategies to reduce the impact to bases and training areas.⁵

The Government's Public Management Reform Agenda—as expressed through the PGPA Act and related legislation and policy—requires all entities to take a deliberate approach to corporate planning and performance management, supported by a stronger risk management framework that aligns to the Commonwealth Risk Management Policy 2014. Improved corporate risk management, business planning and performance management will enable Defence to focus all activities on achieving Government-directed outcomes.

The Government's First Principles Review, *Creating One Defence*, required Defence become a more integrated organisation, with clear accountabilities and streamlined decision-making processes. Implementation of the recommendations of the First Principles Review was designed to ensure that Defence has the organisational capability it needs to deliver the 2016 Defence White Paper and to respond to a wide range of operational requirements both now and into the future.

The First Principles Review identified the Defence workforce as one of the most critical contributors to the delivery of the full range of capability expected by Government. The Defence Strategic Workforce Plan was delivered in 2016 and is designed to set the framework for the management of the current and future workforce. Implementation of the plan will continue in 2017–18, with workforce challenges to be monitored and actively managed through the stewardship of the Enterprise Business Committee and the Defence Committee.

National climate resilience and adaptation strategy p. 31 http://www.environment.gov.au/system/files/resources/3b44e21e2a78-4809-87c7-a1386e350c29/files/national-climate-resilience-and-adaptation-strategy.pdf

Enterprise Risks

Risks to the achievement of the Defence mission are managed by risk stewards in accordance with the Defence Risk Management Framework, which is described in the Risk Oversight and Management section.

Defence has identified four enterprise risks, which are classified. Management of these risks is overseen by the Enterprise Business Committee, with significant issues escalated internally for Defence Committee consideration. The risks are reviewed and updated at least annually, or when there are changes in Defence's operating environment.

Implementation of the First Principles Review, *Creating One Defence*, required changes to be made to the accountabilities, structures, systems and processes required to build and manage the required organisational capability. It also introduced the One Defence Business Model, which focuses Defence's organisational capability on achieving Government-directed outcomes. The business model has three key features:

- 1. A stronger strategic centre able to provide clear direction, contestability of decision making as well as enhanced control of resources and monitoring of organisational performance.
- 2. An end-to-end approach for capability development. Capability Managers will be assigned clear authority and accountability for the delivery of capability outcomes to schedule and budget, supported by an integrated capability delivery function and subject to stronger direction setting and contestability from the centre.
- 3. Enablers that are integrated and customer-centric with greater use of cross-functional processes, particularly in regional locations.

Direction Setting

We have strengthened our strategic management capability to set direction for the organisation, monitor and manage the performance of Defence, and provide assurance to Government that Government-directed outcomes are being delivered effectively and efficiently. In 2017–18 the Defence Strategy Framework and Enterprise Performance Management Framework will be implemented, supporting the role of the Defence 'strategic centre' in setting direction for the organisation and in ensuring advice provided to Government has been contested rigorously.

Defence Capability

Defence has one of the largest capital investment programs in the Commonwealth, consisting primarily of acquisition, sustainment and support of Defence materiel. Introduced at the same time as the 2016 Defence White Paper, the Integrated Investment Program includes all capital and related investments (such as materiel, estate and facilities, workforce and information and communications technology).

The Integrated Investment Program is supported by a contestability function that informs the development of the risk assessment and decision support framework to ensure that acquisitions are aligned with strategy and resources. Upgrading Australian Defence Force bases and logistics systems, including fuel and explosive ordnance facilities in accordance with 2016 Defence White Paper requirements, remains a priority.

Enablers (internal service delivery)

The First Principles Review identified that organisational capability is derived from a strong work force enabled by modern and effective security services, facilities and estate, information management and information and communications technology, people management systems, legal services, and health and logistics, supported by an integrated service delivery system. A service delivery system was developed as part of First Principles Review implementation. The focus for the system in 2017–18 involves standardising services, removing duplication of functions, professionalising the workforce and ensuring there are single, clear lines of ownership and accountability.

Security

We will continue to develop and mature our principles-based approach to security. Remediation of the processes and practices of the Australian Government Security Vetting Agency (AGSVA) will continue in 2017–18, with a focus on the positive vetting remediation program, which is addressing a backlog of clearances to achieve benchmark timeframes.

Facilities and Estate

In 2017–18, we will implement the Defence Estate Strategy 2016–2036 and plan and continue our work in developing future estate profile options on what parts of the estate can be optimised through future acquisitions and expansions, and the parts that could be rationalised through disposal. Delivery of an estate strategy, plan and profile are key steps in ensuring that Defence's estate footprint aligns with current and future force needs.

Information Management

Information management is a critical enabler for Defence. In the military environment, information management must provide the war fighter with common battlespace awareness and information superiority through integrated and interoperable information. It underpins the next generation of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, and links sensors and weapons platforms. It is crucial to offset the relatively small size of the Australian Defence Force and enable a competitive war fighting advantage over Australia's adversaries.

Defence is undertaking a large-scale transformation program that will deliver a secure, integrated and easier to manage information and communication technology environment and support improved information management. This will improve collaboration and productivity to support the integration of future technologies, and ensure the longevity of Defence information and communication technology capability.

Workforce

An integrated Australian Defence Force and Australian Public Service workforce is the foundation for delivering the organisational capability envisaged in the First Principles Review. It is also necessary to ensure Defence is fit for purpose and able to deliver its long-term strategy as described in the 2016 Defence White Paper. To achieve its mission, Defence needs Australian Defence Force personnel and Australian Public Servants who have the right attitude, the right skills, and are in the right roles. The Defence workforce also extends to integrated service providers and Defence industry, which provide critical services that contribute to Defence being able to meet Government policy expectations.

A key focus for 2017–18 is the implementation of the 10-year Defence Strategic Workforce Plan that sets out the skills Defence needs and details how Defence will attract, retain and develop its people. The Strategic Workforce Plan provides workforce priorities, initiatives and resources for attracting, growing and retaining the people Defence needs.

Defence will continue cultural reform through implementation of the *Pathway to Change* strategy. This will be with a planned and professional workforce built on a foundation of strengthened accountability and an inclusive and diverse culture to meet the direction of the First Principles Review and capabilities required under the 2016 Defence White Paper.

Defence is creating a more diverse and inclusive culture, which will assist Defence to access the broadest available talent in Australia and harness the capability benefit and improved decision making that a diverse workforce generates, and to achieve its cultural reform efforts. The Defence Diversity and Inclusion Strategy 2012–2017 identifies the five strategic goals that underpin successful diversity and inclusion in Defence and identifies Defence's diversity priorities:

- women
- Indigenous Australians
- people with disability
- people from culturally and linguistically diverse backgrounds
- lesbian, gay, bisexual, transgender and intersex people.

Five strategic goals underpin successful diversity and inclusion in Defence:

- 1. Defence is a flexible, adaptable and agile organisation that is able to accommodate the diverse needs of people as they move through various life and career stages.
- 2. Defence utilises creative, targeted human resource solutions to achieve the numerous strategic capability benefits that diversity brings to all levels of the organisation.
- 3. Defence recognises and understands that true inclusiveness does not mean treating everyone exactly the same way, all the time.
- 4. Defence is viewed by all as an organisation committed to diversity and inclusion.
- 5. Defence has strategies in place to support the employment of identified diverse groups that require immediate priority attention.

In 2017–18, Defence will continue to implement programs and initiatives that harness the diverse knowledge, skills and attributes of its people. Through diversity, Defence gains the varied perspectives needed to deal with complex problems and develop innovative solutions.

Legal

The portfolio administers a number of Acts and regulations that contain small entities, including a number of statutory offices, trusts and companies that are regulated by the provisions outlined in the PGPA Act. These entities are independent bodies; however, the stakeholder management and administration of these bodies reside within Defence. These include, among others, Defence Housing Australia, the Australian Strategic Policy Institute and a number of Services trust funds and canteen services.

The Defence portfolio also contains the Department of Veterans' Affairs, together with its associated bodies, as it is designated as part of the Defence portfolio in the Administrative Arrangements Order. The Department of Veterans' Affairs is administered separately to Defence and performance information related to the department may be found in the Department of Veterans' Affairs corporate plan.

Health, Logistics, Education and Training

In 2017–18, the focus will remain on delivering health, welfare and family support services to meet the requirements of the Australian Defence Force. Defence will also continue to work with the Department of Veterans' Affairs to enhance the transition process for Members and veterans. Other people priorities in 2017–18 include implementing the new ADF Total Workforce model to provide greater flexible working arrangements for ADF Members and further developing a comprehensive program of professionalisation and development to support careers in the Australian Defence Force and the Australian Public Service.

Control and Governance

The way Defence is managed will be described in a Defence Business Framework, which will be implemented in 2017–18. The business framework will not only describe how the One Defence Business Model operates, but will set out the high-level processes and standards to be used and achieved in supporting the Secretary in discharging governance and performance accountabilities, as set out in the PGPA Act.

In 2017–18 Defence will continue to mature its control functions—financial management, internal audit, inspectors-general and judge advocate—so that they can provide assurance to the Defence senior committees—the Defence Committee, the Enterprise Business Committee and the Investment Committee—that Government-directed outcomes are being delivered in accordance with legislative and policy requirements.

Effective financial management enables Defence to ensure Government-allocated resources are being used to deliver Government-directed outcomes. Both the First Principles Review and the 2016 Defence White Paper highlighted the importance of keeping in balance strategy, capability and resources. The Chief Finance Officer will work closely with the Associate Secretary in 2017–18 to ensure that enterprise financial management and corporate planning and performance management are aligned so as to support the work of the Defence senior leadership in maintaining this balance, as directed by Government.

In accordance with the PGPA Act and in support of the Commonwealth Fraud Control Framework, Defence has instituted Defence Fraud Control Plan No. 11, which describes the fraud control framework our organisation has implemented to prevent, detect and respond to fraud. A focus for 2017–18 will be to develop our capacity to identify and manage enterprise-wide vulnerabilities and risk factors within a diverse operating environment.

In 2017–18 we will finalise implementation of the Defence Legislative Compliance Framework, which is a central component of Defence's internal system of controls. The framework assigns accountability to a single senior leader for the management and oversight of Defence compliance with Commonwealth and selected state legislative requirements relevant to Defence business.

Risk Oversight and Management

Risk management is governed by the Commonwealth Risk Management Policy 2014 and is undertaken in accordance with an overarching Defence Risk Management Framework which provides:

- 1. Transparency of risk management within the business units of Defence;
- 2. A structure to draw out accountabilities and responsibilities of shared risk of the business units across the Department; and
- 3. A collective frame that articulates accountabilities and responsibilities for risk shared with Commonwealth, industry and international partners.

Through this framework, Defence addresses risks at three levels:

- **Strategic risks**—These risks are described in the 2016 Defence White Paper and are managed as shared risks with Commonwealth, international and industry partners. Understanding of the national security risk environment informs the risk context for enterprise-level risks.
- Enterprise-level risks—These are events which may limit or compromise Defence's collective ability to meet the obligations and requirements set by Government. These risks may arise from four 'enterprise vulnerabilities', which are: integration across Defence; integration with key external partners; compliance with legislation and Government policy; and efficient, effective, economical and ethical use of resources.
- **Operating risks**—These are risks to Defence achieving efficient and effective operating intent. They are the inward focus of how Defence undertakes the activities in support of this Plan.

The Secretary and Chief of the Defence Force have set out their minimum expectations for risk management in Defence in a *Joint Directive on the Management of Risk in Defence*.

Defence senior management exercises high-level oversight and provides assurance of risk to Government. A Defence enterprise risk assessment is produced for senior committees to support their collective management. The Defence Audit and Risk Committee provides the Secretary and the Chief of the Defence Force with independent advice on all aspects of Defence governance including implications arising from Australian National Audit Office audits and Joint Committee of Public Accounts and Audit reports.

The management and oversight of risk across Defence will continue to evolve as a key component within the enterprise governance and organisational performance functions.

Planned Performance

Purpose 1. Defend Australia and its national interests

We defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction.

We plan for, develop and maintain the capability to deter and defeat armed attacks on Australia or on Australian interests. This includes planning for, conducting, controlling and evaluating Defence and/or coalition contributions to Government-directed operations.

Defence also supports the Commonwealth and State/Territory Governments with emergency and non-emergency tasks, as well as supporting events of national significance as requested by the Australian Government.

Defence performance in achieving Purpose 1 in 2017–18 will be measured using the criteria described in Table 2.

Performance measures

1.i. Required preparedness levels are achieved. 2017–2021			
Measured and reported Measured bi-annually. Reported annually.			
Methodology	Assessment of preparedness against the Chief of the Defence Force Preparedness Directive.		
1.ii. Operational outcomes me	eet the requirements of Government policy.	2017–2021	
Measured and reported Measured bi-annually. Reported annually.			
Methodology Assessment of operational deployments against operational outcomes agreed with Government.			
1.iii. State/Territory and inter-agency cooperation enables Defence to contribute effectively to whole-of-Government outcomes, in accordance with Government direction. 2017–2021			
Measured and reported Measured bi-annually. Reported annually.			
Methodology Assessment of inter-agency engagement against whole-of-Government outcome agreed with Government.		nment outcomes	

Table 2: Purpose 1 performance measures.

Key Activities

The key activities Defence will undertake in 2017–18 to achieve Purpose 1 and to control relevant strategic and enterprise-level risk are described in Table 3.

Activity	Intended result	Performance Criteria	2017-18	2018-19	2019-20	2020-21
Ensure Defence's operational capabilities are available to meet Government direction. Lead PBS program: 2.4 Vice Chief of the Defence Force	Government is able to deploy Defence capability to support Government policy objectives.	Measure: Chief of the Defence Force preparedness levels meet Government requirements. Target: Chief of the Defence Force preparedness levels are achieved as agreed with Government.	✓	✓	✓	✓
Deliver intelligence services. Lead PBS program: 2.1 Strategic Policy & Intelligence	Defence intelligence services enable efficient operations across national security agencies.	Measure: Defence intelligence outputs align with Government intelligence priorities. Target: Whole-of-Government and Australian Defence Force intelligence requirements are met.	√	✓	✓	✓
Conduct joint, combined and inter-agency operations as directed by Government. Lead PBS program: 2.8 Joint Operations Command	Joint forces are able to be deployed and sustained efficiently and effectively, and in accordance with Government timeframes.	Measure: Operational outcomes meet the requirements of Government policy. Target: All operational requirements are met.	✓	√	√	√
Manage the Defence estate in accordance with Government direction and community expectations Lead PBS program: 2.10 Estate & Infrastructure	The generation and sustainment of the Australian Defence Force are enabled by a fit-for-purpose estate.	Measure: The estate meets the requirements of the Capability Managers. Target: The Defence Estate Strategy implementation plan is delivered as agreed.	✓	✓	✓	✓

Table 3: Purpose 1 key activities.

¹² 58

Purpose 2. Protect and advance Australia's strategic interests

We protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by Government.

Defence must provide high-quality, coherent and timely advice to Government on Defence strategy, capability and resourcing. Defence has implemented the 'strategic centre' model to ensure that all advice provided to Government is rigorously contested for alignment with Government strategic direction and to ensure the options being presented to Government support achievement of its Defence strategy, as described in the 2016 Defence White Paper.

The Government expects Defence to play an active role in contributing to regional security and stability, and to contribute to coalition operations around the world where our interests are engaged. Delivering on these requirements will require Australia to build on its strong network of bilateral and multilateral relationships. Through regular dialogue and practical cooperation, Defence is strengthening its engagement with partners to support shared responses to shared challenges.

Capability delivery is a core business process that enables Defence to perform its mission of defending Australia and its national interests now and into the future. Defence must procure capability efficiently and effectively. In 2017–18, Defence will continue building the new levels of capability required by Government and described in the 2016 Defence White Paper and the Integrated Investment Program. Major investments will enhance Australian Defence Force capability to conduct operations to deter and defeat threats to Australia, operate over longer distances to conduct independent combat operations in our region, and make more effective contributions to international coalitions.

Australia's defence industry is a major partner in the Government's plans for current and future Defence capabilities. It is vital that Australia maintains a science and technology base and defence industry capable of supporting Defence's acquisition and sustainment requirements during peacetime and operations. A highly skilled and capable Australian defence industry is necessary for Defence to achieve its strategic objectives and deliver large-scale, complex projects and sustain military capability. Defence will work with industry to reflect a shared policy agenda that supports the growth and competitiveness of Australian businesses.

Defence performance in achieving Purpose 2 in 2017–18 will be measured using the criteria described in Table 4.

Performance measures

2.i. Government has confidence in the relevance and quality of Defence advice. 2017–2021			
Measured and reported Measured bi-annually. Reported annually.			
Methodology	Methodology Bi-annual survey of the relevant Ministers and the central agencies.		
2.ii. Government is assured to	Government is assured that Defence advice has been appropriately contested. 2017–2021		
Measured and reported	Measured and reported Measured bi-annually. Reported annually.		
Methodology	Methodology Bi-annual survey of the relevant Ministers and the central agencies.		
2.iii. The capability delivery process maintains the integrity of the Integrated Investment Program and delivers the required capability for the force-in-being. 2017–2021			
Measured and reported	leasured and reported Measured bi-annually. Reported annually.		
Methodology	ethodology Assessment of delivery against the Integrated Investment Program.		
2.iv. Defence capability is sustained consistent with Government requirements. 2017–2021			
Measured and reported	Measured and reported Measured bi-annually. Reported annually.		
Methodology	Sustainment meets capability manager requirements.		

³ 59

Performance measures continued

2.v.	International and inter-agency cooperation enables Defence to shape the international security environment, in accordance with Government direction. 2017–2021			
Meas	Measured and reported Measured bi-annually. Reported annually.			
Meth	Methodology Assessment of delivery against the Defence International Engagement Strate			
2.vi.	i. The Integrated Investment Program is managed effectively and comprises all investment and sustainment inputs, incorporating the Fundamental Inputs to Capability. 2017–2021			
Meas	Measured and reported Measured bi-annually. Reported annually.			
Meth	odology	 Regular independent assurance of the Defence capability development process by the Defence Audit and Risk Committee. Regular reviews of the Integrated Investment Program in consultation with the Minister and central agencies. 		
2.vii.	2.vii. Emerging science and technology is used to support development of best value capability. 2017–202			
Meas	sured and reported	Measured bi-annually. Reported annually.		
Meth	odology	Regular assessment of how Defence's strategic research builds understanding of future Defence capability.		
2.viii.	2.viii. Defence capability development leverages industry to promote innovation. 2017–2021			
Meas	asured and reported Measured bi-annually. Reported annually.			
Meth	odology	Regular assessment of the value of Defence engagement with industry.		

Table 4: Purpose 2 performance measures.

Key Activities

The key activities Defence will undertake in 2017–18 to achieve Purpose 2 and to control relevant strategic and enterprise-level risk are described in Table 5.

Activity	Intended result	Performance Criteria	2017-18	2018-19	2019-20	2020-21
Defence provides clear, accurate and timely policy advice to Government. Lead PBS program: 2.1 Strategic Policy & Intelligence	The Minister receives policy advice that supports effective decision-making.	Measure: Government has confidence in the relevance and quality of Defence policy advice. Target: Minister expresses high to very high confidence in Defence advice.	✓	✓	✓	✓
Defence ensures that the policy development process incorporates inputs from relevant stakeholders through processes that include contestability. Lead PBS program: 2.1 Strategic Policy & Intelligence	Defence strengthens its engagement on policy development with other national security participants and other relevant parties.	Measure: Proposals presented to Government for decision incorporate all relevant considerations. Target: Stakeholders express high confidence in Defence engagement.	✓	✓	✓	✓

Key Activities continued

Activity	Intended result	Performance Criteria	2017-18	2018-19	2019-20	2020-21
Use data and information to support risk-informed decision-making by Defence's senior leaders. Lead PBS program: 2.2 Defence Executive Support	An appropriate risk appetite is actively exercised based on all available information. Assured data is available to support the design of good performance measures. Managers across Defence have a view of organisational performance within their work area which is based on true information, enabling them to make effective and robust decisions.	Measure: Performance information uses validated information to support decision-making. Target: All performance information is supported by a reliable and validated data source.	√	✓	√	√
Deliver health and welfare services to meet the requirements of the Australian Defence Force. Lead PBS program: 2.4 Vice Chief of the Defence Force	Effective and efficient health support and welfare services are provided.	Measure: Quality of health and welfare services delivered to Australian Defence Force members and families. Target: Delivery meets agreed standards.	✓	✓	✓	✓
Achieve Government's strategic policy requirements as set out in the 2016 Defence White Paper. Lead PBS program: 2.1 Strategic Policy & Intelligence	Defence implements policy direction to meet Government's requirements now and into the future.	Measure: Effective implementation of the 2016 Defence White Paper. Target: The 2016 Defence White Paper implementation plan activities for 2017–21 are delivered as agreed with Government.	✓	√	√	√
Deliver the capability required by the 2016 Defence White Paper. Lead PBS program: 2.4 Vice Chief of the Defence Force	Defence develops the capability it needs to meet Government's requirements now and into the future.	Measure: Effective implementation of the Integrated Investment Program. Target: The Integrated Investment Program is delivered as agreed with Government.	✓	✓	√	√
Engage with industry through the Centre for Defence Industry Capability and the Defence Innovation Hub to enhance and sustain Defence capability. Lead PBS program: 2.1 Strategic Policy & Intelligence	A competitive Australian industrial base is able to support Defence capability.	Measure: The intent of the Defence Industry Policy Statement is met. Target: The Centre for Defence Industry Capability and the Defence Innovation Hub operate in accordance with the Defence Industry Policy Statement.	√	√	√	✓

Table 5: Purpose 2 key activities

¹⁵ 61



Defending Australia and its National Interests www.defence.gov.au



2018-19 Defence Corporate Plan





STATEMENT OF PREPARATION

I, as the accountable authority of Defence, present the 2018–19 Defence Corporate Plan, which covers the periods of 2018–22, as required under paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

Greg Moriarty

Secretary of Defence 28 June 2018

© Commonwealth of Australia 2018

ISSN 2205-5282 (online)

ISBN 978-0-6480977-8-5

This publication is available for your use under a <u>Creative Commons BY Attribution 3.0 Australia</u> licence, with the exception of the Commonwealth Coat of Arms and the Department of Defence logo, signatures and where otherwise stated. The full licence terms are available from http://creativecommons.org/licenses/by/3.0/au/legalcode.



Use of the Department of Defence's material under a <u>Creative Commons BY Attribution 3.0 Australia</u> licence requires you to attribute the work (but not in any way that suggests that the Department of Defence endorses you or your use of the work).

Department of Defence material used 'as supplied'

Provided you have not modified or transformed the Department of Defence material in any way including, for example, by changing the Department of Defence text, the Department of Defence prefers the following attribution:

Source: The Australian Government Department of Defence

Derivative material

If you have modified or transformed the Department of Defence's material, or derived new material from those of the Department of Defence in any way, then the Department of Defence prefers the following attribution:

Based on the Australian Government Department of Defence's data.

Contents

Introduction	2
Purposes	3
Environment	6
Defence Capability	9
Risk Oversight and Management	12
Planned Performance	14

Introduction

The 2018–19 Defence Corporate Plan sets out Defence's role, objectives and functions, referred to as Purposes in the Public Governance, Performance and Accountability Act 2013¹ (PGPA Act), and describes how we will measure our performance in achieving our Purposes. Performance against the Corporate Plan will be reported through annual performance statements, to be included in the Defence Annual Report for 2018–19. The Corporate Plan is a living document and will be updated at least annually to reflect changes in our operating environment and to meet the requirements of the PGPA Act.

The Australian Defence Force (ADF) is constituted under the *Defence Act 1903*. Its mission is to defend Australia and its national interests. In fulfilling this mission, Defence serves the Government of the day and is accountable to the Commonwealth Parliament which represents the Australian people to efficiently and effectively carry out the Government's defence policy.

The Defence Corporate Plan focuses on the two outcomes we deliver for Government2:

- Defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction; and
- Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by Government.

In 2018–19, we will continue to build a single integrated Defence organisation working towards a common goal, whilst embedding change and driving reform in Defence.

We will undertake activities to deliver an effective defence capability³ for Government. Over the life of this plan, we will build capability to support our national security interests and promote them in our complex and challenging security environment. In delivering this capability for Government, Defence will work to mature significant organisational change that resulted from the First Principles Review, *Creating One Defence*, while continuing to deliver cultural reform, through our *Pathway to Change* program.

This reform aims to build our organisational capability and culture that enables achievement of our Purposes both now and into the future.

We are pleased to present the 2018–19 Defence Corporate Plan.

Greg Moriarty

Secretary of Defence

28 June 2018

Mark Binskin AC

Air Chief Marshal Chief of the Defence Force

28 June 2018

Purposes are defined by Part 1, Division 2–8 of the Public Governance, Performance and Accountability Act 2013 as 'the objectives, functions or role' of an entity.

The Defence Outcomes are published in the Portfolio Budget Statements.

Defence Capability is the power to achieve a desired operational effect in a nominated environment within a specified time and to sustain that effect for a designated period. In a military context, capability is achieved by developing a force structure appropriately prepared for a range of military operations. Australian Defence Doctrine Publication 00.2, 'Executive Series: Preparedness and Mobilisation', 2013.

Purposes

The Defence mission is to defend Australia and its national interests.

Defence's primary role is to protect and advance Australia's strategic interests through the promotion of security and stability, the provision of military capabilities to defend Australia and its national interests, and the provision of support for the Australian community and civilian authorities as directed by Government.

Programs that contribute to the achievement of the Defence Purposes and Defence Outcomes are shown in Table 1.

Purpose	Outcome Statement	Budget Program			
Purpose 1: Defend Australia and its	Outcome 1: Defend Australia and its national interests through the conduct	1.1 Operations Contributing to the Safety of the Immediate Neighbourhood			
national interests	of operations and provision of support for the Australian community and	1.2 Operations Supporting Wider Interests			
	civilian authorities in accordance with Government direction.	1.3 Defence Contribution to National Support Tasks in Australia			
Purpose 2: Protect	Outcome 2: Protect and advance	Departmental			
and advance Australia's strategic	Australia's strategic interests through the provision of strategic policy,	2.1 Strategic Policy and Intelligence			
interests	the development, delivery and	2.2 Defence Executive Support			
	sustainment of military, intelligence and enabling capabilities, and the	2.3 Chief Finance Officer			
	promotion of regional and global security and stability as directed by Government.	2.4 Joint Capabilities			
		2.5 Navy Capabilities			
		2.6 Army Capabilities			
		2.7 Air Force Capabilities			
		2.8 ADF Headquarters			
		2.9 Capability Acquisition and Sustainment			
		2.10 Estate and Infrastructure			
		2.11 Chief Information Officer			
		2.12 Defence People			
		2.13 Defence Science and Technology			
		Administered			
		2.14 Defence Force Superannuation Benefits			
		2.15 Defence Force Superannuation Nominal Interest			
		2.16 Housing Assistance			
		2.17 Other Administered			

Table 1. Portfolio Budget Statement programs mapped to Defence Purposes and Outcomes for 2018–19. This table reflects the information as per the 2018–19 Portfolio Budget Statements.

DEFENCE CORPORATE PLAN 2018-19 AT A GLANCE



Defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction.

How we will achieve this:

• Defence operational capability is able to be deployed to support Government policy objectives.

Activity 1.1a - Immediate Neighbourhood

Activity 1.1b - Wider Interests

 Defence contributions to National Support Tasks in Australia are provided in accordance with Government direction.

Activity 1.2a - National Support



Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by Government.

How we will achieve this:

• Defence develops strategic policy that guides the design, development, integration and preparedness of Defence capability as directed by Government.

Activity 2.1a - Strategic Risk

Activity 2.1b - Policy Advice

Activity 2.1c - 2016 White Paper

• The generation and sustainment of Defence capabilities achieve the objectives of Government.

Activity 2.2a - Future Force

Activity 2.2b – Interagency Operations

Activity 2.2c - Preparedness

Activity 2.2d - Raise, Train and Sustain

Activity 2.2e – Intelligence Services

Activity 2.2f – **Infrastructure Delivery**

Activity 2.2g – Infrastructure Enablers

Activity 2.2h - Materiel Acquisition

Activity 2.2i – Materiel Delivery

Activity 2.2j – Workforce

Activity 2.2k - ICT

 Defence delivers on the objectives of its enterprise reform program as agreed by Government.

Activity 2.3a – **Reform**

Activity 2.3b – **Enabling Services**

Activity 2.3c – ADF Total Workforce Model

Activity 2.3d - Cultural Reform

Activity 2.3e – **Resourcing**

 Defence's capability and capacity is enabled by supporting engagement and innovation with Australian industry.

Activity 2.4a - Defence Industry

Activity 2.4b - Research

 Australia's reputation as a strategic partner is enhanced by international engagement.

Activity 2.5a – International Engagement

• Defence provides appropriate health and welfare services.

Activity 2.6a - Health Support

Activity 2.6b - Welfare Services

Activity 2.6c - Welfare Delivery Reform

DEFENCE'S MISSION: DEFEND AUSTRALIA AND ITS NATIONAL INTERESTS.

OUR STRATEGIC DEFENCE INTERESTS ARE:

A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication.

A secure nearer region, encompassing maritime South East Asia and South Pacific (comprising Papua New Guinea, Timor-Leste and Pacific Island countries).

A stable Indo-Pacific region and a rules-based global order.

OUR OPERATING CONTEXT IS:

OPERATIONS

The Government deploys ADF personnel to operations overseas and within Australia to protect Australia and its national interests. ADF members are actively protecting Australia's borders and offshore maritime interests.

The Government's Defence policy, articulated in the 2016 Defence White Paper, is to align Australia's defence strategy with capability and resources, grow our international defence partnerships and invest in the Defence–industry partnership to develop and deliver innovative, cutting-edge capabilities. Inherent in this policy is a greater focus on seizing opportunities while managing strategic risks. This will be achieved through developing Defence's ability to take a more active role in shaping regional affairs and to respond to developments that threaten our interests. This is designed to ensure the ADF is better prepared to respond to complex emerging strategic risks by providing Government with greater options and flexibility.

ENVIRONMENT

RISK

Risks to the achievement of the Defence mission are managed by risk stewards in accordance with the Defence Risk Management Framework. Management of enterprise risks is overseen by the Enterprise Business Committee, with significant issues escalated internally for Defence Committee consideration. The risks are reviewed and updated at least annually, or when there are changes in Defence's operating environment.

Defence has one of the largest capital investment programs in the Commonwealth, consisting primarily of acquisition, sustainment and support of Defence materiel. The Integrated Investment Program includes all capital and related investments (such as materiel, estate and facilities, workforce and information and communications technology). The Integrated Investment Program is supported by a contestability function that informs the development of the risk assessment and decision support framework to ensure that acquisitions are aligned with strategy and resources.

CAPABILITY

Environment

The Strategic Centre

The Strategic Centre sets the direction for Defence, strengthens accountability and makes top-level decisions. The strategic centre is responsible for setting priorities, managing resources and steering the organisation to implement the Government's defence policies. Defence's strategic centre is based around its primary decision-making committee – the Defence Committee – which includes the Secretary, the Chief of the Defence Force, the Associate Secretary, the Vice Chief of the Defence Force, the Deputy Secretary Strategic Policy and Intelligence and the Chief Finance Officer.

Initiatives underway to improve the strategic centre include:

- Streamlining the top-level management structure, ensuring that it is aligned to the One Defence business model;
- Clarifying, documenting and promulgating the accountabilities of the Secretary and the Chief of the Defence Force;
- Strengthening the role of the Vice Chief of the Defence Force as the integrator of the future force;
- Strengthening the role of the Associate Secretary as an integrator of enterprise functions and as the central authority to deliver centre-led enterprise planning and performance monitoring;
- Ensuring the Defence Committee is focused on strategic issues and is supported by two subordinate committees, the Enterprise Business Committee chaired by the Associate Secretary and the Investment Committee chaired by the Vice Chief of the Defence Force;
- Building a strong and credible internal contestability function;
- Strengthening centre-led, enterprise-wide planning and performance-monitoring processes; and
- Improving enterprise planning, risk and organisational performance management.

Operations

The Government deploys Australian Defence Force (ADF) personnel to operations overseas and within Australia to protect Australia and its national interests. ADF members actively protect Australia's borders and offshore maritime interests.

Direction Setting

Since the release of the 2016 Defence White Paper, some strategic trends have accelerated – arguably faster than was anticipated. Defence will pay close attention to these trends and their impact on Australian interests as they develop, through a revised and more agile Strategy Framework released across the Department in 2018. The Strategy Framework reinforces the importance of alignment between strategy, capability, and resources. Importantly, it also gives effect to the recommendations in the First Principles Review for a strong strategic centre.

Internal review has confirmed that the strategic and capability ambitions outlined in the 2016 Defence White Paper remain relevant and appropriate in the face of these trends. In response to a more contested and competitive environment, where established rules and norms of behaviour are under challenge, the White Paper ushered in a proactive posture for Defence, aimed at strengthening our relationships with countries across the region, developing a shared capacity to work together to address security challenges, buttressing regional and global norms, and preferably preventing, when possible, security challenges from escalating rather than simply responding when they do. To meet this ambition, the White Paper funded and prioritised, for the first time, international engagement as core Defence business.

This more proactive strategy is backed up by significant investment in credible hard power, including regeneration of our maritime capability. Investment in Defence is on track to meet the Government's target of 2 per cent of GDP by 2020-21. And with it, the ADF will become more capable of operations to deter and defeat threats to Australia, operate

⁶ 70

over long distances to conduct independent combat operations in our region, and make more effective contributions to international coalitions that support our interests in a rules-based global order.

Defence is enacting this new Framework through rolling review of strategic planning and direction-setting. The Annual Strategic Review identifies risks in the strategic environment that Defence needs to be aware of, with significant issues escalated internally for Defence Committee consideration. This risk assessment informs the Department's highest level classified planning document, the Defence Planning Guidance, which includes specific direction on what Defence needs to do, and measures of success that are subject to rolling review to track progress against strategic ambition and lessons learned along the way. This will flow through into similarly regular reviews of Defence capability, the Defence budget, our preparedness settings, and Defence international engagement and the Defence Intelligence Enterprise, among others. The identification of individual accountable officers to drive integration across Defence missions, services, systems and capabilities forms a central element of our ongoing reform agenda. This will be particularly important during 2018-19 within the Defence Intelligence Enterprise, given the scale and pace of change within the national intelligence system.

Through these changes, we have strengthened our strategic management capability to set direction for the organisation, monitor and manage the performance of Defence, support the national security community, and provide assurance to Government that its outcomes are being delivered effectively and efficiently.

This framework identified three Strategic Defence Interests linked to three equally weighted Strategic Defence Objectives:

1. A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication.

The **Strategic Defence Objective** for this interest is: Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches. This objective relates to Defence Purpose 1.

2. A secure nearer region, encompassing maritime South East Asia and South Pacific (comprising Papua New Guinea, Timor–Leste and Pacific Island Countries).

The **Strategic Defence Objective** for this interest is: Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor–Leste and of Pacific Island Countries to build and strengthen their security. This objective relates to Defence Purpose 2.

3. A stable Indo-Pacific region and a rules-based global order.

The **Strategic Defence Objective** for this interest is: Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order. This objective relates to Defence Purpose 2.

Enterprise challenges

Defence has made significant progress in recent years implementing the First Principles Review and the 2016 Defence White Paper. However, challenges still remain. Defence must continue to embed reforms and ensure that they are adopted across the organisation. During 2018-19, Defence will focus on improving the capability life cycle, capability acquisition and sustainment reforms, service delivery, cyber security, information and communications technology and behaviours.

There are challenges associated with the recapitalisation of Defence as outlined in the 2016 Defence White Paper. This is particularly true for shipbuilding, where Defence is leading a significant national enterprise. Collective effort is required from other Commonwealth departments, state and territory governments and industry to be successful. Relationships will be coordinated and harmonised through a detailed governance structure, to maintain clarity of communication and decision making.

⁷

More broadly, the Government's new agenda around defence industry is also a priority. The Australian defence industry employs around 25,000 people, with over 3,000 small-to-medium enterprises. Defence's ability to deliver capability relies on a stronger relationship with Australian defence industry, and future defence procurement will be underpinned by a strategic contracting approach through collaborative relationships with industry.

Defence will also focus on cultural reform, building an environment where leaders are accountable for a positive culture that is collegiate and mutually respectful of people's skills. Defence will focus on embedding expected behaviours across the organisation but with a particular focus on our senior leaders.

Implementation of the Defence Strategic Workforce Plan 2016-2026 will continue, addressing workforce challenges for the Defence Australian Public Service, the ADF and defence industry. This plan is the key Defence workforce management document and gives Defence a whole-of-organisation view of our workforce needs.

Implementation of the Defence Estate Strategy 2016-36 will also continue during 2018-19. Defence has the most extensive land and property holdings in Australia, and the strategy provides enterprise-level direction on how Defence will manage this estate to ensure it is strategically aligned, safe, sustainable and affordable, and enables Defence capability and operations.

Defence will support the Australian Signals Directorate following its establishment as a statutory agency, so that it is able to meet current and future national intelligence challenges with appropriate resources and autonomy, while remaining in the Defence portfolio and continuing to closely support the ADF.

Defence Capability

The First Principles Review identified that organisational capability is derived from a strong workforce enabled by modern and effective security services, facilities and estate, information management, information and communications technology, people management systems, legal services, and health and logistics, supported by an integrated service delivery system. A service delivery framework was developed as part of First Principles Review implementation. The focus for the framework in 2018–19 involves standardising services, removing duplication of functions, professionalising the workforce and ensuring there are single, clear lines of ownership and accountability.

As part of the Defence White Paper, the Government will deliver a more capable, agile and potent ADF that can respond wherever Australia's interests are engaged. Defence designs, develops and integrates capability to provide the Government with options to mitigate strategic national security risks and ensure Defence can respond to direction.

Defence maintains capabilities to conduct military operations and provide civil aid and assistance in multiple domains. Defence capability encompasses multiple warfighting domains: sea, land, air, cyber, information and space. Defence is working to deliver an organisation that is more integrated on technical, organisational and cultural levels to deliver cohesive military effects across a joint warfighting domain.

The provision of a joint force that is capable, agile and potent in achieving the Strategic Defence Objectives directed by the Government is enabled through a flexible and scalable force design process. Informed through analysis of Government strategic guidance, the development of military strategy, and Defence planning guidance; Defence assesses emerging gaps, risks, issues and opportunities; develops and tests operating concepts; and proposes force structures and capability options that enhance and enable the joint force. The result is the provision of balanced, costed, and prioritised future force structure proposals (nested with extant Integrated Investment Program guidance) that are consistent with the Government's requirements of the ADF. This process draws on expertise and knowledge from across the Defence organisation as well as externally from other government agencies, industry, academia and our international partners.

The Service Chiefs, Chief of Joint Capabilities and Heads of enabling Groups are responsible for managing component capabilities, which are aggregated into the joint force. Working closely with partners across the Defence organisation, defence industry and Coalition forces; Defence capabilities are holistically introduced into service, sustained with agreed enhancements, and removed from service via retirement or replacement, as part of the Capability Life Cycle.

Defence has one of the largest capital investment programs in the Commonwealth, consisting primarily of acquisition, sustainment and support of Defence capabilities. Introduced at the same time as the 2016 Defence White Paper, the Integrated Investment Program includes all capital and related investments (such as materiel, estate and facilities, workforce and information and communications technology).

The Integrated Investment Program is supported by a contestability function that informs the development of the risk assessment and decision support framework to ensure that acquisitions are aligned with strategy and resources. Upgrading Defence bases and logistics systems, including fuel and explosive ordnance facilities in accordance with 2016 Defence White Paper requirements, remains a priority.

Over 2018-19, implementation of the Naval Shipbuilding Plan will continue in an environment where the successful tenderers for the major programs will be known. Naval Group Australia is progressing work on the Future Submarine (SEA1000), Luerssen Australia and its partners are progressing the Offshore Patrol Vessel (SEA1180), and a decision is expected on the Future Frigate (SEA5000) before the end of 2017-18. Work continues to implement enterprise-wide programs such as the Naval Shipbuilding College, the development of industrial bases to support sovereign shipbuilding, and the development and maintenance of whole-of-Government relationships necessary for the national shipbuilding endeavour. Defence will continue to implement policies to plan and guide development of the defence industry over the next decade to ensure that it can meet our capability needs and mature into an internationally competitive and sustainable industry.

In 2018-19, we will commence implementation of the Defence Industrial Capability Plan (DICP), the Defence Skilling and Science Technology Engineering and Mathematics strategy and the Defence Industry Participation Policy. This will include embedding the management of the Sovereign Industrial Capability Priorities, established as part of the DICP, across Defence.

By the end of the 2018-19 financial year Defence will have also significantly advanced the implementation of the major initiatives of the Defence Export Strategy, including consolidation of the internal and external presence of the recently established Australian Defence Export Office and the Australian Defence Export Advocate.

Enablers of Defence

Security

In 2018-19, we will implement a principles-based security policy. The Australian Government Security Vetting Agency (AGSVA) will concentrate on sustained achievement of its performance benchmarks with a continued focus on positive vetting backlog remediation. AGSVA will support and implement whole-of-Government personnel security reforms aimed at mitigating the insider threat.

Facilities and Estate

In 2018–19, we will continue to implement the Defence Estate Strategy 2016–36 to achieve a strategically aligned, affordable, safe and sustainable estate that enables Defence capability and operations. We will continue to optimise investment in renewal of the estate by delivering the facilities and infrastructure projects in the Integrated Investment Program. Delivery of an estate strategy, plan and profile, and fit-for-purpose facilities are key steps in ensuring that Defence's estate footprint aligns with current and future needs.

The Defence Environmental Policy and 2016-2036 Defence Environmental Strategy will be delivered through the Defence Environmental Plan across Defence with a focus on enabling the Defence mission through compliance, trust, accountability and efficiency. Priority action areas for 2018-19 will focus on increased resilience and environmental stewardship across Defence, while ensuring stronger integration of environmental and sustainability considerations into the Capability Life Cycle.

Defence continues to respond comprehensively to perfluoroalkyl sulfonate (PFAS) contamination on and around Defence sites. Defence is conducting a national program of environmental investigations to understand the nature and extent of PFAS contamination at its sites and in the surrounding communities. To ensure a coordinated and evidence-based response, Defence works with its Federal counterparts in the Department of the Prime Minister and Cabinet-led PFAS Taskforce, Department of the Environment and Energy, the Department of Health and also with relevant state and territory agencies. Defence engages with affected communities by conducting walk-in sessions, providing local points of contact and transparently sharing investigation outcomes and fact sheets via the Defence website. Defence continues to work towards the effective monitoring and management of PFAS contamination at its sites and is committed to responsible environmental management of its estate.

Information

Information is a critical enabler for Defence. In the military environment, information must be managed to provide the war fighter with common battlespace awareness and information superiority through integrated and interoperable information. It underpins the next generation of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance systems, and links sensors and weapons platforms. It is crucial to offset the relatively small size of the ADF and enable a competitive war fighting advantage over Australia's adversaries.

To enable this advantage, Defence will continue a period of change. As the organisation's digital transformation progresses, the new enhanced capability will transform the ADF into a fifth generation force. As outlined in the Defence Information and Communications Technology Strategy 2016-20 and the Enterprise Information Management Strategy 2015-25, the ability to manage information at an enterprise level and to enhance system interoperability, are fundamental enablers to Australia's future war fighting capability and central to this change.

⁰ 74

Workforce

An integrated ADF, Australian Public Service (APS) and defence industry workforce is the foundation for delivering the organisational capability recommended by the First Principles Review. It is also necessary to ensure Defence is fit-for-purpose and able to deliver its long-term strategy as described in the 2016 Defence White Paper. To achieve its mission, Defence needs ADF personnel and APS who are committed, with the right skills, and in the right roles. The Defence workforce also extends to contractors, consultants and defence industry, who provide critical services that contribute to Defence being able to meet Government policy expectations.

A key focus for 2018-19 is the continued implementation of the 10-year Defence Strategic Workforce Plan that sets out the skills Defence needs and details how Defence will attract, retain and develop its people. The Strategic Workforce Plan provides workforce priorities, initiatives and resources for attracting, growing and retaining the people Defence needs.

Defence will continue its cultural reform through implementation of the next iteration of *Pathway to Change. Pathway to Change: Evolving Defence Culture 2017-22* is an enterprise level strategy underpinned by a refreshed cultural intent statement and six cultural reform priorities: leadership accountability, capability through inclusion, ethics and workplace behaviours, health, wellness and safety, workplace agility and flexibility, and leading and developing integrated teams.

Building a diverse and inclusive workforce remains a key priority for the organisation. Attracting and retaining people that represent the Australian population in its diversity ensures that we are getting the best talent that Australia can provide. Gender equality and increasing female participation in our workforce and in senior leadership roles is fundamental to achieving Defence capability. In 2018-19, Defence will continue to implement strategies, such as the ADF Total Workforce Model, which enable us to build and maintain a diverse, motivated, engaged and talented workforce.

Health, Logistics, Education and Training

In 2018-19, the focus will remain on providing comprehensive health care to ADF members, delivering quality and safe health and wellbeing services and programs that are affordable and effective. Defence will continue to work closely with the Department of Veterans' Affairs to enhance the transition process for serving and ex-serving members. Other health priorities in 2018-19 include the continued delivery of the improved mental health and wellbeing program through the Defence Mental Health and Wellbeing Strategy, the eHealth system and a newly contracted supply arrangement for ADF Health Services.

The continued delivery of a fully integrated Joint Logistics program to the ADF will be achieved through the integration of logistics functions, resources, capability and infrastructure across the Defence logistics enterprise. This will also be achieved in partnership with defence industry to deliver three essential capability outputs, logistics support to operations and readiness activities, strong strategic centre for Defence logistics and logistics support and advice throughout the Capability Life Cycle.

Joint professional military education and training will be delivered and improved to enable excellence in joint warfighting and the mastery of the profession of arms. This will be achieved through the professional education and development of ADF officers, sailors, soldiers, airmen and airwomen, and Defence's public servants. This goal will be supported by the comprehensive and continuous review of the Joint Professional Military Education continuum and curricula to sustain and evolve a unified approach to joint learning delivery and curriculum management across the Australian Defence College and the Defence learning domain. There will be enhanced linkages with the existing joint force design process to ensure education, training and research are complementary to joint modernisation. Additionally in 2018-19, the Centre for Defence Research program will be enhanced to further the Defence organisation's mastery of the profession of arms.

¹¹ 75

Risk Oversight and Management

Enterprise Risks

Risk management is governed by the *Commonwealth Risk Management Policy 2014* and is undertaken in accordance with an overarching Defence Risk Management Framework. Through this framework, Defence addresses risks at three levels:

- **Strategic risks** These risks are described in the 2016 Defence White Paper and are managed as shared risks with Australian Government, international and industry partners. Understanding of the national security risk environment informs the risk context for enterprise-level risks.
- Enterprise-level risks These are events which may limit or compromise Defence's collective ability to meet the obligations and requirements set by Government. These risks may arise from four 'enterprise vulnerabilities', which are: integration across Defence; integration with key external partners; compliance with legislation and Government policy; and efficient, effective, economical and ethical use of resources.
- **Delivery risks** These are risks to Defence achieving efficient and effective operating intent. They are inwardly focused on how Defence undertakes the activities in support of this plan.

Risks to the achievement of the Defence mission are managed at all levels of the organisation through appropriate, risk-informed decision making. Enterprise risk management relies on the oversight and governance of risk communication to understand the capacity pressures being borne across Defence in managing these risks.

To do this the strategic centre looks at four 'enterprise vulnerabilities':

- Integrate across Defence the integration of Defence's major business processes
- Integrate with key partners the cooperation between Defence and its external partners
- Compliance assurance that Defence meets its legal obligations
- Use of resources assuring the effective and efficient use of resources to meet Government's objectives

Defence senior management exercises high-level oversight and provides assurance of risk mitigation to Government. A Defence enterprise risk assessment is produced for senior committees to support their collective management.

In 2018-19, Defence will increase the transparency of its internal control environment to better understand the impact of major business processes in protecting the business of Defence against its vulnerabilities. Focus will remain on embedding clear individual and collective decision rights around shared risk together with a compliance program which will support risk-informed decision making.

Control and Governance

In 2018-19, Defence will continue to mature its control functions – financial management, internal audit, inspectors-general and judge advocate – so that they can provide assurance to the Defence senior committees – the Defence Committee, the Enterprise Business Committee and the Investment Committee – that Government-directed outcomes are being delivered in accordance with legislative and policy requirements.

Both the First Principles Review and the 2016 Defence White Paper highlight the importance of maintaining a balance between Defence strategy, capability and resources. The Chief Finance Officer (CFO) will work closely with key accountable officers to ensure that enterprise financial management, corporate planning and performance management are aligned to support the Defence senior leadership in maintaining this balance and achieving compliance with the PGPA Act.

² 76

Effective financial management enables Defence to ensure Government-allocated resources are used to deliver Government-directed outcomes. The CFO has responsibility for ensuring appropriate financial governance within Defence.

The CFO will drive financial management improvement programs through uniform financial management approaches and a streamlined accountability structure for ensuring appropriate financial governance within Defence.

The Defence Audit and Risk Committee provides the Secretary and the Chief of the Defence Force with independent advice and assurance on the appropriateness of Defence's financial reporting, performance reporting, system of risk oversight and management, and the system of internal control, in accordance with the PGPA Act and *Public Governance, Performance and Accountability Rule 2014*.

In accordance with the PGPA Act, and in support of the Commonwealth Fraud Control Framework, Defence has instituted Defence Fraud Control Plan No. 11, which describes the fraud control framework our organisation has implemented to prevent, detect and respond to fraud. A focus for 2018-19 will be to develop our capacity to identify and manage enterprise-wide vulnerabilities and risk factors within a diverse operating environment.

Defence's Legal Framework

Defence Legal Division provides an in-house legal service and other legal support to all Services and Groups in Defence. As Defence operates in an increasingly complex legal and regulatory environment, the work by Defence Legal contributes to the effectiveness of the ADF and to the prudent management and administration of the Defence organisation as a whole.

A primary focus of Defence Legal's work is on operations and security law, including international humanitarian law and the laws of armed conflict. Other important fields of focus, particularly in peacetime, are administrative law and discipline law, together with international agreements and arrangements, non-material commercial projects and legal advice on a range of matters across Defence. In recent years there has been a focus on the proactive management of large-scale litigation associated with contamination as well as the resolution of historic civil compensation matters.

Planned Performance

This section sets out the intended results and high-level activities that contribute to Defence's purpose, including indicators of performance over the next four years. These should be read in conjunction with the Portfolio Budget Statements 2018-19, the Portfolio Additional Estimate Statements 2018-19, and the Defence Annual Report 2017-18.

Purpose 1: Defend Australia and its national interests

Defence defends Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction.

Defence plans for, develops and maintains the capability to deter and defeat armed attacks on Australia or on Australian interests. This includes planning for, conducting, controlling and evaluating Defence and/or coalition contributions to Government-directed operations.

Defence also supports the Federal, State and Territory governments with emergency and non-emergency tasks, as well as supporting events of national significance when requested by the Australian Government.

Portfolio Budget Statement 2018-19 Outcome Statement 1: Defend Australia and its national interests through the conduct of operations and the provision of support for the Australian community and civilian authorities in accordance with Government direction.

Intended Result 1.1: Defence operational capability is able to be deployed to support Government policy objectives.

Activity	Performance Criteria	Target	Timeframe
1.1a Conduct and sustain operations contributing to the security and safety of the immediate neighbourhood in accordance with Government strategic direction.	Assessment of operational deployments against outcomes agreed with Government.	All Government directed tasks are met.	2018-22
1.1b Conduct and sustain operations supporting wider interests in accordance with Government strategic direction.	Assessment of operational deployments against outcomes agreed with Government.	All Government directed tasks are met.	2018-22

Intended Result 1.2: Defence contributions to National Support Tasks in Australia are provided in accordance with Government direction.

Activity	Performance Criteria	Target	Timeframe
1.2a Contribute to national security and support tasks as directed by Government.	Assessment of capacity and capability provided in support of whole-of-Government outcomes.	All Government directed tasks are met.	2018-22

¹⁴ 78

Purpose 2: Protect and advance Australia's strategic interests

Defence protects and advances Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security and stability as directed by Government.

Defence must provide high-quality, relevant and timely advice to Government on Defence strategy, capability and resourcing. Defence has implemented the 'strategic centre' model to ensure that all advice provided to Government is contested for alignment with Government strategic direction and to ensure the options being presented to Government support achievement of its Defence strategy, as described in the 2016 Defence White Paper.

The Government expects Defence to play an active role in contributing to regional security and stability, and to contribute to coalition operations around the world where our interests are engaged. Delivering on these requirements will require Australia to build on its strong network of bilateral and multilateral relationships. Through regular dialogue and practical cooperation, Defence is strengthening its engagement with partners to support shared responses to shared challenges.

Capability delivery is a core business process that enables Defence to perform its mission of defending Australia and its national interests now and into the future. Defence must procure capability efficiently and effectively. In 2018-19, Defence will continue building the new levels of capability required by Government and described in the 2016 Defence White Paper and the Integrated Investment Program. Major investments will enhance ADF capability to conduct operations to deter and defeat threats to Australia, operate over longer distances to conduct independent combat operations in our region, and make more effective contributions to multinational coalitions.

Australia's defence industry is a major partner in the Government's plans for current and future Defence capabilities. It is vital that Australia maintains a science and technology base and defence industry capable of supporting Defence's acquisition and sustainment requirements during peacetime and operations. A highly skilled and capable Australian defence industry is necessary for Defence to achieve its strategic objectives and deliver large-scale, complex projects and sustain military capability. Defence will work with industry to reflect a shared policy agenda that supports the growth and competitiveness of Australian businesses.

Portfolio Budget Statement 2018-19 Outcome Statement 2: Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security as directed by Government.

Intended Result 2.1: Defence develops strategic policy that guides the design, development, integration and preparedness of Defence capability as directed by Government.

Activity	Performance Criteria	Target	Timeframe
2.1a Undertake regular review of strategic risks and mitigations through Defence's strategic-level documents.	Defence's strategic policy is updated to reflect changes in Defence strategic risks.	Defence's strategic review framework supports and manages risk through annual reviews.	2018-22
2.1b Provide Ministers with quality, relevant and timely strategic policy advice.	Quality, relevant and timely strategic policy advice is available for Government.	Ministers are able to make informed decisions in a timely fashion based on advice received.	2018-22
2.1c Deliver and implement the 2016 Defence White Paper.	Effective implementation of the 2016 Defence White Paper.	The 2016 Defence White Paper implementation plan activities for 2018-22 are delivered as agreed with Government.	2018-22

¹⁵ 79

Intended Result 2.2: The generation and sustainment of Defence capabilities achieve the objectives of Government.

Activity	Performance Criteria	Target	Timeframe
2.2a Design the future force through management of the capability lifecycle and the Integrated Investment Program.	The future force design is realised through resourcing delivered through the Integrated Investment Program.	Future force design development aligns to strategic policy.	2018-22
2.2b Integrate and prepare capability elements, and plan for the effective conduct of joint, combined and interagency operations.	Defence's maritime, land, air force and joint capabilities are generated and sustained to ensure forces are available to meet Government requirements.	Forces meet preparedness requirements to conduct joint, combined and interagency operations as directed by Government.	2018-22
2.2c Monitor preparedness for Government-directed operations and national support tasks through the preparedness management system.	Chief of the Defence Force preparedness levels meet Government requirements.	Chief of the Defence Force preparedness levels are achieved as agreed with Government.	2018-22
2.2d Conduct raise, train and sustain activities to ensure maritime, land and aerospace forces are available to meet Government direction.	Chief of the Defence Force preparedness levels meet Government requirements.	Chief of the Defence Force preparedness levels are achieved as agreed with Government.	2018-22
2.2e Develop, deliver and sustain intelligence capability to meet Government, Defence and partner requirements.	Defence intelligence outputs align with Government intelligence priorities.	Government intelligence priorities are met.	2018-22
2.2f Manage and sustain the Defence estate to meet Government and Defence requirements by developing and delivering major infrastructure, property and environmental programs.	The management and sustainment of the estate meets the requirements of the Capability Managers.	The Defence Estate Strategy implementation plan is delivered as agreed.	2018-22
2.2g Deliver integrated estate and infrastructure services to enable Defence people, equipment and systems, including base support for	Service delivery is aligned to capability outputs.	Less than 5% service failures impacting operational capability.	2018-22
the ADF.	Service delivery meets customer requirements.	An increase in the overall customer satisfaction rate.	2018-22
2.2h Manage the acquisition and sustainment of Defence materiel equipment to meet Government and Defence requirements.	Capability proposals, once approved by Government, meet agreed schedule and are delivered within agreed costs and scope.	Deliver Government approved acquisition projects to budget, schedule and agreed capability scope.	2018-22
2.2i Deliver agreed materiel equipment support to meet operational requirements.	Sustainment products are delivered consistent with Capability Manager requirements.	Deliver sustainment products to meet Capability Manager requirements.	2018-22

Activity	Performance Criteria	Target	Timeframe
2.2j Implement the Defence Strategic Workforce Plan 2016-2026 to attract, recruit, develop and retain a highly skilled workforce.	Progress in the delivery of actions from the Defence Strategic Workforce Plan 2016-2026.	Implementation milestones are achieved.	2018-22
2.2k Deliver and sustain a dependable, secure and integrated ICT capability that ensures a secure and integrated information environment to support Defence business and military operations.	ICT services meet requirements.	ICT capabilities are delivered in accordance with the Integrated Investment Program as governed by the Investment Committee.	2018-22

Intended Result 2.3: Defence delivers on the objectives of its enterprise reform program as agreed by Government.

by Government.			
Activity	Performance Criteria	Target	Timeframe
2.3a Resource, implement and review Defence's enterprise reform program.	Business outcomes are improved as part of broader Defence reform.	Defence reform is achieved in accordance with Reform Implementation Plans.	2018-22
2.3b Integrate enabling services to deliver a single Defence enterprise.	The Service Delivery system enables ADF operations.	Enabling services are delivered in accordance with agreed requirements.	2018-22
	Enterprise planning and performance monitoring processes are delivered in line with the One Defence Business Framework, supporting Defence capability.	Defence meets its non- financial performance management and risk management obligations.	2018-22
2.3c Implement the ADF Total Workforce Model to support individual and organisational flexibility.	All elements of the ADF Total Workforce Model, including Service Category 6 (mature) are implemented.	The Defence Workforce has the agility and skills required to meet current and future demand to support capability.	2018-22
2.3d Implement and evaluate Defence's cultural reform strategy, Pathway to Change: Evolving Defence Culture 2017-22.	Implementation of the six key cultural priorities through the regular enterprise performance reviews.	Cultural reform priorities are implemented as set out in the Pathway to Change strategy.	2018-22
2.3e Deliver enterprise resource planning and budget management in accordance with Commonwealth legislation and policy frameworks.	Produce Defence's Budget, Financial Statements and the annual Defence Management and Finance Plan.	Produced in accordance within agreed statutory timeframes.	2018-22

Intended Result 2.4: Defence's capability and capacity is enabled by supporting engagement and innovation with Australian industry.

Activity	Performance Criteria	Target	Timeframe
2.4a Engage with industry to enhance the Australian industrial base that supports Defence capability.	The objectives of the Defence Industry Policy Statement are met.	Delivery of the outcomes of the Defence Industry Policy Statement.	2018-22
2.4b Conduct applied research focused on supporting Defence and national security operations, sustaining and enhancing current capability,	Defence's strategic research builds understanding of future Design capability.	Strategic research activities are aligned with Integrated Investment Program priorities.	2018-22
and supporting the development and acquisition of future capability.	Defence capability is enhanced by collaborative research partnerships with Publicly Funded Research Agencies, academia, industry, and international research agencies.	Collaborative activities with academia, industry, and allied defence research agencies are aligned to 2016 Defence White Paper and Defence Industry Policy Statement priorities.	2018-22
	Science and technology research supports Defence operations, sustainment and enhancement of current capability, and the development and acquisition of future capability.	Science and technology activities are balanced to support Defence operational and capability priorities in accordance with 2016 Defence White Paper.	2018-22

Intended Result 2.5: Australia's reputation as a strategic partner is enhanced by international engagement.

Activity	Performance Criteria	Target	Timeframe
2.5a Conduct international engagement to enhance Australia's strategic position as directed by Government in accordance with the 2016 Defence White Paper.	Defence has met its commitments to Government and the intention of the Defence International Engagement Policy.	Short-term (2018-2022) government objectives are met including those outlined in the Defence International Engagement Policy	2018-22

Intended Result 2.6: Defence provides appropriate health and welfare services.

Activity	Performance Criteria	Target	Timeframe
2.6a Deliver health support to meet the requirements of the ADF.	Quality of health services delivered to ADF members and families.	Delivery of health services meets standards.	2018-22
2.6b Deliver welfare services to agreed standards to meet the requirements of the ADF.	Quality of welfare services delivered to Defence personnel and families.	Delivery of welfare services meets standards.	2018-22
2.6c Deliver initiatives to improve the delivery of welfare services to current and former members of the ADF.	ADF members and families are supported through the delivery of welfare services and support services.	Support is delivered in a timely and professional manner.	2018-22







2019-20 DEFENCE CORPORATE PLAN

COVERING THE PERIOD OF 2019-23



STATEMENT OF PREPARATION

I, as the accountable authority of Defence, present the 2019–20 Defence Corporate Plan, which covers the periods of 2019–23, as required under paragraph 35(1)(b) of the Public Governance, Performance and Accountability Act 2013.

Greg MoriartySecretary of Defence
13 July 2019

Moreuty

© Commonwealth of Australia 2019

ISSN 2205-5282 (online)

ISBN 978-1-925890-15-0

This publication is available for your use under a <u>Creative Commons BY Attribution 3.0 Australia</u> licence, with the exception of the Commonwealth Coat of Arms and the Department of Defence logo, signatures and where otherwise stated. The full licence terms are available from

http://creativecommons.org/licenses/by/3.0/au/legalcode.



Use of the Department of Defence's material under a <u>Creative Commons BY Attribution 3.0 Australia</u> licence requires you to attribute the work (but not in any way that suggests that the Department of Defence endorses you or your use of the work).

Department of Defence material used 'as supplied'

Provided you have not modified or transformed the Department of Defence material in any way including, for example, by changing the Department of Defence text, the Department of Defence prefers the following attribution:

Source: The Australian Government Department of Defence

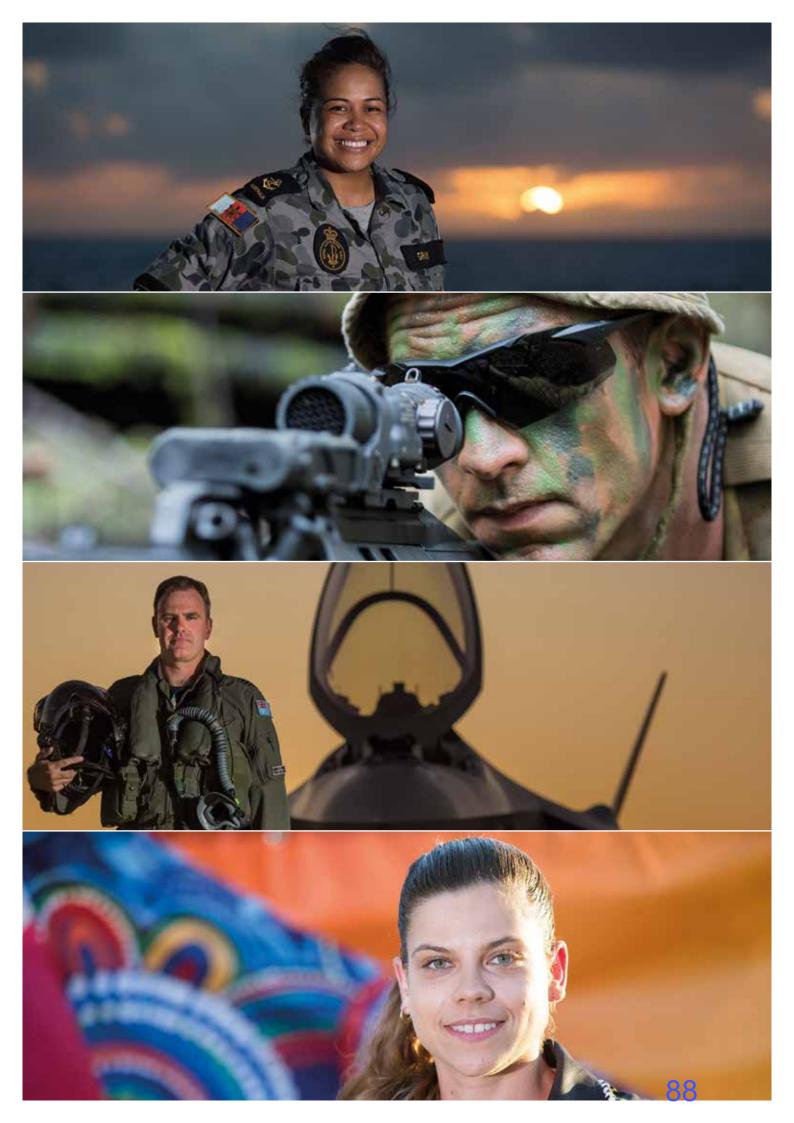
Derivative material

If you have modified or transformed the Department of Defence's material, or derived new material from those of the Department of Defence in any way, then the Department of Defence prefers the following attribution:

Based on the Australian Government Department of Defence's data.

Contents

INTRODUCTION	5
DEFENCE PORTFOLIO	6
OPERATING ENVIRONMENT	7
DEFENCE CAPABILITY	9
REFORM, GOVERNANCE AND RISK OVERSIGHT	13
PERFORMANCE	16



Introduction

The 2019–20 Defence Corporate Plan sets out Defence's purpose, intended results and key activities to be achieved covering the period 2019-23. In line with the requirements under the Public Governance, Performance and Accountability Act 2013¹ (PGPA Act), this plan describes the expected performance required to achieve Defence's purpose over the life of the Corporate Plan.

Defence's purpose is to:

Defend and protect Australia and advance its strategic interests.

Underpinning this purpose are two outcome statements² through which we focus our portfolio resourcing and delivery of intended results for Government. These are:

- Defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction; and
- Protect and advance Australia's strategic interests through the provision of strategic policy, the
 development, delivery and sustainment of military, intelligence and enabling capabilities, and the
 promotion of regional and global security and stability as directed by Government.

In 2019–20, we will continue to deliver significant outcomes for the Australian Government and the Australian people, including the conduct of operations and national support tasks, enhanced defence capability, strong partnerships with Defence industry and effective international engagement.

Performance against the Corporate Plan will be reported through annual performance statements, to be included in the Defence Annual Report for 2019–20.

The Corporate Plan is a living document and will be updated at least annually to reflect changes in our operating environment, refresh organisational priorities and ensure Defence delivers against its purpose.

Together, we are pleased to present the 2019–20 Defence Corporate Plan.

Greg Moriarty

Secretary of Defence

Mounty

13 July 2019

Angus Campbell, AO, DSC

General

Chief of the Defence Force

10 July 2019

Purposes are defined by Part 1, Division 2–8 of the Public Governance, Performance and Accountability Act 2013 as 'the objectives, functions or role' of an entity.

² The Defence outcomes statements are published in the Portfolio Budget Statements

Defence Portfolio

Defence is established as a Department of State under the Administrative Arrangements Order. Operating as one Defence entity under a diarchy, the Department of Defence operates under the *Public Service Act 1999*; and the Australian Defence Force (ADF) is constituted through the *Defence Act 1903*.

In addition to the Department of Defence and the ADF, the Defence portfolio comprises other entities including the Australian Signals Directorate, Defence Housing Australia, the Australian Defence Force Cadets, and a number of trusts, companies and other statutory offices and entities. The portfolio also contains the Department of Veterans' Affairs and associated bodies as designated in the Administrative Arrangements Order.

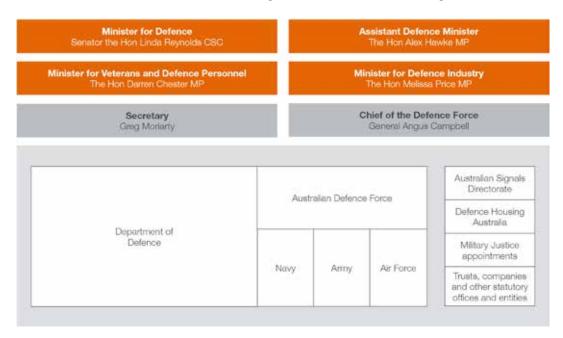


Figure 1: Defence portfolio structure as at 30 June 2019. Note the Department of Veterans' Affairs is not included in the figure.

Defence's annual Portfolio Budget Statements detail the program structures against outcomes and purpose for Defence.

Purpose	Outcome Statements	Budget Programs
Defend and protect Australia and advance its strategic interests	Outcome 1: Defend Australia and its national interests through the conduct of operations and provision of support for the Australian community and civilian authorities in accordance with Government direction	Operational Programs 1.1 – 1.3
	Outcome 2: Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global stability as directed by Government	Departmental Programs 2.1 – 2.13
		Administered Programs 2.14 – 2.17

The scope of the 2019-20 Defence Corporate Plan includes priorities for Defence (Department of Defence and ADF components). The Department of Veterans' Affairs, Australian Signals Directorate and Defence Housing Australia have developed their own corporate plans.

Operating Environment

Defence organisation

Defence's purpose is to defend and protect Australia and advance its strategic interests.

Defence protects and advances Australia's strategic interests through the provision of military capabilities, to promote security and stability and to provide support for the Australian community and civilian authorities, as directed by the Government.

Defence is administered by a diarchy, which is the term used to describe the joint leadership of Defence by the Secretary of Defence and the Chief of the Defence Force under the general control of the Minister for Defence. The diarchy, which is supported by legislative and administrative arrangements, encompasses the individual and joint responsibilities and accountabilities of the Secretary and the Chief of the Defence Force, to ensure Defence operates cohesively as one organisation, working together to meet Australian Government requirements and achieves its purpose.

The organisational structure of Defence includes capability and enabling functions structured under Defence Groups and Australian Defence Force Services. The Defence organisational chart can be found at www. defence.gov.au.

The One Defence Business Model below reflects the way the core functions within Defence operate together.

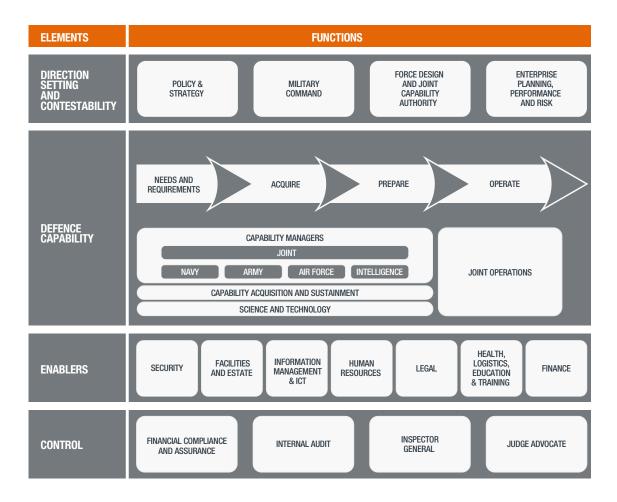


Figure 2: One Defence Business Model

To deliver our purpose, Defence must be a diverse and inclusive employer of choice; respectful, trusted and proven to deliver. To maximise our capability, sustain the trust of Government, the Australian community and each other, we must take the best in our culture forward and hold to account those that do not meet our standards. Our cultural objectives for 2019-20 are: leadership accountability; capability through inclusion, ethics and workplace behaviours; health, wellness and safety; workplace agility and flexibility; and leading and developing integrated teams. We will build on the progress we have made over the past several years to foster a more inclusive culture, to be representative of the community we serve, and to drive high-performance at all levels.

Defence values provide a common and unifying thread for all people working in Defence. These values are:

- Professionalism-striving for excellence in everything we do
- · Loyalty-commitment to each other and Defence
- Integrity—doing what is right
- Courage the strength of character to honour our convictions (moral courage) and bravery in the face of personal harm (physical courage)
- Innovation—actively looking for better ways of doing our business
- Teamwork—working together with respect, trust and a sense of collective purpose.

The Secretary and the Chief of the Defence Force lead Defence's workforce, which include Australian Defence Force members of the Navy, Army and Air Force, and Australian Public Service employees. Defence works in partnership across the Australian Government, with international counterparts, industry and academia.

Operations

The Government deploys Defence personnel to operations overseas and within Australia to protect Australia and advance its strategic interests. Defence is also called upon to provide support to the Australian community and civil authorities within Australia as directed by Government. National security is a whole-of-government commitment, requiring Defence to work with other security agencies, both across Government and internationally, to ensure strategic objectives are achieved.

The Government expects Defence to be able to defend Australia, play an active role in contributing to regional security and stability, and contribute to coalition operations around the world where our interests are engaged. Figure 3 identifies ADF operations as at 1 July 2019.

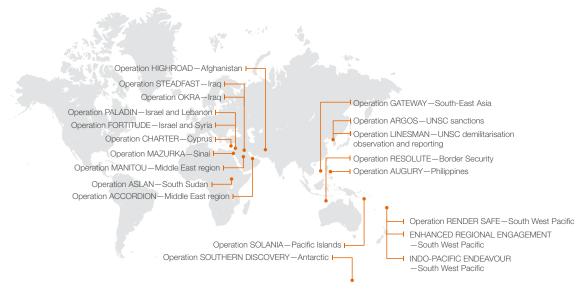


Figure 3: ADF operations as at 1 July 2019

Defence Capability

The 2016 Defence White Paper identified Australia's strategic defence interests as: a secure and resilient Australia; a secure near region, encompassing maritime South-East Asia and the South Pacific; a stable Indo-Pacific region; and a rules-based global order that supports our interests.

Since the release of the 2016 Defence White Paper, some strategic trends have accelerated faster than initially anticipated. Defence strategic and capability ambitions remain relevant and appropriate in the face of these international trends. A more proactive posture for Defence is desirable to strengthen our relationships with countries across the region to address security challenges; regional and global norms; and preventing, when possible, security challenges from escalating rather than simply responding when they do.

The Challenge	Defence's response
A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication.	Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches.
A secure nearer region, encompassing maritime South East Asia and South Pacific (comprising Papua New Guinea, Timor–Leste and Pacific Island Countries).	Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor–Leste and of Pacific Island Countries to build and strengthen their security.
A stable Indo-Pacific region and a rules-based global order.	Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order.

Figure 4: Strategic Defence Objectives

The Defence Corporate Plan is Defence's principal public planning document to assure Government and the Australian people that strategy, capability and resources are aligned to the highest priorities in achieving Defence's purpose and the strategic objectives within the 2016 Defence White Paper. A defence force that can meet the challenges of the future requires the generation, integration and sustainment of Defence capability across multiple decades. This is balanced with the need to be agile and responsive to Government direction to address emerging threats within changing environments and evolving geopolitical dynamics.

Defence's Strategic Framework supports planning and direction-setting, and risk assessments to understand the strategic environment. These risk assessments inform the Department's highest level classified planning document, the Defence Planning Guidance.

Figure 5 demonstrates the strategic, complex and multi-layered nature of planning within Defence. It should be noted that this does not include all documents and that there are classified environments and systems in place designed to ensure planning, resourcing, prioritisation, risk management and delivery is aligned with Government direction and the Secretary and the Chief of the Defence Force's strategic priorities.



Figure 5: Enterprise planning hierarchy in Defence

Defence has one of the largest capital investment programs in the Commonwealth, consisting primarily of acquisition, sustainment and support of Defence capabilities. Introduced at the same time as the 2016 Defence White Paper, the Integrated Investment Program includes all capital and related investments (such as materiel, estate and facilities, workforce and information and communications technology).

The Integrated Investment Program is supported by a contestability function that informs the development of the risk assessment and decision support framework to ensure that investment proposals are aligned with strategy and resources. Upgrading Defence bases and logistics systems, including fuel and explosive ordnance facilities in accordance with 2016 Defence White Paper requirements, remains a priority.

The National Naval Shipbuilding Enterprise will continue to build capacity and Defence will strive to achieve the planned milestones with the *Naval Shipbuilding Plan* to establish a sovereign industrial capability. Work on the development and implementation of the Sovereign Industrial Capability Priority Plans has commenced, providing information to Defence industry on the focus and requirements of Defence for sovereign industrial capabilities to support the Australian Defence Force. Collective effort is required from other Commonwealth departments, state and territory governments and industry to be successful. Relationships will be coordinated and harmonised through a detailed governance structure to maintain clarity of communication and decision making.

Preparing the Future Force

As part of the 2016 Defence White Paper, the Government is delivering a more capable, agile and potent ADF that can respond in support of Australia's interests. While the 2016 White Paper identified the key geopolitical factors driving changes in Defence's strategic environment, the rate of change has accelerated across the Indo-Pacific region beyond projections made as recently as three years ago.

Defence, as a key element of national power and influence, must be agile and responsive to deliver the priorities of the government of the day. Defence capabilities are increasingly part of a whole-of-government strategic effect, which also includes academia, defence industry and international partners in the delivery of national security outcomes.

A joint force that is capable, agile and potent in achieving the Strategic Defence Objectives directed by the Government requires a flexible and scalable force design process. Informed through analysis of Government strategic guidance, the development of military strategy, and Defence planning guidance; Defence assesses emerging gaps and opportunities; develops and tests operating concepts; and proposes force structures and capability options that enhance and enable the joint force.

In 2019-20, Defence will continue to design, develop and integrate capability to provide the Government with options to mitigate strategic national security risks. This includes Defence's ability to respond and conduct military operations and provide civil aid and humanitarian assistance in multiple domains as a joint force, bringing together land, air, sea, intelligence, electronic warfare, space, information (including cyber) and personnel capability. Defence is working to integrate the technical, organisational and cultural aspects of our business to deliver cohesive military effects across a joint warfighting domain.

Enabling and delivering capability requirements

The Chief of Defence Force's Preparedness Directive (CPD) articulates the preparedness requirements of the joint force, including the required fundamental inputs to capability. The Capability Managers in Defence are responsible for managing component capabilities in accordance with the CPD to deliver leading edge defence capabilities that provide strategic advantage and avoid strategic surprise, supported by delivery and enabler Groups. These are integrated into the current and future joint force.

Working closely with partners across the Defence organisation, defence industry and Coalition Forces; Defence capabilities are introduced into service, sustained with agreed enhancements, and removed from service via retirement or replacement, as part of the Capability Life Cycle.

The identification of individual accountable officers to drive integration across Defence systems and capabilities is a One Defence initiative and forms a central element of Defence's ongoing reform agenda. Defence will continue to strengthen its strategic management capability to set direction for the organisation, monitor and manage organisational performance, and provide assurance to Government that its outcomes are being delivered effectively and efficiently.



Figure 6: Enabling and delivering defence capability. The figure provides an overview of the elements that contribute through the Capability Life Cycle and achieve One Defence outcomes.

Reform, Governance and Risk Oversight

Defence 2022: Embedding One Defence Reform

Defence must be efficient, agile and responsive to deliver the priorities of the government in a dynamic strategic environment. Defence has reformed significantly in recent years, through the implementation of the First Principles Review, which has delivered a fundamental leap in Defence's efficiency and effectiveness as an organisation, and provided an enduring foundation for operating into the future.

Defence is now challenging itself to move beyond the First Principles Review to drive a continuous reform and improvement journey. There are significant reforms underway that build upon the strong foundation provided by the First Principles Review, including workforce skills and flexibility, transforming business processes, integrating delivery of corporate and enabling services, and increasing the ability to work with Defence industry. These initiatives will be under the central oversight and control of the Defence Committee, reporting to the Minister for Defence.

Building on the First Principles Review. The purpose of the First Principles Review was to make sure Defence is outcomes-orientated, agile and responsive to Government priorities. Defence remains committed to the principles at the heart of the review, implementing a One Defence approach and embedding the One Defence Leadership Behaviours.

Workforce reform. Defence is transforming its workforce to meet rapidly evolving national security challenges. It faces issues attracting, recruiting, training, professionalising and upskilling its workforce, both generally and in specific workforce areas such as shipbuilding, cyber and ICT. A concentrated effort is underway to attract, recruit, retrain and retain the right people. This includes ensuring Defence's employment offer is competitive, implementing programs and pathways to foster specialised skillsets, modernising recruitment practices, and creating a work environment that makes Defence an employer of choice. Defence is collaborating and partnering with industry and academia to build skills, noting building skills of defence industry yields better results for Defence capability.

Business process transformation. Defence is changing the way it conducts its business by enhancing integration and connectivity across the organisation. This will significantly increase efficiency. Key to this process are Defence's enterprise information management (EIM) and enterprise resource planning (ERP) projects. These projects are very ambitious and the largest such initiatives ever undertaken by the Australian Government. Successful implementation will fundamentally improve the administration of the entire Defence enterprise. Further improvements are also being implemented to Defence's estate and supply chain management.

Integrated service delivery. Defence is introducing a more strategic and customer-focused integrated service delivery system. This will reduce the time needed to navigate Defence systems and processes, enabling the Defence workforce to remain focussed on its core business. Defence's fiscal stewardship is being enhanced by the transition to a contemporary financial management approach.

Defence industry. Defence is continuing to improve its relationship with sovereign defence industry. This supports more effective delivery of defence capability and strengthens Australia's industrial base.

Having a strong sovereign defence industrial base is an expression of our national power and supports our agility to meet the challenges of the changing strategic environment. A strong exporting defence industry also gives us influence on the world stage.

The First Principles Review provided Defence with a strong foundation. By embedding a continuous improvement culture and maintaining a disciplined focus on our reform priorities, Defence will continue to evolve and adapt to Australia's changing strategic circumstances.

Governance and Control

The strategic centre within Defence is responsible for setting priorities, managing resources and steering the organisation to implement the Government's defence policies and achieve Defence's purpose. Defence's strategic centre is based around its primary decision-making committee – the Defence Committee (Tier 1). The Defence Committee is focused on strategic issues and is supported by the Tier 1 Defence Audit and Risk Committee, and four Tier 2 subordinate committees: the Strategic Policy Committee, the Chiefs of Service Committee, the Enterprise Business Committee, and the Investment Committee.

The Defence Committee approved the Defence Enterprise Committee Governance Framework in December 2018. The Framework, through its supporting systems and processes, will:

- · Clearly align with the Defence Business Cycle
- Show how the role, function and decision-making authority and accountability of the Tier 1 Committees connect and intersect with the Tier 2 and Tier 3 Committees
- Ensure strategic planning and prioritisation decisions are made by appropriate committees based on relevant information
- Focus on performance and assurance of Defence strategic intent
- Facilitate escalation of risk and issue management
- Provide formal guidance to communicate and drive effective committee processes.

The Framework aims to further enhance Recommendation 1.14 of the First Principles Review, 'that all other enterprise-wide committees be reviewed for their relevance and alignment with the One Defence business model with the aim of a substantial reduction in the number of committees' and is expected to promote a performance orientation; clarify accountabilities and decision rights; encourage openness, transparency and integrity; and promote effective collaboration.

Under the Framework, the Defence Audit and Risk Committee's role is to review and provide written advice to the Secretary and CDF on the appropriateness of Defence's financial reporting, performance reporting, system of risk oversight and management, and the system of internal control.

In 2019–20, Defence will continue to mature its control functions – financial management, risk management, internal audit, inspector general and judge advocate – so that they can provide assurance to the Defence senior committees that Government-directed outcomes are being delivered in accordance with legislative and policy requirements.

Both the First Principles Review and the 2016 Defence White Paper highlight the importance of maintaining a balance between Defence strategy, capability and resources.

Key accountable and responsible officers will work together to ensure that enterprise financial management, corporate planning and performance management are aligned to support the Defence senior leadership and comply with the *Public Governance, Performance Accountability Act 2013* (PGPA Act).

Effective financial management ensures Defence uses Government-allocated resources to deliver Government-directed outcomes in accordance with the PGPA Act. The Chief Finance Officer has responsibility for ensuring appropriate financial governance within Defence.

Defence's financial stewardship is being enhanced to deliver a robust and strategic finance function that transitions the Department towards a more contemporary financial management approach. This will provide focus on process improvement, automation of transactional services, and building financial management capability across Defence. It will better balance control and assurance activities with a client-focused business partnering approach to financial management. This integration will facilitate effective communication to understand and connect to internal and external stakeholder requirements; and provide integrated controls for managing risks, supporting continued success in achieving compliance obligations.

In accordance with the PGPA Act, and in support of the Commonwealth Fraud Control Framework, Defence has instituted the Defence Fraud and Corruption Control Plan, which describes the fraud control framework to prevent, detect and respond to fraud. A focus for 2019–20 will be to develop our capacity to identify and manage enterprise-wide vulnerabilities and risk factors within a diverse operating environment.

Defence's Legal Framework

The *Defence Act 1903* sets outs the framework for the command and administration of Defence, including the role of the CDF to command the ADF.

The Secretary has all the rights, duties and powers of an agency head under the *Public Service Act 1999*, and is responsible for the Department and the ADF under the PGPA Act.

Head Defence Legal is accountable to the Secretary and the CDF for the provision, procurement and coordination of legal services across Defence, subject to the *Legal Services Directions 2017*, issued from time to time by the Attorney General, including:

- provision of effective and efficient legal service delivery
- establishment of standards and monitoring of service delivery performance for the legal services shared service function.

This ensures commanders and line managers receive the legal support they require to fulfil their accountabilities and deliver capability.

Risk Management

Risk management is an essential element in Defence's framework of good governance. Defence maintains a system of risk oversight and management to support its capability to achieve strategic objectives.

Defence recognises risk is inherent in its work and can present opportunities and threats to the achievement of its outcomes. Defence's risk management system aims to support the achievement of Defence's outcomes and ensure it is able to meet its risk management obligations in accordance with the *Public Governance*, *Performance and Accountability Act 2013* and the Commonwealth Risk Management Policy. All Defence personnel have a responsibility in managing risk, including complying with legislation, policies and delegations.

Risk appetite is the level of risk Defence is willing to accept to achieve its outcomes. Defence's risk appetite and tolerance is influenced by the nature of its activities, emerging priorities and changes in the environment. Defence generally prefers to accept low to medium levels of risk, so far as reasonably practical. However, due to its complex operating environment, Defence may need to manage higher levels of risk. Risk tolerance levels may also be reflected in Group and Service business plans.

An understanding of risks informs Defence's priorities, enables calculated risks to be taken when prudent to do so and allows Defence to identify and address issues that might otherwise jeopardise its capability and credibility. Effective risk management enables and supports innovation, the development of new ways of working and the proper use of public resources to achieve Defence outcomes.

Enterprise Risks are risks to the implementation of government decisions and achievement of Defence's required outcomes. They concern the operations of the organisation and may have internal and external causes. Defence has identified ten categories of enterprise risks: Capability, Estate, Finance, Information, People, Preparedness, Reform, Security, Stakeholder Engagement, Work Health and Safety.

Group and Service business plans identify risks to the achievement of Activities outlined in the Corporate Plan.

Defence also assesses Australia's strategic environment to identify potential **strategic risks** that could impact Defence and may require changes to Defence policy, strategic guidance, or force posture. Strategic risks may be managed as shared risks with Australian Government, international and industry partners.

In 2019-20, Defence will update its **risk management policy**, which outlines enterprise risk management expectations, accountabilities and responsibilities in the organisation.

Performance

This section sets out the intended results and high-level activities that contribute to Defence's purpose, including indicators of performance over the next four years. These should be read in conjunction with the Portfolio Budget Statements 2019-20, the Portfolio Additional Estimate Statements 2019-20, and the Defence Annual Report 2019-20.

Defend and protect Australia and advance its strategic interests

Portfolio Budget Statement 2019–20 Outcome Statement 1: Defend Australia and its national interests through the conduct of operations and the provision of support for the Australian community and civilian authorities in accordance with Government direction.

Defence plans for, develops and maintains the capability to deter and defeat armed attacks on Australia or on Australian interests. This includes planning for, conducting, controlling and evaluating Defence and/or coalition contributions to Government-directed operations.

Defence also supports the Federal, State and Territory governments with emergency and non-emergency tasks, as well as supporting events of national significance when requested by the Australian Government.

Portfolio Budget Statement 2019–20 Outcome Statement 2: Protect and advance Australia's strategic interests through the provision of strategic policy, the development, delivery and sustainment of military, intelligence and enabling capabilities, and the promotion of regional and global security as directed by Government.

Defence must provide high-quality, relevant and timely advice to Government on Defence strategy, capability and resourcing. Defence has implemented the 'strategic centre' model to ensure that all advice provided to Government is contested for alignment with Government strategic direction and to ensure the options being presented to Government support achievement of its Defence strategy, as described in the 2016 Defence White Paper.

The Government expects Defence to play an active role in contributing to regional security and stability, and to coalition operations around the world where our interests are engaged. Delivering on these requirements will require Australia to build on its strong network of bilateral and multilateral relationships. Through regular dialogue and practical cooperation, Defence is strengthening its engagement with partners to support shared responses to shared challenges.

Capability delivery is a core business process that enables Defence to perform its mission of defending Australia and its national interests now and into the future. Defence must procure capability efficiently and effectively. In 2019-20, Defence will continue building the new levels of capability required by Government and described in the 2016 Defence White Paper and the Integrated Investment Program. Major investments will enhance ADF capability to conduct operations to deter and defeat threats to Australia; operate over longer distances to conduct independent combat operations in our region; and make more effective contributions to multinational coalitions.

Australia's defence industry is a major partner in the Government's plans for current and future Defence capabilities. It is vital that Australia maintains a science and technology base and defence industry capable of supporting Defence's acquisition and sustainment requirements during peacetime and operations. A highly skilled and capable Australian defence industry is necessary for Defence to achieve its strategic objectives and deliver large-scale, complex projects and sustain military capability. Defence will work with industry to reflect a shared policy agenda that supports the growth and competitiveness of Australian businesses.

Intended Result 1. Defence meets operational capability requirements and supports the Australian community as directed.

Senior Committee Alignment: Chiefs of Service Committee

Steward: Vice Chief of the Defence Force

Defence plans for, develops and maintains the capability to deter and defeat armed attacks on Australia or against Australian interests. This includes planning for, conducting, controlling and evaluating Defence and/or coalition contributions to Government-directed operations.

Defence also supports the Commonwealth and State/Territory Governments with emergency and non-emergency tasks, as well as supporting events of national significance as directed by the Australian Government.

Defence will play an active role in contributing to regional security and stability, and to coalition operations around the world where our interests are engaged.

Activity	1.1 Conduct and sustain operations where our interests are engaged
Performance Criteria	Assessment of operations against directed outcomes agreed with Government
Target	All Government-directed outcomes are met
Timeframe	2019-23
Activity	1.2 Contribute to national security and support tasks
	1.2 Contribute to national security and support tasks Assessment of Defence support provided to contribute to whole-of-Government outcomes.
	Assessment of Defence support provided to contribute to whole-of-Government

Intended Result 2. Defence strategic, international and industry policy guides the design, development, integration and preparedness of Defence capability.

Senior Committee Alignment: Strategic Policy Committee **Steward:** Deputy Secretary Strategic Policy and Intelligence

Defence provides high-quality, coherent and timely policy advice to Government on Defence strategy, capability and resourcing. Defence is expected to assist the building of strong networks of bilateral and multilateral relationships. Through regular dialogue and practical cooperation, Defence will strengthen its engagement with partners to support shared responses to shared challenges.

The growth of Australia's defence industry is a key component of the Government's plans for current and future Defence capabilities. Australia must maintain a science and technology base and defence industry capable of supporting Defence's acquisition and sustainment requirements during peacetime and operations. Success will be a highly skilled and capable Australian defence industry, allowing Defence to achieve its strategic objectives and deliver large-scale, complex projects and sustain military capability. Defence will work with industry to reflect a shared policy agenda that supports the growth and competitiveness of Australian businesses.

Activity	2.1 Defence maintains future-focused strategic policy to guide Defence initiatives and address strategic risks.
Performance Criteria	Our strategic policy is regularly reviewed and updated.
Target	Defence strategic policy and risk review informs decision making to ensure strategy, capability and resources are aligned to Government priorities.
Timeframe	2019-23

Activity	2.2 Defence protects and advances Australia's interests globally to address current and future challenges.
Performance Criteria	Defence international engagement meets Defence International Engagement Policy objectives.
Target	Australia's strategic position is enhanced through international engagement by Defence.
Timeframe	2019-23
Activity	2.3 Defence engages industry to enhance support of sovereign capability.
Performance Criteria	Defence industry engagement meets requirements of the Defence Industry Policy Statement.
Target	Defence capability is enabled through industry and innovation.
Timeframe	2019-23
Activity	2.4 Defence maintains intelligence analysis and capability to deliver
	Government and Defence strategic objectives.
Performance Criteria	Defence intelligence outputs align with Government intelligence priorities.
Target	Intelligence services and capabilities are delivered according to Government priorities.
Timeframe	2019-23

Intended Result 3. The generation and sustainment of Defence capabilities achieves strategic planning objectives and preparedness requirements.

Senior Committee Alignment: Investment Committee

Steward: Vice Chief of the Defence Force

Defence will bring together key elements of investment to deliver and sustain Australia's defence capabilities, including equipment, infrastructure, information and communications technology, science and technology, and workforce. The design of the future force will be aligned with defence strategy, capability and resources, resulting in an affordable and balanced plan for a highly capable, agile and potent ADF and Defence capability that can meet future requirements. Key enablers of capability will be accorded appropriate priority in investment decisions.

Activity	3.1 Defence designs the future force to address strategic risks.
Performance Criteria	Our Future Joint force is designed, integrated and developed through the analysis of the future operating environment, development of potential responses and Government direction.
Target	The force-in-being and future force are designed and developed in accordance with strategic policy and risk.
Timeframe	2019-23
Porformanco Critoria	Stratagic research anables Defence to anticinate and exploit advances in science

Performance Criteria	Strategic research enables Defence to anticipate and exploit advances in science and technology for future Defence capability.
Target	Strategic research investments (including the Next Generation Technologies Fund) are creating disruptive scientific and technological opportunities for Defence.
Timeframe	2019-23

Activity	3.2 Raise, train and sustain Defence capabilities through the coordination of fundamental inputs to capability.
Performance Criteria	Defence's integrated capabilities, including workforce, are generated, trained and sustained to meet preparedness requirements.
Target	Forces meet preparedness requirements and are available for the conduct of operations and national support tasks.
Timeframe	2019-23
Performance Criteria	Joint enabling elements are generated and sustained at the required rate and standard to support the delivery of Defence capability.
Target	Joint enabling elements effectively support the delivery of Defence capability.
Timeframe	2019-23
Activity	3.3 Manage the investments required to realise the future force design through the Integrated Investment Program
Performance Criteria	Biannual Integrated Investment Program updates are agreed by Government.
Target	The Integrated Investment Program is delivered as agreed with Government.
Timeframe	2019-23
Activity	3.4 Manage the acquisition and sustainment of Defence equipment, supplies and services to meet Government and Defence requirements.
Performance Criteria	Assessment of acquisition projects delivery to meet Government and Defence requirements.
Target	Deliver Government approved acquisition projects to budget, schedule and agreed capability scope.
Timeframe	2019-23
Performance Criteria	Progress to deliver a sustainable, sovereign shipbuilding enterprise, as detailed in the Naval Shipbuilding Plan.
Target	The naval shipbuilding enterprise is designed and developed in accordance with the Naval Shipbuilding Plan and biannual updates to Government.
Timeframe	2019-23
Performance Criteria	Assessment of sustainment products delivery to meet Capability Manager requirements.
Target	Deliver sustainment products to meet Capability Manager requirements.
Timeframe	2019-23
Activity	3.5 Deliver science and technology research and development to enhance Defence capability.
Performance Criteria	Science and technology research supports Defence operations, sustainment and enhancement of current capability, and the development and acquisition of future capability.
Target	The balance of investments in science and technology activities are delivering outcomes in line with agreed Capability Manager priorities.
Timeframe	2019-23
Performance Criteria	Defence capability is enhanced by outreach and partnerships with the broader community, including publicly funded research agencies, academia, industry and allied international research agencies.
Target	Collaboration and outreach activities are delivering Defence capability in line with agreed Defence priorities.
Timeframe	2019-23

Intended Result 4: Strategy, capability, workforce and resources are balanced and aligned through One Defence systems, enabling Defence to anticipate, adapt and respond to changing priorities.

Senior Committee Alignment: Enterprise Business Committee

Steward: Associate Secretary

Defence will continue to develop a stronger and more strategic centre to provide clear direction and governance, better integrated and more customer-focussed corporate and enabling services, and a better planned, more professional workforce with a strong performance management culture. Defence has introduced a continuous improvement cycle to manage its ongoing reform journey, which is based around a central enterprise reform planning and reporting process.

Defence will reform capability acquisition and sustainment by focusing on how acquisition projects and sustainment services are managed; improve information and communications technology, including enterprise information management and enterprise resource planning; enhance service delivery, including reducing duplication of services, consolidating service entry points, improving staff satisfaction with customer services; and embed behavioural and cultural change across the Defence workforce.

The service delivery framework was refreshed in December 2018. The focus for the framework in 2019–20 involves standardising services, removing duplication of functions, professionalising the workforce and ensuring there are single, clear lines of ownership and accountability.

Activity	4.1 Deliver integrated, secure and fit-for-purpose enabling services
Performance Criteria	The delivery of services by enabling Groups is progressively integrated.
Target	Services are delivered in accordance with agreed measures.
Timeframe	2019-23
Performance Criteria	The management and sustainment of the Estate meets the requirements of the Capability Managers.
Target	The Defence Estate Strategy implementation plan is delivered as agreed.
Timeframe	2019-23
Performance Criteria	Defence's strategic centre sets priorities, manages resources and steers the organisation to implement Government policy and legislative requirements.
Target	Defence senior committees and accountable officers undertake informed decision-making to ensure strategy, capability and resources are aligned to highest priorities.
Timeframe	2019-23
Performance Criteria	Quality and timeliness of financial advice to the Minister, the Secretary and Chief of the Defence Force.
Target	Financial advice meets the Minister, Secretary and Chief of the Defence Force's requirements.
Timeframe	2019-23
Performance Criteria	Production of Defence's Budget and annual Financial Statements.
Target	Defence meets legislated financial requirements and timeframes.
Timeframe	2019-23

Activity	4.2 Resource, implement and review Defence's reform programs
Performance Criteria	Agreed reform programs, including legal services, enterprise resource management, security services, information management and strategic communications, are progressed as planned.
Target	Reform implementation plan milestones are met.
Timeframe	2019-23
Performance Criteria	Implementation of the six key cultural priorities.
Target	Cultural reform priorities are implemented as set out in the Pathway to Change: Evolving Defence Culture 2017-22 strategy.
Timeframe	2019-23
Activity	4.3 Develop and support the Defence workforce to enable required capability.
Performance Criteria	Defence's workforce has the agility and skills to meet current and future demand to deliver capability.
Target	Milestones within the Defence Strategic Workforce Plan and Total Workforce Model are implemented and critical skillset levels achieved.
Timeframe	2019-23
Performance Criteria	The workforce is safe and supported.
Target	Defence is compliant with Work Health and Safety legislation, regulations and standards to ensure the wellbeing of its workforce and members of the broader Australian community.
Timeframe	2019-23
Performance Criteria	Appropriate support and services are provided to Defence people and their families.
Target	Delivery meets appropriate standards, including welfare support, transition services and health services.

Activity	4.4 Deliver on the outcomes of its administered programs
Performance Criteria	Timely and accurate administration of the Administered Programs ³
Target	Administration meets agreed requirements.
Timeframe	2019-23

Timeframe

2019-23

Performance Criteria	Eligible ADF members continue to access the scheme.
Target	The scheme is consistently identified in surveys as a contributor to the retention of ADF personnel.
Timeframe	2019-23

Administered Programs include 2.14 Defence Force Superannuation Benefits, 2.15 Defence Force Superannuation Nominal Interest, 2.16 House Assistance and 2.17 Other Administered

Performance reporting

In line with the Enhanced Commonwealth Performance Framework, Defence enterprise performance management aims to provide a clear line of sight between:

- Corporate Plan (purpose, activities and intended results)
- Portfolio Budget Statements (allocation of resources to Programs to achieve Government outcomes and a forecast of expected performance)
- Annual Report, which includes
 - Annual Performance Statements (actual performance results for the financial year against the Corporate Plan and the Portfolio Budget Statements)
 - Financial Statements (actual financial position for end of financial year against the Portfolio Budget Statements and Portfolio Additional Estimates Statements).

To enable this clear line of sight, the 2019-20 Defence Corporate Plan informed the development of the Portfolio Budget Statements for 2019-20. Further alignment is pursued through internal Defence planning and performance management with Defence Groups and ADF Services under enterprise governance mechanisms, which support the operation of the One Defence Business Model.

Internal monitoring and reporting occurs at multiple levels to ensure appropriate management and alignment of resources to achieve intended results. This culminates in enterprise level reporting twice a year for Corporate Plan performance and risk monitoring and an end of financial year performance evaluation, which is reported both internally and externally via the Annual Performance Statements.

Internal assurance of performance is monitored by the Enterprise Business Committee. The Defence Audit and Risk Committee reviews the appropriateness of performance information included in the Portfolio Budget Statements, the Corporate Plan, and the Annual Performance Statements. Financial Statements are independently audited by the Australian National Audit Office. Defence aims to be transparent on its performance, however it should be noted that due to national security considerations, not all targets and performance information is available to be published.

The Defence Audit and Risk Committee provide written advice to the Secretary and the CDF on the appropriateness of the Defence's performance reporting as a whole, with reference to areas of concern or suggestions for improvement.

Defence's enterprise performance reporting is continuing to mature, to further enable improved performance and traceability in demonstrating the achievement of Defence's purpose in accordance with the requirements of the PGPA Act.



Defending Australia and its National Interests www.defence.gov.au



SDEFENCE WHITE PAPER

© Commonwealth of Australia 2016

ISBN: 978-0-9941680-5-4

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968* (Cwth), no part may be reproduced by any process without prior written permission from the Department of Defence.





► Table of Contents

Minister's Introduction	9
Executive Summary	13
Strategy	14
Australia's strategic outlook	14
Australia's defence strategy	17
Capability	18
A more capable, agile and potent future force	18
Australian defence industry and innovation	20
Shipbuilding	21
Defence posture – more active and internationally engaged	21
International engagement	22
Defence preparedness	22
People	23
Resources	24
Reform	24
Funding	24
Implementation	25
Chapter One: The Government's Approach to Defence	29
The purpose of this Defence White Paper	29
Why now?	
Managing strategic risk	32
Chapter Two: Strategic Outlook	39
Australia's security environment	30

The United States and China	41
The rules-based global order	44
The threat of terrorism and foreign terrorist fighters	46
State fragility	48
Military modernisation	49
Cyber and space	51
Regional security environments	53
Australia's borders and offshore territories	53
Our immediate neighbourhood	54
South East Asia	56
Indonesia	59
North Asia	60
South Asia and the Indian Ocean Rim	61
The Middle East	63
Weapons of Mass Destruction	64
Chapter Three: Australia's Defence Strategy	67
Australia's Strategic Defence Framework	68
Strategic Defence Interests	68
A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication	68
A secure nearer region, encompassing maritime South East Asia and the South Pacific	69
A stable Indo-Pacific region and a rules-based global order	70
Strategic Defence Objectives	71
Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches	

Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor-Leste and of Pacific Island Countries to build and strengthen their security
Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order
Implications for force structure and force posture
Chapter Four: The Future Australian Defence Force
Designing the future force
Capability priorities
Intelligence, Surveillance and Reconnaissance, Space, Electronic
Warfare, and Cyber Security
Maritime Operations and Anti-Submarine Warfare Forces
Strike and Air Combat
Land Combat and Amphibious Warfare
Key Enablers
Air and Sea Lift
Industry, innovation, research and development
A new approach to Australian defence industry policy108
A new approach to defence innovation
Shipbuilding113
Chapter Five: Positioning Defence for Tomorrow's Challenges
International engagement
International defence relationships120
The Australia-United States Alliance
New Zealand124
Indonesia 125

The South Pacific
Timor-Leste
South East Asia
North Asia
South Asia
Global relationships
Defence preparedness
Current operations
Chapter Six: People
Growing the integrated Defence workforce
Permanent Australian Defence Force146
Reserves
Australian Public Service
Recruiting the people we need
Developing our people
Retaining our people
Defence culture
Looking after our people
The Defence community
Delivering the future workforce
Chapter Seven: Reform of Defence
The First Principles Review – The Government's reform program 165
A strong strategic centre168
Capability development life cycle
Corporate and military enablers
Implementing the First Principles Review

Chapter Eight: Funding Defence	177
The Government's plan for funding Defence	177
The funding model1	177
How will Defence funding be spent?	181
Budgeting in Defence	182
Chapter Nine: Implementing this Defence White Paper.	185



Minister's Introduction

The 2016 Defence White Paper represents the Government's firm commitment to the Australian people that we will keep our nation safe and protect our way of life for future generations. This is a fundamental responsibility of the Australian Government; the safety and security of the Australian people and the defence of our territory and interests is our first and abiding priority.

The *2016 Defence White Paper* is the most rigorous and comprehensive in Australia's history — it is the culmination of a thorough process of review and assessment of Australia's security environment spanning the next 20 years.

Over the next two decades, we face greater security uncertainty and complexity, globally. This White Paper, together with the accompanying 2016 Integrated Investment Program and 2016 Defence Industry Policy Statement, sets out the Government's vision to enhance Australia's defence capability, deepen our international security partnerships and collaborate with defence industry and science and technology research partners in support of our nation's security.

The Defence White Paper presents the strong strategic argument for Australia's future defence based on seizing opportunities while managing strategic challenges. An important part of the Government's strategy is to continue to strengthen our alliance with the United States, as well as our other regional and international partnerships, to meet shared security challenges such as the pervasive threat of terrorism.

We have been careful in this White Paper to match our strategy and capability plans with appropriate resources. This is the first Defence White Paper to be fully costed, with external private sector assurance of the White Paper's investment plans. The Government will fund the White Paper goals by increasing the defence budget to two per cent of Australia's Gross Domestic Product by 2020–21, providing an unprecedented investment in Australia's defence capability of approximately \$195 billion over ten years.

The Australian Defence Force is already highly capable and respected for its professionalism world-wide. Our challenge is to maintain our capability edge and prepare for the more complex and high-tech conflicts of the future. To achieve this, the Government has prioritised the development of a more capable, agile and potent force structure. We will invest in modern space and cyber capabilities and the infrastructure, information and communications systems that support defence capability. Australian Defence Force personnel will continue to be appropriately trained, equipped and supported to undertake their diverse, critical roles.

The 2016 Defence White Paper sets out the most ambitious plan to regenerate the Royal Australian Navy since the Second World War. The White Paper reaffirms the Government's commitment to a strong, internationally competitive and sustainable Australian naval shipbuilding industry.

Key to the successful delivery and sustainment of our enhanced defence capabilities will be a new level of collaboration with Australian defence industry and science and technology research organisations. Positive new opportunities for enhanced collaboration and partnering between Defence and Australian defence industry will allow us to harness the leading-edge Australian innovation and technological expertise that can provide unique capability advantages for the Australian Defence Force. The Defence Industry Policy Statement accompanying this White Paper transforms the framework for effective engagement between Defence and defence industry.

The Defence organisation is undergoing a once in a generation level of change through implementation of reforms recommended by the First Principles Review of Defence. Successful implementation of this significant reform program, including a genuine commitment to effective cultural reform across Defence, will be critical to realising the Government's White Paper goals. Defence has made good progress in implementing cultural change and there is more to be done. A more diverse and inclusive workplace, with a focus on gender equality in professional development and progression opportunities, will be important to enhance the Defence organisation's capability and improve its standing as an employer of choice within the Australian community.

Our highly dynamic and interconnected world enables the Government to adopt an active and engaged approach in ensuring security and defence policy remains relevant and responsive. We will review our policy to meet the pace of change, through regular national security statements and defence updates to the Parliament. We will also ensure the availability and accessibility of current information on Defence's capability and industry plans and programs.

I am optimistic about Australia's future prosperity and security; the Government will continue to provide the direction and resources to protect and promote our nation and its interests, including through an enhanced capacity to shape Australia's security environment. I look forward to continuing an open dialogue with the Australian people as we implement this important White Paper.

Marise Payne

Minister for Defence



Executive Summary

This Defence White Paper explains how the Government is investing in Australia's defence capabilities to strengthen Australia's security in the more complex strategic environment Australia will face in the years ahead.

The Government's policy is to align Australia's defence strategy with capabilities and resourcing, grow our international defence partnerships to support shared security interests and invest in the partnership with Australian defence industry to develop innovative technologies and deliver essential capabilities.

Because decisions about our defence capabilities taken now will determine our capacity to manage the challenges of the future, it is important that defence decision making and planning take a clear long-term view. This Defence White Paper looks out to 2035 to identify where and what sorts of security challenges are likely to arise and what capabilities Defence — the Australian Defence Force (ADF) and the Department of Defence — will need to meet them. While Australia has effective defence capabilities to draw on to meet current security challenges, significant under-investment in Defence in the past and the deferral of decisions about future major capabilities need to be fixed. Defence's capability plans have become disconnected from defence strategy and resources, delaying important investments in Australia's future security and frustrating Australian defence industry.

In April 2014, the Government announced that it would deliver a new Defence White Paper to align Defence's strategy, capability and resources.

This Defence White Paper is based on a comprehensive review of Australia's strategic environment, including the changes underway in the Indo-Pacific region, encompassing the Indian Ocean to the Pacific Ocean, and across the world and the implications of these changes for Australia and for Defence. This includes an assessment of the different challenges created by the complex

dynamics between states and the ongoing threat posed by non-state actors, including terrorists that seek to launch attacks internationally, regionally and within Australia.

A fully-costed Force Structure Review underpins the Defence White Paper. The Force Structure Review assessed Defence's future capability needs and developed the force structure required to achieve Australia's defence objectives.

An Expert Panel supported the development of the Defence White Paper together with a comprehensive consultation process which incorporated input from across Government, Australian defence industry, the Australian public, the United States, New Zealand and our other international partners.

The Defence White Paper sets out in three sections the elements of the Government's defence policy in response to this comprehensive analysis and consideration: Strategy, Capability, and Resources.

Strategy

Australia's strategic outlook

Australia and the Indo-Pacific region are in a period of significant economic transformation, leading to greater opportunities for prosperity and development. Rising incomes and living standards across the Indo-Pacific are generating increased demand for goods and services. By 2050, almost half the world's economic output is expected to come from the Indo-Pacific. This presents opportunities to increase Australia's economy and security as the Indo-Pacific region grows in economic and strategic weight.

The growing prosperity of the Indo-Pacific and the rules-based global order on which Australia relies for open access to our trading partners are based on the maintenance of peace and stability. Over the last 70 years that peace and stability has been underpinned by a strong United States presence in our region and globally as well as active engagement by regional states in building a rules-based order.

Australia's strategic outlook to 2035 also includes a number of challenges which we need to prepare for. While there is no more than a remote prospect of a military attack by another country on Australian territory in the foreseeable future, our strategic planning is not limited to defending our borders. Our planning recognises the regional and global nature of Australia's strategic interests and the different sets of challenges created by the behaviours of countries and non-state actors such as terrorists.

The roles of the United States and China and the relationship between them will continue to be the most strategically important factors in the Indo-Pacific region to 2035. A strong and deep alliance is at the core of Australia's security and defence planning. The United States will remain the pre-eminent global military power and will continue to be Australia's most important strategic partner. Through this Defence White Paper, Australia will seek to broaden and deepen our alliance with the United States, including by supporting its critical role in underpinning security in our region through the continued rebalance of United States military forces.

The stability of the rules-based global order is essential for Australia's security and prosperity. A rules-based global order means a shared commitment by all countries to conduct their activities in accordance with agreed rules which evolve over time, such as international law and regional security arrangements. This shared commitment has become even more important with growing interconnectivity, which means that events across the world have the potential to affect Australia's security and prosperity. The Government is committed to making practical and effective military contributions to global security operations to maintain the rules-based order and address shared security challenges where it is in our interest to do so.

Australians will continue to be threatened by terrorism at home and abroad. The spread of extremism and violence will be worsened by foreign terrorist fighters returning from conflicts to their countries of origin, including Australia and other countries in our region, and terrorist attacks by individuals inspired and radicalised by extremist messages. Over the next 20 years, it can be expected

that terrorism will continue to evolve in ways which threaten Australia's interests

Australia is one of the most successful and most harmonious multicultural societies in the world. The highest priority of the Government is to keep the Australian community safe. To do this, the Government is working with our international partners and with Australian state and territory governments. The Government is committed to contributing to international efforts to meet the threat of terrorism, including maintaining Australia's significant contribution to the United States-led coalition to disrupt, degrade and ultimately defeat the terrorist threat from Daesh. Within Australia, Defence will provide important capabilities as part of our national counter-terrorism arrangements.

Instability in our immediate region could have strategic consequences for Australia and we will continue to take a leading role in providing humanitarian and security assistance where required. Within the South Pacific, variable economic growth, crime and social, governance and climate change challenges will all contribute to uneven progress and may lead to instability in some countries.

Maintaining Australia's technological edge and capability superiority over potential adversaries is an essential element of our strategic planning. The capability superiority that Australia has traditionally maintained in the wider region will be challenged by military modernisation. Over the next 20 years a larger number of regional forces will be able to operate at greater range and with more precision than ever before. The growth in the capability of China's military forces is the most significant example of regional military modernisation, but other countries are also undertaking extensive modernisation programs.

New and complex non-geographic security threats in cyberspace and space will be an important part of our future security environment. The cyber threat to Australia is growing. Cyber attacks are a real and present threat to the ADF's warfighting ability as well as to other government agencies and other sectors of Australia's economy and critical infrastructure.

Australia's defence strategy

The Government's defence strategy will ensure that Defence is prepared to respond if the Government decides the pursuit of Australia's interests requires the use of military force. This strategy sets out three Strategic Defence Interests which are of fundamental significance for strategic defence planning. To provide more detailed guidance for planning, each Strategic Defence Interest is linked to a Strategic Defence Objective which sets out the activities the Government expects Defence to be able to conduct if it decides to use military power in support of the Strategic Defence Interests.

Our most basic Strategic Defence Interest is a secure, resilient Australia. The first Strategic Defence Objective is to deter, deny and defeat any attempt by a hostile country or non-state actor to attack, threaten or coerce Australia. The Government is providing Defence with the capability and resources it needs to be able to independently and decisively respond to military threats, including incursions into Australia's air, sea and northern approaches.

Our second Strategic Defence Interest is in a secure nearer region, encompassing maritime South East Asia and the South Pacific. The second Strategic Defence Objective is to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor-Leste and of Pacific Island Countries to build and strengthen their security. In South East Asia, Defence will strengthen its engagement, including helping to build the effectiveness of regional operations to address shared security challenges, and the ADF will have increased capabilities to make contributions to any such operations. The Government will continue its commitment to strengthened regional security architectures that support transparency and cooperation. Australia will continue to seek to be the principal security partner for Papua New Guinea, Timor-Leste and Pacific Island Countries in the South Pacific.

Our third Strategic Defence Interest is in a stable Indo-Pacific region and rules-based global order which supports our interests. The third Strategic Defence Objective is to provide meaningful contributions to global responses

to address threats to the rules-based global order which threaten Australia and its interests. Australia will work closely with our ally the United States and other international partners to play an important role in coalition operations wherever Australia's interests are engaged.

Recognising the interconnected nature of the global environment and the fact that Australia's security and prosperity is directly affected by events outside our region, all three Strategic Defence Objectives will guide force structure and force posture decision-making in, and flowing from, this White Paper.

Capability

A more capable, agile and potent future force

The Government will ensure Australia maintains a regionally superior ADF with the highest levels of military capability and scientific and technological sophistication. The future force will be more capable, agile and potent. The future force will be more capable of conducting independent combat operations to defend Australia and protect our interests in our immediate region. This force will also enhance Australia's ability to contribute to global coalition operations.

More emphasis will be placed on the joint force, bringing together different capabilities so the ADF can apply more force more rapidly and more effectively when required.

To provide our forces with comprehensive situational awareness, the Government is strengthening Defence's intelligence, surveillance and reconnaissance capabilities. Defence's imagery and targeting capacity will be enhanced through greater access to strengthened analytical capability, enhanced support and space-based capabilities.

The Government will strengthen the Defence cyber workforce and systems to deter and defend against the threat of cyber attack.

Modernising our maritime capabilities will be a key focus. The submarine force will be increased from 6 to 12 regionally superior submarines with a high degree of interoperability with the United States. The surface naval capability will include three *Hobart* Class Air Warfare Destroyers and a new class of nine future frigates supported by new replenishment vessels. Defence's ability to contribute to border protection will be enhanced with the introduction of more capable offshore patrol vessels, new manned and unmanned aircraft and a new large-hulled multi-purpose patrol vessel, the Australian Defence Vessel *Ocean Protector*.

The ADF will be equipped with a potent air combat and air strike capability centred around the F-35A Lightning II and the E/A-18G Growler that builds on its current fleet of F/A-18 Super Hornet, Wedgetail Airborne Early Warning and Control and air-to-air refuelling aircraft. More air-to-air refuellers will be acquired to support future combat, surveillance and transport aircraft.

The land force will be equipped with new personal equipment for soldiers and a new generation of armoured combat reconnaissance and infantry fighting vehicles, as well as new combat engineering equipment. A new long-range rocket system will further enhance fire power, and armed medium-altitude unmanned aircraft will enhance surveillance and protection for the land force. The ADF's capacity for amphibious operations will be strengthened by the introduction of new weapons and equipment for our amphibious ships. New light helicopters will be acquired to support Special Forces operations.

To ensure the ADF is able to perform at the highest level of effectiveness, the Government will fix the underinvestment in the vital enabling capabilities that bind military capabilities together. The Government will upgrade ADF bases and logistics systems, including fuel and explosive ordnance facilities, and upgrade training and testing facilities, health services and information and communications technology.

The ADF's air lift capability will be increased to comprise 8 heavy lift C-17A Globemasters with additional heavy lift aircraft to be considered in the longer term, 12 upgraded C-130J Hercules, 10 C-27J Spartans and 10 CH-47F

Chinook helicopters. Sea lift capability will be strengthened by extending the life of and upgrading our current logistics ship.

With this Defence White Paper the Government has released for the first time a 10-year 2016 Integrated Investment Program, a detailed capability investment plan for the future force covering all of its major elements. It includes major acquisitions of new weapons, platforms and systems and investment in information and communications technology, infrastructure and the enabling workforce. The Integrated Investment Program is underpinned by a rigorous cost assurance program undertaken by private sector experts to provide higher levels of confidence that our plans are affordable.

Australian defence industry and innovation

The Government recognises the vital contribution to defence capability provided by Australian defence industry and science and technology research organisations. Australian defence industry provides a range of critical direct and support services and is a fundamental input to Defence capability. Innovation drives the development of defence capability. Defence, Australian defence industry and our national research community have a proven record of collaborating on leading-edge innovation that enhances the ADF's capability. This includes developing new technologies and transforming the maintenance of Defence capabilities.

The Government is committed to forming a new partnership with Australian defence industry to ensure Defence gets the equipment, systems and personnel it needs on time and on budget. The Government will strengthen Defence's collaboration with Australian defence industry, cut red tape and invest in new technologies to help build Australian defence industry competitiveness, create economic opportunity for Australians and support our nation's defence. The Government will better link our capability needs with Australian defence industry's capacity to deliver, and ensure that the decisions we make about defence capability take proper account of Australian defence industry.

With this White Paper the Government is releasing a new 2016 Defence Industry Policy Statement focused on maximising the defence capability necessary to achieve the Government's defence strategy. Fragmentation of current Australian defence industry programs will be addressed by consolidating numerous industry and innovation initiatives into two key initiatives that have clear and measurable outcomes for defence capability. The Government will streamline its approach to tendering and contracting to reduce red tape and make it easier for Australian defence industry to support Defence.

Shipbuilding

The Government's shipbuilding plans are based on long-term continuous builds of surface warships, commencing with construction in Australia of offshore patrol vessels from 2018 and future frigates from 2020. These plans will transform Australia's naval shipbuilding industry, generate significant economic growth, sustain Australian jobs over the coming decades and assure the long-term future of this key Australian defence industry.

The Government will ensure that the future submarine project provides a regionally superior capability and value-for-money for Australian taxpayers while maximising the involvement of Australian defence industry. The competitive evaluation process, which is underway, will provide a clear pathway for Australian defence industry to maximise its involvement in the project, without compromising capability, cost or the project schedule. More detail on the Government's shipbuilding plans are set out in Chapter Four.

Defence posture – more active and internationally engaged

The Government will reshape Defence's posture to ensure Defence is best positioned to protect Australia's security and prosperity. This includes strengthening Defence's international engagement and international defence relationships and arrangements, enhancing the ADF's preparedness and investing in upgrades to the ADF's basing and infrastructure.

International engagement

As Australia's strategic environment becomes more complex it is important to further develop our international partnerships including with our allies the United States and New Zealand, and with Japan, Indonesia, India, Singapore, the Republic of Korea, China and other key partners. Defence's international engagement is an important part of the Government's approach to building international partnerships, which also includes trade, diplomacy, foreign aid and economic capacity building in a range of government and non-government sectors.

Defence will increase its investment in international engagement over the next 20 years to help reduce the risk of military confrontation, build interoperability with key partners and improve the coordination of responses to shared international challenges including terrorism and humanitarian assistance and disaster relief.

International engagement will become an integrated core function across the entire Defence portfolio, aligned with the Strategic Defence Objectives. The Defence Cooperation Program, currently providing defence assistance to 28 countries, will be enhanced to build the confidence and capacity of our important regional partners. The ADF will participate more regularly in multinational exercises and the overseas presence of Defence personnel will be gradually increased over time.

Defence preparedness

Higher levels of Defence preparedness will be required to support increased ADF activity in the region, while maintaining the ADF's ability to make meaningful contributions to global security operations where our interests are engaged. The Government has directed an increase in the ADF's preparedness level, based on raising its overall capability and improving its sustainability on operations. More funding is being provided to ensure that the ADF has greater capacity and agility to respond to strategic risks.

People

The quality of our people is the foundation of Defence's capability, effectiveness and reputation. Defence is an integrated workforce with military and civilian personnel working together across the spectrum of Defence activities. All parts of the Defence workforce will need to upgrade their skills as part of building a more capable, agile and potent future force. To meet the demands of the higher-technology future force set out in this Defence White Paper, the Government will undertake the largest single rebalance of the Defence workforce in a generation.

The Permanent ADF workforce will grow to around 62,400 over the next decade to return it to its largest size since 1993. A new contemporary workforce management model will increase the ability of ADF members to move between the Permanent ADF and Reserves to better meet their individual circumstances and best harness their skills and expertise. This will provide ADF members with more opportunities to contribute to Australia's defence.

This Defence White Paper provides for a future Australian Public Service (APS) workforce of around 18,200 Full Time Staff Equivalent (FTE), down from 22,300 FTE in June 2012. This workforce will be rebalanced with around 1,200 new APS positions in areas critical to Defence's future capability, including intelligence, cyber security and space-based capabilities, offset by ongoing reductions elsewhere in the APS workforce.

The strength of Defence's leadership, and its ability to adapt and embrace a more diverse and inclusive culture, will be critical to attracting and retaining the workforce it needs for the future. Gender equality and increasing female participation in the Defence workforce and in senior leadership roles is fundamental to achieving Defence capability now and into the future. Defence has confronted the need for behavioural and attitudinal change with the release in 2012 of *Pathway to Change: Evolving Defence Culture*. The cultural change program continues to strengthen Defence's capability through creating an organisational climate focused on diversity and inclusion that will attract the best people for the job. Further details can be found in Chapter Six.

The Government is committed to investing in better health care systems for ADF members, including more medical personnel, and we will improve the links between Defence and the Department of Veterans' Affairs to better support current and former ADF members. Additional resources will provide more specialist mental health care, including for ADF Reservists and their families.

Resources

Reform

In August 2014, the Government commissioned the First Principles Review to ensure that Defence is appropriately structured and organised to meet the challenges of the future. Implementing the Review will ensure Defence becomes an integrated organisation driven by a stronger strategic centre rather than a federation of separate parts. The strategic centre will set priorities, manage resources and be responsible for steering the whole organisation to implement the Government's defence plans. The reforms are essential to delivering the Government's plans to implement the substantial force modernisation program set out in this Defence White Paper.

Funding

Central to the development of this Defence White Paper has been the Government's direction to align defence strategy, capability and resources. Addressing the growing gap between planning and resourcing by increasing defence funding will provide a sustainable basis for future investment and procurement decisions.

To deliver the capabilities set out in this Defence White Paper, the Government's long-term funding commitment provides a new 10-year Defence budget model to 2025–26, over which period an additional \$29.9 billion will be provided to Defence. Under this new budget model, the Defence budget will grow to \$42.4 billion in 2020–21, reaching two per cent of Australia's Gross Domestic Product (GDP) based on current projections.

The long-term nature of defence force structure planning, acquisitions and sustainment means this long-term funding commitment is critical to executing the Government's plans for Defence. The 10-year funding model is based on a fully costed future force structure, including its equipment, infrastructure and workforce, with external validation of those costs by private sector experts. This is the first time this has been done for a Defence White Paper. This program of external validation has provided assurance that our defence strategy is affordable and achievable within the budget that has been allocated.

Implementation

Implementation of this Defence White Paper will be driven by Defence's stronger strategic centre. The Minister for Defence will consider a formal strategic assessment of the alignment between Defence's strategy, capability and resources every six months to drive the Government's annual Defence budgeting and priority setting. These biannual reviews of our defence strategy and plans, including First Principles Review and cultural reform implementation, will ensure the Government and Defence have the flexibility to seize opportunities and manage risks as our strategic circumstances change.

Chapter Three: Australia's Defence Strategy

- 3.1 As outlined in Chapter Two, over the next two decades Australia's strategic outlook will change as the shift in global economic and political power to the Indo-Pacific continues. Australia is fortunate to be part of the most dynamic region in the world and we are benefiting from the economic transformation in the Indo-Pacific and the opportunities it is bringing to build Australia's prosperity. In order for Australia to continue to benefit from our region we will need to address the challenges of a more complex and uncertain strategic environment.
- 3.2 In response to this complex and uncertain strategic environment, the Government's strategic defence policy is to manage strategic challenges by: developing Defence's capabilities and agility to take a more active role in shaping regional affairs and to respond to developments which threaten our interests; while strengthening our alliance with the United States and developing our partnerships with other countries. This policy is articulated in the Government's new strategic framework for Defence to ensure the ADF is better prepared to respond if the Government decides the pursuit of Australia's interests requires the use of military force.
- 3.3 The new strategic framework is set out in the table below and explained in the rest of this chapter. The strategic framework explains why Australia's Strategic Defence Interests are of fundamental significance for Defence planning, what they mean for strategic defence planning Strategic Defence Objectives and how they will be reflected in the future Defence force structure.

Australia's Strategic Defence Framework

Strategic Defence Interests				
A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication.	A secure nearer region, encompassing maritime South East Asia and the South Pacific.	A stable Indo-Pacific region and a rules-based global order.		
Strategic Defence Objectives				
Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches.	Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor-Leste and of Pacific Island Countries to build and strengthen their security.	Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order.		

Strategic Defence Interests

3.4 The Strategic Defence Interests drive Australia's defence strategy. They set out that sub-set of Australia's national interests in a secure and prosperous Australia for which the Government may want to use its military power and guide the future development of Defence's capabilities.

A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication

3.5 Our most basic Strategic Defence Interest is a secure, resilient Australia.

This means a nation protected against attack or the threat of attack

and coercion and where Australia exercises full sovereignty over its territories and borders. A secure, resilient Australia extends into our northern approaches, our Exclusive Economic Zone, and our offshore territories, including our Southern Ocean and Antarctic territories. A secure, resilient Australia includes protection from non-geographic threats such as cyber attack, anti-satellite weapons and ballistic missile systems.

3.6 Our interest in a secure, resilient Australia also means an Australia resilient to unexpected shocks, whether natural or man-made, and strong enough to recover quickly when the unexpected happens.

A secure nearer region, encompassing maritime South East Asia and the South Pacific

- 3.7 Our second Strategic Defence Interest is in a secure nearer region. Australia cannot be secure if our immediate neighbourhood including Papua New Guinea, Timor-Leste and Pacific Island Countries becomes a source of threat to Australia. This includes the threat of a foreign military power seeking influence in ways that could challenge the security of our maritime approaches or transnational crime targeting Australian interests.
- 3.8 Instability or conflict in South East Asia would threaten Australia's security and our vital and growing economic relationships in that region. Stability in South East Asia is important to countering other threats including transnational crime and terrorism. Australia's reliance on maritime trade with and through South East Asia, including energy supplies, means the security of our maritime approaches and trade routes within South East Asia must be protected, as must freedom of navigation, which provides for the free flow of maritime trade in international waters.

A stable Indo-Pacific region and a rules-based global order

3.9 Our third Strategic Defence Interest is in a stable Indo-Pacific region and rules-based global order which supports Australia's interests. The Indo-Pacific includes North Asia, the South China Sea and the extensive sea lines of communication in the Indian and Pacific Oceans that support Australian trade. A stable rules-based regional order is critical to ensuring Australia's access to an open, free and secure trading system and minimising the risk of coercion and instability that would directly affect Australia's interests. A stable rules-based global order serves to deal with threats before they become existential threats to Australia, and enables our unfettered access to trading routes, secure communications and transport to support Australia's economic development.

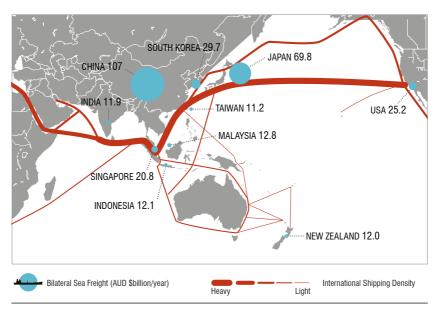


Figure 2: Sea Freight: Australia's top ten trading partners

Strategic Defence Objectives

- 3.10 To ensure Defence has the necessary force structure and force posture to defend and further Australia's Strategic Defence Interests, the Government has agreed to three equally-weighted high-level Strategic Defence Objectives to guide the development of the future force set out in this White Paper. The Strategic Defence Objectives outline the activities the Government expects Defence to be able to conduct if the Government decides to use military power in support of Australia's Strategic Defence Interests.
- 3.11 The Strategic Defence Objectives are to:
 - Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches.
 - Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor-Leste and of Pacific Island Countries to build and strengthen their security.
 - Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order.

Deter, deny and defeat attacks on or threats to Australia and its national interests, and northern approaches

- 3.12 In support of a secure, resilient Australia, the first Strategic Defence Objective is to deter, deny, and defeat any attempt by a hostile state or non-state actor to attack, threaten or coerce Australia.
- 3.13 While there is no more than a remote chance of a military attack on Australian territory by another country, Australians rightly expect that our military force be capable of the self-reliant defence of our territory from attack or coercion by another country. The Government is

providing Defence with the capability and resources it needs to be able to decisively respond to military threats to Australia, including incursions into our air, sea and northern approaches. Investment in Australia's military bases will be increased so they can support new capabilities that would be used to defeat any attack on our territory. Investment in our national defence infrastructure — including the Army, Navy and Air Force bases in northern Australia, including in Townsville and Darwin, as well as the Air Force bases Tindal, Curtin, Scherger and Learmonth — will be a focus of this Defence White Paper.

- 3.14 The Government is also providing Defence with enhanced domestic security capabilities to help respond to the threat of complex terrorist attacks within Australia. Australian states and territories lead the response to any attacks within their jurisdictions, but can request assistance from the Commonwealth as required, including the provision of specialist Defence support to prevent, assist in response to, and recover from a terrorism incident.
- 3.15 This specialised support includes: protection of Australia's offshore oil and gas infrastructure; special forces Tactical Assault Groups, which can rapidly deploy to support local law enforcement operations; explosive detection and disposal; contributing to security at major events (such as the G20 Leaders Summit in Brisbane in 2014); chemical, biological, radiological and nuclear response operations; and intelligence cooperation with other government intelligence and law enforcement agencies, to identify and disrupt foreign terrorist threats.
- 3.16 The Government will invest in the ADF's capabilities to ensure that it can continue to effectively contribute to domestic counter-terrorism operations. This includes enhancing the weapons, equipment, tactical mobility, and situational awareness of our Special Forces and strengthening Defence's intelligence and air lift capabilities.

- 3.17 Defence shares its responsibility for safeguarding the security of our maritime borders with other agencies, particularly the Department of Immigration and Border Protection. This Defence White Paper will provide Defence with the capabilities necessary to ensure its maritime border security responsibilities can be met. Defence will also need to be prepared to help protect Australia's offshore resource extraction activities, maintain Australia's sovereignty over our offshore territories and Exclusive Economic Zone and fulfil our international search and rescue obligations. The Government has acquired a new large-hulled multi-purpose patrol vessel, the Australian Defence Vessel *Ocean Protector*, in addition to HMAS *Choules*, to provide further capability to safeguard the security of our maritime borders.
- 3.18 Defence will continue to support the states and territories to respond to national disaster relief efforts. ADF personnel work alongside emergency response personnel in providing disaster relief. The Government will ensure the provision of specialist equipment, including air lift and supplies and coordination activities, to enable a close working relationship between Defence and state and territory emergency response services.
- 3.19 To counter the growing threat of cyber attack, the Government is improving our national cyber security capabilities. Defence's cyber security capabilities will be strengthened to protect the ADF's warfighting and information networks. Defence will contribute to the Government's enhanced national cyber security efforts, which include better coordinated cyber security capabilities and working with industry and academia to counter the threat of cyber attack.

Make effective military contributions to support the security of maritime South East Asia and support the governments of Papua New Guinea, Timor-Leste and of Pacific Island Countries to build and strengthen their security

- 3.20 The second Strategic Defence Objective is to work with the governments of South Pacific Island Countries to support stability in the South Pacific and to support the security of maritime South East Asia.
- 3.21 Australia will continue to seek to be the principal security partner for Papua New Guinea, Timor-Leste and Pacific Island Countries, by deepening our security partnerships, including through our Defence Cooperation Program. The most significant element of this program, the Pacific Maritime Security Program, will provide replacement patrol boats to 12 Pacific Island Countries from 2018.
- 3.22 The Government will work with Pacific Island Countries to strengthen their ability to manage internal, transnational and border security challenges, including natural resource protection, and to build their resilience to natural disasters. This includes working to limit the influence of any actor from outside the region with interests inimical to our own.
- 3.23 Protecting the lives of Australians abroad in our region is a priority for the Government. Defence must have the capability to conduct evacuation operations for Australians under threat in our immediate region and other areas as directed, whether in response to natural disasters or as a consequence of instability.
- 3.24 Defence must also be prepared to cooperate with Pacific Island Countries to conduct humanitarian assistance and disaster relief, security or stabilisation operations in our immediate region as it has done successfully in Solomon Islands and in Bougainville and in response to the devastation of Tropical Cyclone Pam in Vanuatu in

- March 2015. The ADF's enhanced maritime forces and amphibious capability set out in this White Paper means the ADF will have more capability and will be more responsive and flexible in providing assistance to our neighbours when requested.
- 3.25 Australia has a strong foundation of longstanding bilateral and multilateral partnerships with countries in South East Asia which have an interest in maritime security in the region. This includes Indonesia, Singapore, Malaysia, Brunei, the Philippines, Thailand and Vietnam. Defence will have enhanced capability to make meaningful contributions to operations addressing shared regional security challenges and humanitarian assistance and disaster relief efforts. Defence will help build the capacity of regional countries to respond effectively to security challenges through contributions to bilateral and multilateral activities such as exercises, training activities and the Defence Cooperation Program.
- 3.26 The Government will help shape security in the South East Asia maritime environment through a strengthened commitment to a strong security architecture that supports transparency and cooperation. This architecture includes the East Asia Summit, the ADMM-Plus and the ASEAN Regional Forum. Australia's Defence contributions to these forums will reflect the importance we place on the value of being active in regional institutions such as Australia's participation in all six ADMM-Plus Experts' Working Groups.

Contribute military capabilities to coalition operations that support Australia's interests in a rules-based global order

3.27 The third Strategic Defence Objective is to work closely with our ally the United States and other international partners to provide meaningful contributions to global responses to emergent threats to the rules-based global order that threaten Australia and its interests.

- 3.28 While Australia has sophisticated and growing military capabilities, Australia does not have the capacity to unilaterally protect and further our interests in maintaining a rules-based global order. Our current military contribution to the multinational United States-led Combined Maritime Forces in the Middle East region, targeting terrorism, piracy and drug smuggling, is an example of how we can address security threats to Australia by working with other like-minded partners. The ADF will continue to play an important role in coalition operations where Australia's Strategic Defence Interests are engaged including our role in international efforts to prevent the spread of weapons of mass destruction.
- 3.29 Australia will continue contributing to coalition operations with like-minded countries to combat terrorism. Our Special Forces, Air Task Group and Building Partner Capacity training mission will continue their role in the international coalition to defeat Daesh, with progress to be regularly reviewed. Future contributions to combat terrorism could draw on a range of defence capabilities, including combat capabilities, command, intelligence, communications or logistics.
- 3.30 Within the Indo-Pacific, future operations could include contributing to security in North Asia and helping to protect the extensive sea lines of communication that support Australian trade where our interests are sufficiently engaged. Australia will make important contributions to the provision of humanitarian assistance and disaster relief at short notice in the Indo-Pacific region or further afield when required.
- 3.31 Australia remains one of the most active supporters of the United Nations and Defence will continue to make tailored contributions to United Nations operations in the future where it is in Australia's interest to do so. In addition to possible contributions to peacekeeping operations, Defence will continue working with the United Nations to build its capacity to lead international efforts to respond to global

security challenges. Our efforts will include providing targeted funding and expertise to help the United Nations develop standards and training for its future peacekeeping operations.

Implications for force structure and force posture

- 3.32 To ensure Defence is capable of achieving the Strategic Defence Objectives, this White Paper sets out the types of forces that Australia will develop the force structure and the disposition and deployment of those forces the force posture.
- 3.33 The Government has directed Defence to use all three Strategic Defence Objectives to guide force structure and force posture decision making. The Government recognises the interconnected nature of the global environment and the fact that Australia's security and prosperity is directly affected by events outside our region and is not just linked to our geography or confronting threats solely in our maritime approaches. The direction to use all three Strategic Defence Objectives to guide decision making also recognises the reality that Australia has the responsibility and the capability to respond to threats to the rules-based global order. Over many decades, the ADF has deployed and will continue to deploy outside of our immediate region in concert with the United States and other like-minded partners, to pursue Australia's Strategic Defence Interests and in response to shared global challenges.
- 3.34 To be able to achieve the Strategic Defence Objectives, Defence will need to be more agile and adaptable with a broader set of capabilities from which to draw so that it is able to conduct the full range of tasks which might be required by Government. The ADF will also need to maintain a high degree of interoperability with the sophisticated capabilities which the United States deploys when it leads international coalitions to address global security challenges.

3.35 The Government expects Defence to be able to achieve the three Strategic Defence Objectives with the force structure and funding set out in this White Paper. This will require a balanced joint force structure and increased international cooperation and engagement. The Government's specific force structure decisions — based on the Strategic Defence Objectives — are outlined in Chapter Four. The priority placed on international defence cooperation and engagement to meet the Strategic Defence Objectives is discussed further in Chapter Five.



(DEFAULT.ASPX)

Search	Go	
NIAN (IO ATION)		
NAVIGATION ✓		

Home (/default.aspx) / About Us (/about-us.aspx) / Mission

Mission

(http://www.nato.int/cps/en/natohq/topics 113694.htm)

Resolute Support is a NATO-led, non-combat mission to train, advise and assist the Afghan National Defense and Security Forces (ANDSF). It was launched on 1 January 2015, following the conclusion of the previous NATO-led International Security Assistance Force (ISAF) mission, and the assumption of full security responsibility by the ANDSF. The Resolute Support Mission works closely with different elements of the Afghan Army, Police and Air Force.

The purpose of the Resolute
Support Mission is to help the
Afghan security forces and
institutions develop the capacity to
defend Afghanistan and protect its
citizens in a sustainable manner.

The Resolute Support Mission currently comprises around 17,000 personnel from 39 NATO Allies and partners countries. It operates with one 'hub' (Kabul/Bagram) and four 'spokes' (Mazar-e-Sharif in the north, Herat in the west, Kandahar in the south, and Laghman in the east). In addition to the train, advice and assist its purpose is to help the Afghan security forces and institutions:

- develop the capacity to defend Afghanistan
- protect its citizens in a sustainable manner



Resolute Support Mission focuses primarily on training, advice and assistance activities at the security-related ministries, in the country's institutions, and among the senior ranks of the army and police.

The mission performs supporting functions in several areas. These include:

- · operational planning;
- budgetary development;
- force generation process;
- management and development of personnel;
- logistical sustainment;
- civilian oversight (in order to ensure the Afghan security forces and institutions act in accordance with the rule of law and good governance).

149

NATO and its partners remain committed to Afghanistan and its people as they pursue a secure and stable future.

NATO is strongly committed to its mission in Afghanistan

(http://www.nato.int/cps/en/natohq/topics 8189.htm). NATO's support to Afghanistan is focused on three main areas:

- the NATO-led Resolute Support mission to train, advise and assist the Afghan security forces and institutions;
- funding of the Afghan security forces as part of a broader international effort;
- and the NATO-Afghanistan Enduring Partnership, which is being developed jointly with the Government of Afghanistan.

"Our aim is to strengthen the Afghan security forces so they can create the conditions for a peaceful solution. An Afghan-led and Afghan-owned peace process is essential to a long-term, inclusive political settlement."

- NATO Secretary General Jens Stoltenberg



ABOUT US

Mission

<u>History (/about-us/history.aspx)</u>

<u>Leadership (/about-us/leadership.aspx)</u>

RS Commands (/rs-commands.aspx)

is a NATO-led, Train, Advise and Assist mission



Since 2015, the Afghan National Defense and Security Forces have been responsible for Afghanistan's security



Our international effort has resulted in:

Factors	2001	2017
Gross Domestic Product 1 😂	\$2.46b	\$19.5b
GDP per capita 1 6	\$118	\$596
Life expectancy ²	46.2y	60.72y
Literacy ²	31.5%	38.4%
Girls in primary school 3 💮	0%	39%
Electricity ²	1%	43%
Clean water ²	32%	55.3%
Healthcare facilities 1 👚	496	2400
Internet users (PC) 4	0%	8.3%
Mobile phone users 4 🔝	0%	61.6%
Population ¹	20.1m	34.7m
Population in Kabul	500k	5m

1-World Bank 2-CIA Fact book 2001, 2015, 2017 3-Afghanistan Living Conditions Survey 2016-2017 4-Afghan Human Development Report 2016



(https://www.facebook.com/ResoluteSupport)



(http://twitter.com/resolutesupport/) Twitter (https://twitter.com/resolutesupport/)



(https://www.instagram.com/resolutesupport/) Instagram

(https://www.instagram.com/resolutesupport/)



(http://www.youtube.com/user/ISAFMEDIA) YouTube (http://www.youtube.com/user/ISAFMEDIA)

Copyright © 2019 Resolute Support | All Rights Reserved. | Powered by the eForum Factory (http://www.eforumfactory.be)



4

CHAPTER FOUR

Outcome 2



СН **04**

Outcome 2: The advancement of Australia's strategic interests through the conduct of military operations and other tasks as directed by the Government

Summary

The Australian Defence Force (ADF) advances Australia's strategic interests by planning for, and developing and maintaining, the capability to deter and defeat armed attacks on Australia; and by planning for, conducting, controlling and evaluating Defence and/or coalition contributions to government-directed operations. These operations include those that contribute to the security of the immediate neighbourhood (Programme 2.1) and those that support wider interests (Programme 2.2). Their objectives in relation to this outcome and current status are detailed in this chapter.

The ADF has contributed to maintaining a stable security environment where national programmes focus on peace, reconciliation, economic recovery, law and order and good governance across all ADF operations.

All deliverables and key performance indicators for Outcome 2 were fully met.

Table 4.1: Total cost of Defence Outcome 2[1]

	2014–15 budget estimate ^[2] \$'000	2014–15 revised estimate ^[3] \$'000	2014–15 actual result \$'000	Variation \$'000	on %
Programme 2.1 Operations Contributing to the Security of the Immediate Neighbourhood					
Revenue from other sources	-	-	-	-	-
Departmental outputs	3,008	4,022	7,290	3,268	81
Programme 2.2 Operations Supporting Wider Interests					
Revenue from other sources	3,269	3,827	10,452	6,625	173
Departmental outputs	349,721	784,980	510,818	-274,163	-35
Total resourcing					
Total departmental outputs	352,729	789,002	518,108	-270,895	-34
Total departmental revenue from other sources	3,269	3,827	10,452	6,625	173
Equity injection	-	-	-	-	_
Total resources for Outcome 2	355,998	792,829	528,560	-264,270	-33

Notes

- 1. This table excludes capital payments for outcomes.
- 2. As published in the Portfolio Budget Statements 2014-15, Table 37.
- 3. As published in the Portfolio Budget Statements 2015–16, Table 38.

Table 4.2: Net additional cost of operations

	2014–15 budget estimate ^[1] \$m	2014–15 revised estimate ^[2] \$m	2014–15 actual result \$m	Variation \$m
Operation Astute	-	-	0.1	0.1
Operation Slipper ^[3]	240.8	267.5	252.5	-15.0
Operation Manitou	52.0	52.0	39.4	-12.6
Operation Accordion	57.0	120.2	123.5	3.3
Operation Highroad	_	82.4	40.5	-42.0
Operation Resolute ^[4]	59.7	59.7	45.0	-14.7
Operation Okra	-	260.8	159.4	-101.3
Operation Anode	0.1	0.1	0.0	-0.0
Operation Southern Indian Ocean	3.0	3.0	1.1	-1.9
Enhanced Force Protection in Afghanistan ^[3]	16.2	16.2	_	-16.2
Defence Support to 2014 G20 Summit	8.0	8.0	3.5	-4.5
Total net additional costs	436.8	869.9	665.0	-204.9

- 1. As published in the Portfolio Budget Statements 2014-15, Table 4.
- 2. As published in the Portfolio Budget Statements 2015-16, Table 4.
- 3. Government supplementation for the Force Protection Review is included under Operation Slipper (Outcome 2) and Enhanced Force Protection in Afghanistan (Outcome 1).
- 4. Includes funding for expanded activities under Operation Sovereign Borders.

'I was one of the many who were fortunate enough to have received a ballot ticket to attend the Anzac Day Centenary Dawn Service at Gallipoli. The great sacrifice made by the diggers landing at Anzac Cove on the morning of 25 April 1915 was so graphically represented—with a flotilla of naval ships heading towards the cove through the sea haze, extracts from the diggers' letters on their first impressions on the landing being read, and being in the presence of the sheer steepness and harshness of the Gallipoli terrain. This is a memory that will remain with me forever.'

- Troy McKenzie, Defence Security Authority

Table 4.3: Net additional cost of operations from 1999–2000 to 2018–19

	1999–00 to 2013–14 actual result \$m	2014–15 actual result \$m	2015–16 budget estimate \$m	2016–17 forward estimate \$m	2017–18 forward estimate \$m	2018–19 forward estimate \$m	Total \$m
Operation Astute	4,311.9	0.1	-	-	_	-	4,312.0
Operation Bel Isi	47.7	-	-	-	-	-	47.7
Operation Slipper	6,924.8	252.5	121.9	103.9	-	-	7,403.1
Operation Manitou	-	39.4	43.2	2.2	0.5	-	85.3
Operation Accordion	_	123.5	191.0	1.4	0.6	-	316.5
Operation Highroad	-	40.5	115.1	11.3	7.9	-	174.9
Operation Resolute[1]	175.0	45.0	48.7	5.7	-	-	274.4
Operation Catalyst	2,364.5	-	-	-	-	-	2,364.5
Operation Okra	_	159.4	390.8	17.5	10.0	-	577.7
Operation Anode	355.2	-	-	-	-	-	355.2
Operation Sumatra Assist	44.5	-	-	-	-	-	44.5
Operation Acolyte	10.5	-	-	-	-	-	10.5
Operation Deluge	6.7	-	-	_	-	-	6.7
Operation Pakistan Assist	9.8	-	-	-	-	-	9.8
Operation Outreach	14.6	-	-	_	-	-	14.6
Operation Kruger	45.3	-	-	-	-	-	45.3
Operation Southern Indian Ocean	10.8	1.1	-	-	-	-	11.9
Enhanced Force Protection in Afghanistan	540.0	-	-	-	-	-	540.0
Defence Support to 2014 G20 Summit	0.1	3.5	-	-	-	-	3.6
Total net additional costs	14,861.5	665.0	910.7	142.1	19.1	-	16,598.3
Sources of funding for operations							
Government supplementation	13,230.7	660.3	910.7	142.1	19.1	-	14,962.8
Department of Foreign Affairs and Trade	9.1	-	-	-	-	-	9.1
Department of Defence (absorbed)	1,621.7	4.7	-	-	-	-	1,626.4
Total cost	14,861.5	665.0	910.7	142.1	19.1	-	16,598.3

Note

^{1.} Includes funding for expanded activities under Operation Sovereign Borders.

Helping out after Cyclone Pam

As part of a mission led by the Department of Foreign Affairs and Trade, Headquarters Joint Operations Command (HQJOC) executed and coordinated a major humanitarian operation in Vanuatu in March and April 2015.

Davs before the impact of the 14 March cyclone. **HQJOC** Domestic and Regional Operations Branch personnel were deep into the planning for an emerging humanitarian relief effort.

Royal Australian Navy Lieutenant Mark McKenzie, who was part of a small planning group, said the planning effort brought together Defence and government stakeholders to prepare for a range of possible scenarios.

Looking back on the impact of Cyclone Pam, a category five storm, on Vanuatu and surrounding islands, Mark emphasised that an effective HQJOC response to any emergency or disaster required an early appreciation of the situation.

'Deploying and coordinating any response effort is just one part of the puzzle. The Chief of Joint Operations relies on local ADF commands to provide the resources required for the initial response and then to identify potential commitment of non-local Defence assets', Mark said.

'Operation Pacific Assist came on the back of a busy three-month period that included coordination of support to bushfires in South Australia, Victoria and Western Australia, responding to cyclones Lam and Marcia in northern Australia and then the devastating earthquake in Nepal.

'As the deputy lead planner, Domestic and Regional Operations, my role was to assist in the coordination efforts of all branches and enablers to HQJOC in the development of the concept of operations.

'This included things like discussing the availability of assets within the Services, evaluation of possible response options, coordinating information through key staff and drafting of task orders.'



From 15 March through to mid-April, the ADF contributed to the whole-of-government response to assist more than 13,000 people with humanitarian relief.

More than 500 soldiers, sailors and aircrew deployed during Operation Pacific Assist, providing help across the archipelago and significantly assisting the recovery process.

ADF troops played a major part in the immediate relief effort, repairing key infrastructure, restoring basic services and delivering more than 115 tonnes of vital humanitarian assistance and disaster relief support throughout Vanuatu.

Through their efforts, access to clean water was restored, schools, community buildings and medical facilities were repaired, and remote communities had access to food and shelter.

ADF personnel also assisted in critical repairs to Port Vila Central Hospital, 27 schools, five clinics and 13 road and infrastructure sites.

'Being a staff officer integrated with the Operations Staff at HQJOC has been an incredible professional experience', Mark said.

'It's an amazing job when you consider we plan for just about every eventuality, but you're always prepared for the unexpected to occur.'

Programme 2.1

Operations Contributing to the Security of the Immediate Neighbourhood

Defence undertakes a variety of operations in order to preserve the security and stability in our region.

Operation Gateway, which occurs up to eight times a year, is an ongoing maritime surveillance operation conducted in the north-eastern Indian Ocean and the South China Sea to contribute to the stability of important sea lanes.

Operation Solania is an ongoing maritime surveillance operation to support Pacific Island countries in fisheries law enforcement in the South-West Pacific. There are up to four AP-3C Orion aircraft deployments per year to the region, to coincide with operations led by the Forum Fisheries Agency, which is based in Honiara, Solomon Islands.

Operation Render Safe is an enduring operation to dispose of explosive remnants of war in Pacific island nations. In November 2014, there was a significant operation on Bougainville, which disposed of more than 16 tonnes of explosives.

Operation Pacific Assist was an ADF deployment supporting humanitarian assistance and disaster relief in Vanuatu and Solomon Islands following Cyclone Pam. A significant Defence contribution included a major Navy ship, a number of Air Force transport and surveillance aircraft, Army rotary wing aircraft, and personnel from the three Services providing a Joint Task Force and heavy engineering support in disaster-affected areas.

Operation Nepal Assist was an ADF deployment supporting humanitarian assistance and disaster relief in Nepal following the earthquake in April 2015. ADF involvement included a strategic airlift of humanitarian aid stores, evacuation of affected Australian and approved foreign nationals and a small team deployed in support of the Australian Embassy.

Table 4.4: Programme 2.1 deliverables

Deliverable			Status
Operation	Commenced	Objective	
Gateway	1981	Conduct northern Indian Ocean and South China Sea maritime surveillance patrols.	• • • •
Solania	1988	Conduct South-West Pacific maritime surveillance patrols.	• 0 0 0
Render Safe	2011	Provide enduring explosive ordnance disposal support to the nations of the South West Pacific.	• • • •
Southern Indian Ocean	2014	Contribute to the search operations for the missing Malaysia Airlines flight MH370.	• 0 0 0
Saville	2014	Provide responses to non-allied foreign military activity in Australia's maritime approaches.	• • • •
Pacific Assist	2015	Support the whole-of-government contribution to the humanitarian and disaster relief operations as requested by the governments of Vanuatu and Solomon Islands.	• 0 0 0
Nepal Assist	2015	Support the whole-of-government contribution to the humanitarian and disaster relief operations as requested by the Government of Nepal.	• • • •

Table 4.5: Programme 2.1 key performance indicators

Key performance indicator	Status
ADF operations meet their stated objective within the Government's guidance.	• • • •
ADF forces are effectively deployed and sustained.	• • • •
ADF forces are withdrawn for reconstitution when they are no longer required.	• • • •

Programme 2.2

Operations Supporting Wider Interests

On 1 January 2015, Operation Highroad superseded Operation Slipper as the ADF contribution to the stabilisation and security of Afghanistan. Joint Operations Command transitioned its forces from a combat-focused mission to one that continues to provide directed capabilities and forces to the NATO-led Resolute Support mission. This contribution is delivered through the mentoring of the Afghan National Army personnel of 205 Corps in Kandahar and Officer Cadets at the Afghan National Army Officer Academy. Mentoring relationships have also been established with Afghan Special Forces and a small number of operational-level Afghan headquarters.

As part of a broader international humanitarian effort and whole-of-government approach, Joint Operations Command executed air operations and land force training as part of Operation Okra. These operations have degraded Daesh and protected Australia's national interests. Through the execution of the ADF's Build Partner Capacity mission, Iraqi land forces have increased their ability to conduct brigade-level offensive operations.

Under Operation Manitou, the Navy maintained the deployment of a major fleet unit in support of maritime counterterrorism, counter-narcotics and counter-piracy operations conducted by the Combined Maritime Force. Also in support of the Combined Maritime Force and the improvement of maritime security in the Middle East and along the east coast of Africa, Australia routinely commands Combined Task Force 150, which is responsible for the maritime counter-terrorism mission. The next Australian rotation will begin in November 2015.

HMAS Success was the first Navy ship to be assigned to a NATO operation—the counter-piracy operation Ocean Shield in the Gulf of Aden and Indian Ocean for two weeks from 23 March 2015. HMAS Success also achieved key national and Defence objectives in the commemoration of the Centenary of Anzac.

In support of a rules-based global security order, Defence continued to provide support to three United Nations missions—operations Paladin, Palate II and Aslan—and maintained its longstanding links to the Multinational Force and Observers mission in the Sinai, Egypt, under Operation Mazurka.

During 2014-15, ADF members continued to perform key roles in United Nations efforts to maintain peace and security in highly volatile areas such as Afghanistan, the Golan Heights, the Sinai and South Sudan. The ADF role included supporting free and fair elections in Afghanistan; directly contributing to peace-monitoring efforts in Israel, Lebanon and the Sinai Peninsula; contributing to reform in South Sudan; and assisting in humanitarian efforts to provide basic services and subsistence to those in need. It is envisaged that Defence will continue to support these United Nations missions and the Multinational Force and Observers in the Sinai in their critically important and globally significant work.

Operation Hawick was the ADF contribution to the whole-of-government Operation Bring Them Home in support of dealing with the aftermath of the Malaysia Airlines flight MH17 disaster in eastern Ukraine. Joint Operations Command supported the Combined Inter-Agency Task Force charged with carrying out the International Mission for Protection of Investigation, and supported the repatriation of victims of the disaster.

Met Substantially met Partially met Not met | See 'User guide' on page ii for full explanation.

Table 4.6: Programme 2.2 deliverables

Deliverable			Status
Operation	Commenced	Objective	
Paladin	1956	Contribute to the United Nations Truce Supervision Organization in the Middle East.	• • • •
Mazurka	1982	Contribute to the Multinational Force and Observers in the Sinai.	• 0 0 0
Slipper	2001	Support Afghanistan's security, development and governance. The International Security Assistance Force Mission in Afghanistan provided under Operation Slipper ceased on 31 December 2014.	• • • •
Palate II	2005	Provide a military liaison officer to the United Nations Assistance Mission in Afghanistan.	• 0 0 0
Aslan	2011	Contribute to the United Nations mission to the Republic of South Sudan.	• • • •
Manitou	2014	Contribute to international maritime security operations in the Middle East Area of Operations and international counter-piracy operations in the Persian Gulf, the Gulf of Aden, the Red Sea and parts of the Indian Ocean.	• • • •
Okra	2014	Conduct operations in support of the coalition response to the Iraq crisis.	• • • •
Accordion	2014	Provide support to operations Slipper and Manitou from within the Gulf States	• 0 0 0
Highroad	2015	Support Afghanistan's security, development and governance, through a contribution to the NATO-led 'train, advise, assist' mission.	• • • •

Table 4.7: Programme 2.2 key performance indicators

Key performance indicator	Status
ADF operations meet their stated objective within the Government's guidance.	\bullet \circ \circ
ADF forces are effectively deployed and sustained.	• 0 0 0
ADF forces are withdrawn for reconstitution when they are no longer required.	• • • •

ADF sends support to disaster victims in Vanuatu and Nepal

The Australian Defence Force's (ADF) response to the devastation brought by Cyclone Pam to Vanuatu in March 2015 saw more than 500 soldiers, sailors and aircrew deployed to provide assistance in the wake of the category five storm.

The ADF distributed 115 tonnes of vital humanitarian stores throughout Vanuatu. Through the efforts of ADF personnel, access to clean water was restored, schools, community buildings and medical facilities were repaired, and remote communities regained access to food and shelter.

The initial ADF response included the rapid delivery of Australian aid and emergency personnel using Air Force C-17A Globemaster strategic transport aircraft and C-130J Hercules aircraft. Air Force AP-3C Orion maritime patrol aircraft also provided reconnaissance support over Vanuatu and Solomon Islands to give emergency officials a clearer picture of the damage caused by the cyclone.

In addition to the support by Australian agencies, including the ADF, military support was provided by French, British and New Zealand defence forces. The ADF effectively coordinated its response efforts with emergency officials and other nations throughout the affected area.

The amphibious operations ship HMAS *Tobruk* deployed with Army engineers, vehicles and additional aid. On arrival, Tobruk provided the maritime base for much of the ADF's hightempo post-disaster recovery operations in the outer islands. Tobruk offloaded tonnes of stores using two LARC-V amphibious cargo vehicles, two LCM-8 landing craft and an embarked Navy MRH-90 multi-role helicopter.

Army engineers made a significant contribution to the citizens of the worst-affected southern

FEATURE



crew of HMAS Tobruk farewell members of the community of Dillon's Bay, Taféa province, Vanuatu, during Operation

Pacific Assist 2015

islands of Tanna and Erromango. Engineers provided immediate temporary shelter, access to clean water, and debris clearance and repairs to medical facilities.

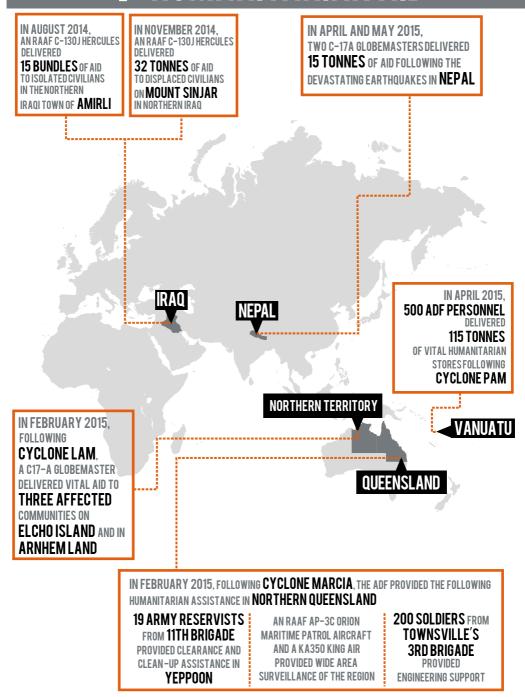
The Air Force flew more than 260 sorties in support of the mission. Air Force C-17A and C-130J aircraft and Army Black Hawk helicopters conducted evacuations of people from Vanuatu and flew aid, stores and personnel for the ADF, the Department of Foreign Affairs and Trade and other responding agencies, while Air Force KA350 King Air tactical aircraft provided interisland transport.

A month later, following the devastating earthquake in Nepal on 25 April 2015, the ADF delivered more than 13 tonnes of Australian aid and evacuated 106 Australian and other foreign nationals to Thailand.

Using two Air Force C-17A Globemaster III strategic airlift aircraft, aid supplied by the Department of Foreign Affairs and Trade was flown into Kathmandu's Tribhuvan International Airport. Civilian evacuees then boarded the aircraft and were flown out to Bangkok.

The Australian aid was delivered in cooperation with Nepalese aviation authorities, who managed the congested airport in Kathmandu following the earthquake.

iti HUMANITARIAN AID





Operation Highroad

The ADF's commitment to Afghanistan is known as Operation HIGHROAD and is fulfilled by personnel serving with the ADF's Task Group Afghanistan.



Task Group Afghanistan's Headquarters is

at Kabul's Hamid Karzai International Airport and comprises a command element of about 40 ADF personnel, which coordinates administration, communications and logistics support for all ADF members deployed to Afghanistan.

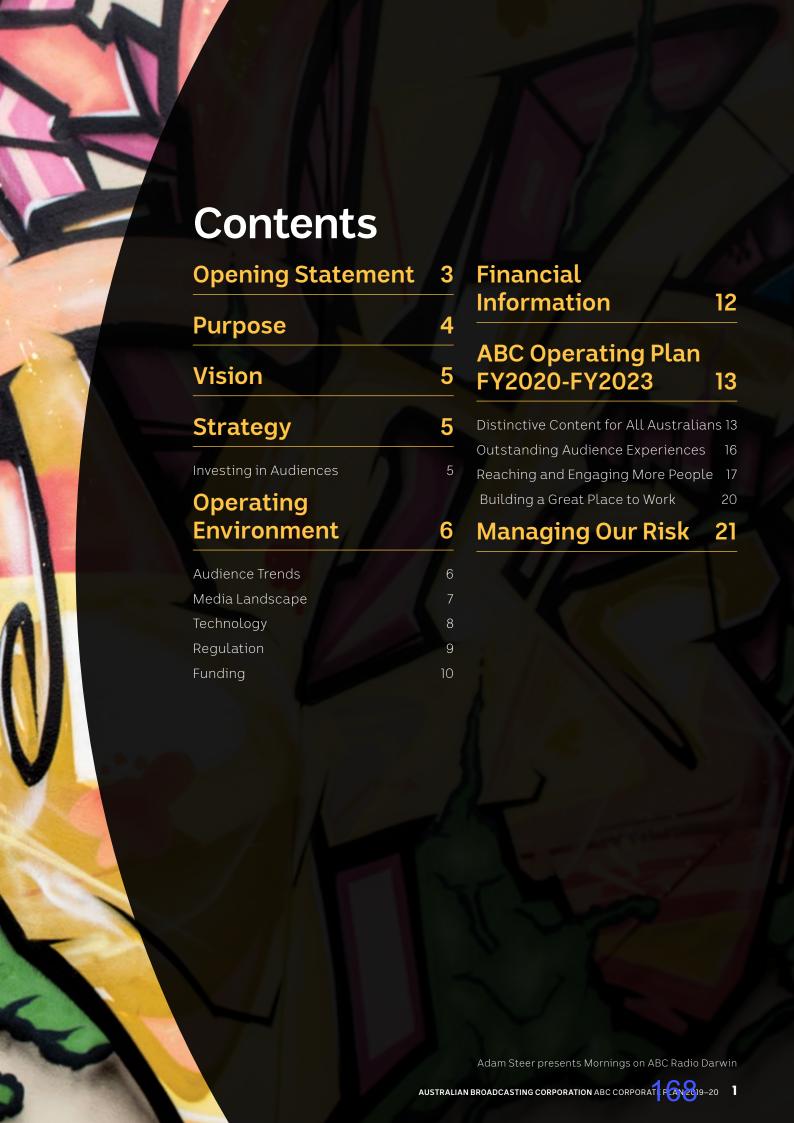
Australia remains committed to a stable and secure Afghanistan and continues to support the NATO-led train, advise and assist mission called Resolute Support which has replaced the previous NATO-led International Security Assistance Force (ISAF) mission.

Around 300 ADF members from the Royal Australian Navy, the Australian Army, the Royal Australian Air Force and Defence civilians are deployed in Afghanistan as part of Operation HIGHROAD.



2019-20







Opening Statement

The Board, as the accountable authority of the Australian Broadcasting Corporation, presents the 2019-20 Corporate Plan, prepared in accordance with section 35(1)(b) of the Public Governance, Performance and Accountability Act 2013 (Cth) (PGPA Act) and associated rules.

This Corporate Plan is prepared for the 2019-20 reporting period (FY20), and covers the reporting periods FY20, FY21, FY22 and FY23.

The ABC is accountable to the Australian Government through the Minister for Communications, Cyber Safety and the Arts.

As a Commonwealth entity, the ABC operates under the Australian Broadcasting Corporation Act 1983 (Cth) (ABC Act) and the PGPA Act. The PGPA Act sets the standards of governance, performance and accountability, with emphasis on use of public resources, planning, reporting and risk management.

The ABC is committed to meeting these requirements and its responsibilities as a cornerstone of Australian culture and the nation's independent and most trusted source of news and information.

The ABC Act and Charter are explicit about the importance of an independent public broadcaster to Australian culture and democracy. They drive the ABC to tell Australian stories for Australians and share their perspectives with the world.

The ABC also serves the public's interest through its commitment to, and defence of, rigorous journalism, press freedom and the public's right to know about the decisions and issues that shape their lives.

There has never been a more important time, or greater need, for the ABC.

Our strategy, outlined in this plan, reflects our focus on providing high-quality, distinctive content, on connecting communities and on delivering outstanding experiences for all Australians. To achieve this, we must continue to improve our technology and processes while continuing to be an innovative leader in the Australian media sector.

This plan sets out the challenges and opportunities we see over the next four years and provides details on the measures we will take to maintain the ABC's value and essential place in Australian life.



Ita Buttrose

Chair, Australian Broadcasting Corporation

Purpose

The ABC was established in 1932 and is one of Australia's most important civic and cultural institutions. It was built on the idea that all Australians should have access to news and entertainment services which served their needs and interests, beyond any commercial considerations. The ABC is now a public broadcaster of international renown and a much-loved part of Australian society and its cultural fabric. It delivers Australian stories and conversations across the nation.

While the country has changed significantly since 1932, the community's need for independent public service media is stronger than ever. The ABC's Charter, set out in section 6 of the ABC Act, states that the ABC must provide innovative and comprehensive broadcasting and digital services that inform, entertain and educate all Australians as well as contribute to a sense of national identity and share Australian perspectives with the world. In doing so, it must also reflect the diversity of interests and experiences of the Australian community.

Today, the ABC delivers services to all Australians across five national radio networks and four TV channels, international services for radio and TV, and a variety of streaming and other digital platforms, including iview and ABC Listen. Operating from 56 domestic and 11 international locations, the ABC's services and programs tell the nation's stories and help Australians understand their place in the world, connecting communities and touching the lives of millions of Australians every day.

The ABC is also Australia's largest creative employer. More than 2,000 content makers create distinctively Australian stories and programs with both broad and special interest appeal, and more than 800 journalists deliver the most trusted news service in Australia. Another 1,000 people work to make the ABC's content and services accessible to all Australians.

Through its people and services, the ABC makes a vital contribution to society by creating engaging and educational children's content and iconic dramas and documentaries that explore what it means to be Australian. It brings Australians together through coverage of national events and elections, and supports democracy through civic journalism that helps to keep industries and institutions accountable. The ABC discovers and celebrates Australian music and the arts, shares the wonders of science, and explores the culture and experiences of Indigenous Australians.

The ABC's purpose has lost none of its relevance, in spite of profound and radical change in the media environment. It continues to serve as a foundation for Australian media and remains one of the country's largest and most important cultural institutions. At the same time, as a voice for the Australian people, the ABC helps them to understand and navigate the world. Through initiatives like our *Navigating the* News media literacy project, the ABC strives to have a positive impact on the community. And, at times when extreme weather events stretch emergency services, the ABC is there, helping people to be prepared and to feel safe.

The loyalty of our audiences is crucial to our success. They trust us and we do our best to live up to their expectations. We value their support.

Vision

To be the independent source of Australian conversations, culture and stories.

Strategy

Investing in Audiences

The ABC's strategy contains four key objectives:



Creating distinctive content that matters for all Australians – We are committed to creating content that reflects our Charter obligations, delivering the services people expect and finding new and innovative ways to tell stories. Our aim is to deliver an ABC that looks and sounds like Australia, both in terms of its contents and teams.



Providing an outstanding audience experience -Meeting audience expectations is a top priority. We want audiences of every age to discover and enjoy more of what the ABC offers across TV, radio, websites, apps, podcasts and social media. We will continue to produce content that audiences can trust and rely on to keep them informed.



Delivering programs that reach and engage with more people – Broadcast and digital platforms will be used to shine a light on important issues through conversations and coverage that will contribute to a sense of national identity. We will explore new and innovative ways to engage with local and regional communities throughout Australia.



Building a great place to work – Our people are our greatest asset. In a supportive, creative environment they will continue to deliver the high-quality work for which the ABC is known and respected. We will build a culture of collaboration within the ABC and also outside the Corporation through local, national and international partnerships.



Operating Environment

Over the past decade, the way people consume content has transformed radically as digital innovation and global competition have disrupted the media landscape. Australians now have access to a wider range of platforms and greater choice of content than ever before.

The increasing demands for people's attention, from video-on-demand (VOD) services, social media, messaging apps, music streaming, podcasts, gaming, and other online activities, continues to challenge all media providers. In this environment, the ABC needs to find innovative ways to invest further in distinctive high-quality content and improve audience experiences.

Audience Trends

Audiences have embraced services that allow them to access content how, when, and where it suits them. Mobile viewing continues to grow, with almost a quarter of Australian smartphone users viewing long-form content on a regular basis.¹ Australians are also increasingly adopting internet-connected TVs and speakers – an estimated 13% of Australians own a home smart speaker² and 4.9 million access internet content via their TV each day.³

Nearly 14 million Australians have access to some form of subscription TV. More than 11.5 million Australians now have a Netflix subscription in their household.⁴ In this competitive media environment, where people can choose from huge volumes of international content, drawing audiences' attention to new Australian content is becoming increasingly difficult. Netflix's content catalogue contains thousands of titles, but it is estimated that only 1.6% of those are Australian.⁵

The viewing habits of children are also changing. Children have an abundance of choice when it comes to screen entertainment options. 61% of Australian children watch YouTube at least once a week, 42% watch Netflix or Stan, 20% use a Foxtel service and 38% watch free-to-air broadcast television. 37% of children use broadcaster VOD services at least once per week.6

ABC News SA presenters Jessica Harmsen and Emma Rebellato

More than 5.4 million Australians now use music streaming services available via websites or apps. Spotify is the clear industry leader, with nearly 3.6 million users in an average week.⁷ Research shows that 41.6% of triple j listeners also use music streaming website/apps, creating strong competition for audience attention.

AM listening is declining everywhere in the world, including Australia. Audiences for FM services have remained relatively steady over the past few years. Streaming services may replace broadcast listening for some audiences, but the need to maintain some broadcast services, including AM services, will continue for many years. The ABC is actively engaged with the radio industry, the Australian Communications and Media Authority (ACMA), and government to meet these needs into the future.

The popularity of podcasts is growing, and weekly podcast listening has increased from 10% of Australians in 2017 to 15% in 2019. Australia has the highest awareness of podcasting in the world at 83%².

The way people access news has also changed. The use of social media as a main source of news has remained relatively stable since 2018, but highlights a significant generational divide - almost half (47%) of 18-21 year-olds use social media as their main source of news, whereas only 3% of 73+ year-olds say it is their main source. Instead, older Australians are heavily dependent on TV for news8.

Demographics are also impacting on audience behaviours and interests. Australians are becoming more multilingual, with the proportion of people who speak a language other than English at home increasing, influencing their information and entertainment needs. Australians are reporting that their lives are busier; for example, an increasing proportion of couple families with children where both parents work means less time for traditional media consumption. There is a growing interest across all age groups (albeit largely driven by younger age groups) in health, wellbeing and mental health.

Media Landscape

Australians now have an abundance of content they can choose to listen to, watch or read. While innovation and globalisation have created new opportunities, for Australian media organisations, including the ABC, this also means audiences are fragmented and more difficult to reach.

The ABC continues to create high-quality, distinctive Australian content, but faces a challenge as Australian content becomes a smaller part of people's media diets. With audiences reducing the time they spend with broadcast radio and television, and spending more time using on-demand services, social media and games, the ABC faces an unprecedented level of competition for audience attention.

The video content market is already crowded and likely to become more so. Netflix and Amazon Prime continue to invest heavily in original content, with Netflix estimated to have spent US\$13 billion on content in 2018, and Amazon US\$5 billion. Disney has announced plans to launch a stand-alone SVOD product, Disney+, and new Warner Media platform, HBO Max, is also expected, as well as a service from NBC Universal. Apple and Facebook have each reportedly spent US\$1 billion on content in 2018, and YouTube remains a popular source of content with over 15 million monthly users in Australia.

The unprecedented global demand for content has seen a drain of talent from Australia, and Australian producers have shifted their business models to make programs directly for international audiences. These influences, together with an increase in production quality, have driven up the cost of making content.

The way organisations buy and sell content rights is also evolving. Traditional deals that covered exclusive distribution for agreed periods and platforms are disappearing in favour of territory rights. This further changes the economics of content-making and reduces residual revenue to producers and broadcasters.

Developments in audio are likely to evolve over the coming years. Music streaming, radio apps, podcasting, smart speakers, connected cars, and personalised services are changing listening behaviours. Greater commercialisation around such services may also mean that more premium audio content will require a paid subscription, much like the model operating for video.

Deloitte 2018 Mobile Consumer Survey

The Infinite Dial Australia, 2019 Edison Research and Triton Digital.

Device Ownership & Trends, iab Australia, January 2019

Roy Morgan Research, July 2019

Ramon Lobato and Alexa Scarlata. "Australian content in SVOD catalogues: availability and discoverability: 2018 edition", 14 October 2018, http://apo.org.au/sites/default/files/resource-files/2018/10/apo-nid196611-1121701.pdf.

Children's Television and Multi-Screen Behaviour, ACMA, August 2017

Roy Morgan Research, March 2019

University of Canberra, 2019

At the same time, the globalisation of media and the disruption of traditional revenue models threatens media diversity. Global competition means Australian news operators are now competing with international outlets. Traditional revenue for news operators has declined substantially, and the Australian Competition and Consumer Commission (ACCC) has raised concerns about the impact of Google and Facebook on the business models of news media9. The challenging operating conditions are resulting in staff cutbacks and consolidation, reducing the quality and diversity of news.

Increasingly, news organisations are turning to subscription models that support journalism, but restrict information to those willing and able to pay for it. Without widespread access to high-quality iournalism, power is not balanced with accountability and citizens are less informed. The ABC offers a vital independent news perspective that remains free for all Australians. The Corporation is working to ensure people can easily access personalised news content wherever and whenever they want.

The rise of digital news media has the potential to cause 'echo chamber' and 'filter bubble' effects, but the extent to which these occur across Australian audiences is not yet clear. Trust in media is a critical issue, and the level of perceived trust for news on social media is much lower than that for traditional news.

The challenging media environment and media consolidation activity has led to closures and consolidation around regional news outlets. The loss of these outlets amplifies the importance of ABC's regional content and presence and adds to the urgency of maintaining and further extending its regional services as well as supporting media diversity where it can.

In this environment, the ABC's news and current affairs content, which is highly trusted, and offers a distinctively Australian perspective, is more important than ever.

In Australia, there has been increasing government interest in using international media to communicate Australian views and values to people beyond its borders, and three Government reviews are currently underway, as discussed in the regulation section on page 10.

Technology

Rapid changes in the technology environment continue to create opportunities for media organisations, while also presenting challenges in adapting to digital platforms. Services for new platforms require new production tools and infrastructure for distribution. The ABC faces the need to move to cloud-based applications and file services, which are now required for efficient media production and multiplatform distribution.

Shifting activity to cloud services frees media organisations from the need to maintain their own dedicated servers, allowing them to increase or decrease their digital outputs in response to changing audience demands. Cloud services also enable the virtualisation of production, including new and more flexible tools for content creators, as well as support improved quality of service, disaster recovery and security.

Advances in technology have created the opportunity to make use of audience data to deliver improved audience experiences. Data collected about content use and audience behaviours enables media organisations to offer more personalised and relevant media experiences, which audiences now want and expect, and inform the commissioning of new programs and services. The use of such data also requires strong security measures to protect user privacy.

Meeting audience needs through such technologies demands continuous investment in production and distribution capabilities. It also unlocks other new technologies, such as machine learning and capabilities like speech recognition, which has given rise to smart speakers and other voice-based interfaces.

The ABC must adapt its own infrastructure and capabilities in line with these developments in order to meet audience expectations. At the same time, the ABC's established broadcast services must be maintained to ensure that all Australians can continue to access ABC services. Broadcast radio and television are expected to remain important for ABC audiences for at least another 20 years.

The transition from analogue to digital technologies in the 2000s led to a shortening of the lifespan of equipment throughout the media value chain. A similar transition is currently underway with the introduction of virtualised production and distribution technologies.

A growing proportion of the ABC's technological infrastructure is approaching end-of-life, as the Corporation has sought to extract the maximum value from its assets. Rather than engaging in a like-for-like replacement of capital, the ABC will seize the opportunity for modernisation presented by the technology transition which is currently underway. Shifting to a more automated or outsourced model in this way will allow the Corporation to improve efficiency and maximise the allocation of resources towards content and content-related activities.

Regulation

On 31 July 2019 the Government reintroduced the Australian Broadcasting Corporation Amendment (Rural and Regional Measures) Bill 2019. The Bill aims to ensure regional communities are provided for in the functions of the Corporation, and represented on the ABC Board. If passed, the Bill will amend the ABC Charter to include regional services, require the ABC Board to establish a new Regional Advisory Council, and create additional annual reporting obligations in relation to the Corporation's regional services.

In 2018/19 the Minister for Communications and the Arts provided the ABC with the report on the inquiry into the competitive neutrality of Australia's national broadcasters and the National Broadcasters Efficiency Review. The ABC is developing its response to these reviews.

The ABC is working closely with the Government and other stakeholders in relation to a number of other inquiries relevant to the broadcasting and digital sectors.

At the end of July 2019, these included:

- Digital Platforms Inquiry (Australian Competition and Consumer Commission). A review of the effects of digital search engines, social media platforms and other digital content aggregation platforms on competition in media and advertising services markets. The final report, released on 26 July 2019, proposed a number of regulatory interventions in digital markets and highlighted the need for stable and adequate funding for the ABC.
- Review of Australian Broadcasting Services in the Asia Pacific (Department of Communications and the Arts, Department of Foreign Affairs and Trade). A joint departmental review assessing the reach of Australian media services in the Region, including whether there is a role for shortwave radio.
- · Soft Power Review (Department of Foreign Affairs and Trade). Inquiry into Australia's 'soft power' capabilities, including international media services.

Advances in technology have created the opportunity for...

improved audience experiences

cloud services for flexibility, improved quality, security

virtualised production and distribution technologies

improved systems and processes and efficiencies

The Modern Slavery Act 2018 came into effect on 1 January 2019, and ABC Procurement is conducting a major review of the Corporation's supply chains to ensure ongoing compliance with its requirements.

The ABC's activities will continue to be influenced by changes in the regulatory environment. Any recommendations or outcomes from these reviews and inquiries are likely to affect the ABC, with the potential to alter the environment in which the Corporation operates.

Funding

The ABC faces a number of funding challenges. The ABC's funding base is declining in real-terms, production costs are rising, and investment is needed in new technologies to realise further efficiencies in production and distribution of content.

In an effort to maintain services, the ABC has pursued efficiencies across its back office functions, such as procurement. Accumulated savings over the 2014/15 to 2018/19 period total \$324 million. More than three quarters has been handed back to government, while \$70 million has been reinvested in new content for audiences. Further savings of this kind are becoming more difficult to find and may not be enough to meet all the challenges the ABC faces in the next four years. The need to find further savings may affect ABC services and jobs, as well as have an impact on its ability to deliver the initiatives outlined in this document.

The ABC's technology requires investment to replace end-of-life assets and it must adapt its infrastructure and capabilities to improve systems and processes and realise efficiencies.

Audiences are increasingly accessing content across multiple platforms and, as such, the cost of providing services to Australians is increasing. Historically, the ABC had a single distribution mode serving two device types – scheduled transmission to televisions and radios. In today's media landscape, to meet its Charter obligations and the expectations of the Australian community, the ABC's distribution must cater for multiple platforms and devices. The ABC must continue to invest in scheduled transmission to televisions and radios, as well as building on-demand and personalised distribution to smart televisions, computers, phones and tablets.

This extends to online news content across websites, news apps, social media and news messenger apps. The costs of developing and maintaining multiple platforms to serve multiple devices are increasing, while the cost of traditional transmission networks remains relatively constant. This is driving production costs overall to increase as content must be adjusted

to the specific requirements of each platform and device (for example, news bulletins must be made available through television, but that content must also be adjusted, and highlights packages created, for online news, social media and app versions of the story).

The internet may have changed media, but the ABC's role as a public broadcaster has not changed. It must continue to reach Australians with informative, educational and entertaining stories that reflect the cultural identity of Australia.

Increased competition in the Australian media landscape, especially from global distributors, is driving up competition for quality content. The average cost per hour of Australian TV drama has increased by approximately 3.3% per annum over five years and 6.5% per annum over the last three years. The level of the ABC's investment in production cannot match that of global players.

By using innovative deal structures and co-producing content with third parties, the ABC achieves greater initial value for money, and the ability to maintain content levels and quality despite lower budgets. However, the ABC often trades its distribution rights to investors when co-producing broadcast material, which limits the depth of content available for audiences on its on-demand platform and impacts its ability to later monetise that content.

Historically, the ABC would get 'passing traffic' as audiences channel-hopped to find something to watch or listen to, and content could be promoted cheaply through its own channels. In an online environment, the ABC can no longer rely on 'passing traffic' and content needs to be made discoverable, which requires increased investment in marketing and metadata. Other major providers are already responding to this with increased spending.

The ABC's unique commitment to servicing regional, rural and remote Australia places pressure on its cost structure. Providing localised content and emergency services during natural disasters to regional and remote areas is of vital importance and provides immense value to the community, but requires the ABC to incur additional costs to ensure delivery.



Financial Information

According to the Portfolio Budget Statements 2019-20, the ABC is appropriated funds to undertake two principal activities. These activities and the forward estimates are set out below:

1. Providing Australian and international audiences with radio, television and digital media services

Resources	2019-20 Budget	2020-21 Forward estimates	2021-22 Forward estimates	2022-23 Forward estimates
Program 1.1 – ABC General Operational Activities				
Expenditure (\$'000)	947,577	959,093	963,393	958,434

2. Managing the broadcast and transmission of ABC radio and television services within Australia

Resources	2019-20 Budget	2020-21 Forward estimates	2021-22 Forward estimates	2022-23 Forward estimates
Program 1.2 – ABC Transmission and Distribution Services				
Expenditure (\$'000)	183,699	186,595	190,088	193,647

A summary of financial information for the 2019-20 budget and the forwards estimates for the ABC is set out below:

Forward Estimates

Revenue	2019-20 Budget \$'000	2020-21 Forward estimates \$'000	2021-22 Forward estimates \$'000	2022-23 Forward estimates \$'000
ABC Government Appropriations				
Operational Appropriations	1,062,265	1,065 354	1,070,649	1,073,090
Total Appropriations	1,062,265	1,065,354	1,070,649	1,073,090
Own Source Revenue	57,881	57,718	57,703	57,693
Total Revenue	1,120,146	1,123,072	1,128,352	1,130,783
Operational Expenditure	1,131,276	1,145,688	1,153,481	1,152,081
Capital Expenditure	58,295	67,045	75,795	75,795
Borrowings	11,251	639	238	_

Note: the inclusion of this table satisfies the requirement of s.31B(1)(b) of the ABC Act in relation to forecasts of revenue and expenditure.

ABC Operating Plan FY2020-FY2023

Pillar I - Distinctive Content for All Australians

Delivering high-quality, distinctive content underpins and defines the ABC. The ABC's strategy has a clear focus on delivering content that reflects the diversity of Australian life and experiences and contributes to national identity. The ABC's priorities in meeting these goals over the current plan period are:

- · ensuring the ABC looks and sounds like the Australia it serves and represents
- · celebrating Australian culture in all its richness and diversity
- shining a light on important issues and hosting important national conversations
- · informing and entertaining audiences with high-quality specialist arts and educational content.

To achieve these goals over the next four years, the ABC will continue key activities, including:

- · investing in high-quality children's content, like Hardball and Bluey – contemporary tales that are inclusive, relatable and highly valued by children.
- producing compelling, original and distinctive drama, comedy and Indigenous content that reflects and celebrates Australian culture as international content continues to rise in volume and popularity.
- offering bold high-impact reporting, documentaries and factual programming that informs and stimulates national conversations and creates opportunities for Australian voices to be heard.
- delivering specialist content around genres such as religion and ethics, arts, education, sport, health, and science to explore and promote Australian culture, lifestyles, and the boundaries of knowledge.
- promoting Australian music and musicians through classical concert recordings and special events like the triple j's Hottest 100 and its regional One Night Stand concerts, ABC Classic's Classic 100, and Oz Music Month.

Over the coming four years, the ABC will also undertake a number of new initiatives to support its major goals. These include the following activities:

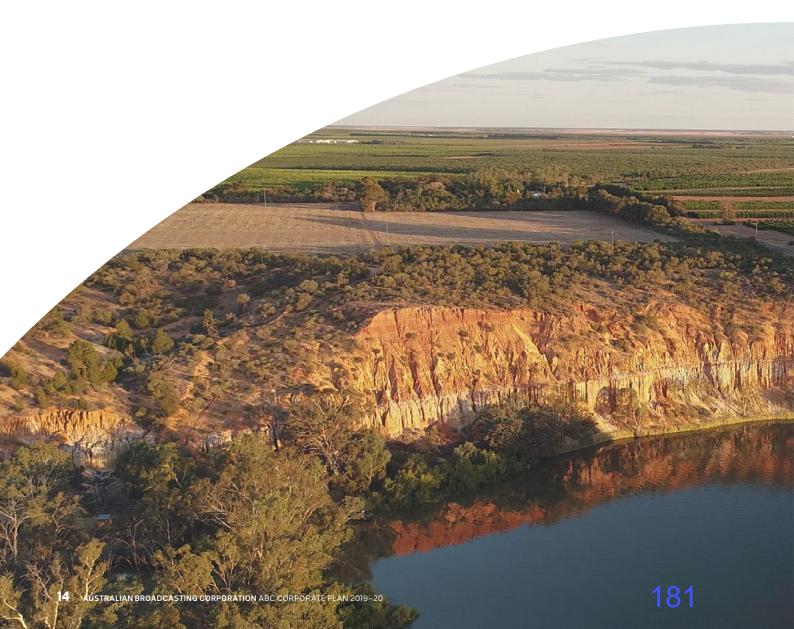
- A stronger focus on fostering relationships with local industry partners and a range of international distributors, broadcasters, public service media organisations and streaming platforms. The ABC will explore opportunities to find more cost-effective ways to deliver highquality content and support media diversity and the creative industries in Australia. These follow the announcement of the ABC partnership with the Canadian Broadcasting Corporation in June, which included content and co-production agreements for comedy, drama, and factual content.
- Maintaining the ABC's role as a trusted source of news and supporting democracy with a range of content and community initiatives across fact-checking and media literacy in schools across Australia. The ABC will also work with other public service media organisations globally to identify systems for content verification on social media platforms. These will be delivered in conjunction with the ABC's ongoing work to provide articles that break down and explain complex issues and deliver detailed policy analysis.
- Creating new educational resources around topics such as Indigenous cultures and histories, news literacy, financial literacy and science.
- Further promoting Australian music through more digital content for triple i, more music festivals, more regional concerts, an expanded Unearthed program, enhancements to Double I and the return of the popular music program The Set.

Pillar 1 Measures - Distinctive content for all Australians

Audience recognition of the high quality and distinctiveness of ABC programs indicates that the organisation is delivering on its core strategic goals. The trust with which Australians regard the ABC indicates the standard of its content at a time of declining trust in institutions and in media organisations in particular.

Measure	Source	2019-20	2020-21	2021-22	2022-23
Distinctiveness Unique market position	ABC Quality & Distinctiveness survey	82%	82%	82%	82%
Quality	ABC Quality & Distinctiveness survey	80%	80%	80%	80%
Supporting Australian Music	ABC Corporate Tracking study	72%	72%	72%	72%
Editorial Quality	Reviews commissioned or conducted by the ABC	Reviews undertaken and reports considered	Reviews undertaken and reports considered	Reviews undertaken and reports considered	Reviews undertaken and reports considered
Editorial Complaints Management	Data from Audience & Consumer Affairs	Complaints investigated and outcomes reported	Complaints investigated and outcomes reported	Complaints investigated and outcomes reported	Complaints investigated and outcomes reported

Outer years to be confirmed annually by the Board



Why this is important

The ABC is committed to commissioning and providing distinctive and high-quality content for Australians, including content that is differentiated from that provided by the commercial and community sectors in important, and often multiple ways. The ABC has set benchmarks across individual pieces of content to achieve an 82% score for distinctiveness and 80% score for quality.

The ABC is committed to supporting Australian music and artists. The ABC seeks to assess its performance through the results of the Corporate Tracking study which asks respondents to rate the ABC on its support of Australian music.

The ABC's commitment to high-quality content that meets its Charter obligations and editorial standards is an essential part of its obligations to the Australian public. The ABC has a detailed set of editorial policies, standards and guidelines, and regularly and systematically trains content makers in this area. This is underpinned by the conduct of regular, proactive reviews of ABC content to ensure these standards are met and to provide advice on ways to improve.

As well as conducting its own editorial reviews, the ABC has in place an effective independent complaints handling system which is transparent and responsive to any concerns raised by audiences. This is an essential tool to maintain and build the trust that is necessary for the ABC to fulfil its role as an independent, impartial and valued public broadcaster.



Pillar 2 – Outstanding Audience Experiences

Audiences are increasingly accustomed to accessing content when, where and how they want. This creates an imperative for the ABC to deliver content across a range of platforms and devices and provide the best audience experiences on each. The ABC must ensure that all Australians have access to ABC services, regardless of their location or socio-economic status. Its digital products must allow personalisation, be intuitive to use and make it easy to discover new content.

Currently, a small but not insignificant proportion of Australians don't have internet access at home, either as a fixed-line service or via a mobile device.10 There will be an ongoing need for the ABC to maintain broadcast services for Australians without access to internet services well into the future. Over the next four years, the ABC will make it easier for audiences to experience the full range of what the ABC offers across television, radio, online, mobile, smart devices and emerging platforms.

Initiatives in this area will include:

- Updating the ABC's digital products to better meet audience expectations, including personalisation, curation and localised content.
- Expanding the range and relevance of ABC content and developing the capabilities that will position the ABC to deliver services for a voice-activated world.
- Beginning the transition to cloud-based services to improve the flexibility and scalability of digital services, while also ensuring that systems and processes are robust in terms of maintaining privacy and data security. This will include a continuing focus on the speed and reliability of production and distribution systems.
- Investing more in content discovery through effective promotion of the ABC's content and services, ensuring that they stand out in a crowded market now dominated by international players.

Pillar 2 Measures – Outstanding Audience Experiences

Audience perceptions of their experience with the ABC and the trust they place in the public broadcaster indicate how well the ABC is delivering its services and fulfilling its purpose.

Measure	Source	2019-20	2020-21	2021-22	2022-23	Why this is important
ABC Experience	ABC Corporate Tracking study	48%	48%	50%	50%	The Exceptional Experience score is based on a percentage of audiences scoring 9s or 10s in relation to rating ABC content and products on a scale of 1 to 10.
Trusted Source	ABC Corporate Tracking study	81%	81%	81%	81%	In 2018-19, the ABC achieved a trusted score which was significantly stronger than other media providers, and will aim to maintain trust at above 80% through the plan period. Trust is something that can be only impacted by continuing to do a good job. It is a measure that is hard to build up, and can be very easy to drive down. As the most trusted news source, the ABC has the highest score in the market on this measure, and will be looking to maintain this lead over the plan period.

Outer years to be confirmed annually by the Board

Pillar 3 - Reaching and Engaging More People

The ABC is an invaluable part of the Australian media landscape and aims to connect with as many Australians as possible each day. It brings people together for national celebrations and conversations and contributes to local communities through its content and services. It provides vital information and support to Australians in times of disaster through emergency broadcasting. The ABC's international operations aim to encourage awareness of Australia and an understanding of Australian perspectives on world affairs.

The ABC will continue its efforts to reach and engage more people by:

- Connecting Australians through storytelling, events and conversations within and beyond their communities; reflecting the interests, concerns, and experiences of all Australians. This includes covering the events that bring us together, such as New Year's Eve and Anzac Day, and creating events where Australians can connect with the ABC and each other, such as Stargazing Live and triple j Hottest 100.
- Developing initiatives that support community resilience, particularly content that helps communities prepare for and navigate emergencies.
- Reaching culturally and linguistically diverse audiences in Australia and internationally with in-language content; connecting with those communities to amplify Australian stories, conversations and culture across the globe.
- Bringing national conversations to the broadest possible audiences, and bringing stories from regional communities to national audiences, as well as connecting Australians to their local communities.

Over the next four years, the ABC will also explore opportunities to further enhance its reach and relevance by:

- Delivering more news video content from, and for, the regions, including regional video news bulletins that will be available on-demand via iview and other apps and services.
- Enhancing its international services, including ABC Radio Australia, ABC Australia and ABC Australia iview; this may include opening up more digital access points for international audiences.
- Developing new creative and distribution partnerships that introduce ABC content to new audiences, especially younger audiences.
- · Finding new ways to support and engage with local communities and creating deeper two-way relationships with audiences.
- Exploring ways of working with other media outlets in regional Australia, especially around emergency broadcasting, content sharing, and story collaboration.
- Serving all Australians by reflecting and representing the diversity and perspectives of Australia's many communities in ABC's content and services and presenting a broad range of views in its coverage of issues.
- Committing to content that reflects Indigenous people, and their experiences and concerns, in the ABC's Elevate Reconciliation Plan 2019-21. This includes a commitment to producing content that brings Aboriginal and Torres Strait Islander Languages and stories into the national conversation.

Pillar 3 Measures - Reaching and Engaging More People

Reach measures the percentage of Australians who have used ABC services in a given time frame. This indicates the effectiveness of, and engagement with, ABC programming.

Measure	Source	2019-20	2020-21	2021-22	2022-23
Digital Engagement	Google Analytics	10.5 million Average weekly users	11.5 million Average weekly users	12.5 million Average weekly users	13.5 million Average weekly users
		24 minutes average time spent per user	25 minutes average time spent per user	26 minutes average time spent per user	26 minutes average time spent per user
Audience – reaching all Australians – Net weekly reach	OzTam (TV), GFK (Radio), ABC Corporate Tracking study (Digital).	70%	70%	70%	70%
Digital reach (weekly)	ABC Corporate Tracking study	23%	24%	26%	26%
Radio reach (weekly)	GfK Radio Ratings	36.5%	36.5%	36.5%	36.5%
Television reach (weekly)	OzTam	47%	44%	42%	41%

Outer years to be confirmed annually by the $\mbox{\sc Board}$

Access

Measuring access to ABC platforms provides a quantitative assessment of the ABC's ability to transmit to Australian audiences - via broadcast or digital services - in keeping with its purpose to provide a comprehensive public broadcasting service.

Measure	Source	2019-20	2020-21	2021-22	2022-23
Access to analog radio Access to digital radio Access to digital	Broadcast Australia data Australian Bureau of Statistics data	At least 99% 100% 100%	At least 99% 100% 100%	At least 99% 100% 100%	At least 99% 100% 100%
television Audience contacts – transmission issues	Reception line management System reports	Availability of reception advice line service			

Outer years to be confirmed annually by the Board

Transmission

Transmission of the ABC's radio and television content is provided by a third party and managed by the ABC via Transmission Service Agreements. The effective management of these agreements is fundamental to ensuring the ABC reaches and engages with as many Australians as possible.

Measure	Source	2019-20	2020-21	2021-22	2022-23
Transmission performance	Broadcast Australia data	At least 99% for all services	At least 99% for all services	At least 99% for all services	At least 99% for all services
Operation of transmission facilities	Broadcast Australia data	100%	100%	100%	100%

Outer years to be confirmed annually by the Board

Why this is important

People are increasingly accustomed to accessing content when, where and how they want. As they increasingly choose to access content on digital platforms, the ABC must ensure that it can continue to engage its audience regardless of platform.

Reaching all Australians is the key strategic indicator of ABC success. In 2017-18 the ABC reached 70% of Australians per week. There continues to be increased global competition and market fragmentation; however, the ABC strives to be relevant to all Australians. The goal is to therefore hold Net Weekly Reach flat.

As Australians' media consumption shifts from traditional broadcast platforms to digital, a growing digital footprint indicates continued relevance and engagement.

This measure includes all ABC owned platforms (ABC apps + websites).

While time spent listening to radio has declined, this decline has not been mirrored in weekly reach. Measurement also includes digital listening (streaming and apps), so the strategy of driving digital radio behaviours (ABC Listen/ Websites) is counted in the measurement footprint.

Television remains the best way to reach the majority of Australian audiences. Declines in this measure are expected, as weekly TV audiences are generally declining over time across all broadcast television.

Why this is important

Terrestrial and satellite delivered TV and radio services are still the main way Australian audiences access ABC content and these will be maintained over the planning period. As the ABC augments its terrestrial and satellite services with other digital and online services over time, the measures used for access to ABC content will be revisited to provide a consistent and integrated set of audience access measures.

Helping audiences to access its content is vitally important to the ABC. The ABC will continue to make information available to its audience on how to obtain access to the ABC's transmissions.

Why this is important

The ABC will continue to actively monitor the performance of its transmission contracts to maximise the availability of the services provided. As the ABC augments its terrestrial and satellite services with other digital and online services over time, the measures used for the availability of ABC content for audiences will be revisited to provide a consistent and integrated set of audience availability measures.

Pillar 4 - Building a Great Place to Work

The ABC's people are its greatest asset. Providing the best creative and supportive environment and encouraging a diverse and inclusive workplace for ABC teams are priorities.

Over the next four years, the workforce is likely to be influenced by a number of external factors, including the changing media and economic landscape in Australia and globally, with consequences for the ABC's ability to secure and retain talent. People's evolving expectations for flexibility and work-life balance, along with advances in technology will reshape how and where people work. Expanding digital capabilities will have consequences for the skills required of employees, and changing population demographics will evolve the ABC's workforce demographics.

Increasing employee engagement and creating a great place to work in the next four years will require the ABC to:

- evolve its content and workforce to look and sound like Australia and build an inclusive workplace
- provide learning and training opportunities to equip staff with appropriate skills for a changing work environment, including digital capabilities
- support employees by creating opportunities for flexibility and different ways of working
- · develop and nurture existing and emerging talent.

Specific initiatives in this area will include the following:

- In accordance with the ABC Diversity and Inclusion Plan 2019-22 and the ABC Elevate Reconciliation Action Plan 2019-22, the ABC will seek to recruit, develop and retain a workforce that reflects the diversity of the Australian community and to also foster an inclusive workforce culture.
- · Continuance and enhancement of the ABC's cadetships, internships and other early-career development initiatives across the organisation, to focus on under-represented groups, and develop the skills of the next generation of media practitioners. Recent program examples include the News Cadetship, Radio Internship, 2018/19 Media Cadetship Program and the 2018/19 Victorian Multiculturism Diversity Internship.

Pillar 4 Measures - Building a Great Place to Work

The progress towards building a great place to work and ensuring a creative environment can be gauged by the engagement of the people working within the public broadcaster. As Australia's largest creative employer, improvements in this measure indicate the ABC is becoming a more creative environment which in turn will enable even better content.

Measure	Source	2019-20	2020-21	2021-22	2022-23	Why this is important
Employee Engagement	Qualtrics – Project Averages	Within moderate range	Above median	Above median	Above median	Employee engagement surveys provide detailed data and insights for leaders and managers to use to improve the workplace. Organisation responsiveness to employee feedback leads to higher retention rates, lower absenteeism, improved productivity, higher service levels and better employee morale.

Outer years to be confirmed annually by the Board

Managing Our Risk

Our ability to reach and engage Australian audiences is crucial to our role as the National Broadcaster. Loss of audience is an ever-present risk. We are proud to be Australia's most trusted media organisation and value our reputation. Any loss of that trust is a key risk for the ABC.

The ABC's Board of Directors and management oversee and continue to be committed to developing and refining a fit-for-purpose risk management framework that will both protect and enhance value through the timely and accurate identification, assessment and management of all risks.

Risk Management Framework

The ABC faces a variety of risks that may have an impact on its performance, reputation and, more broadly, its social licence to operate.

These risks manifest themselves as a result of the strategic objectives that the ABC seeks to achieve and from the external societal, regulatory, political and market environment in which the ABC operates.

The ABC's risk management framework is designed to address this, by embedding a culture of risk awareness in all decisions throughout the Corporation.

The aim of the risk management framework is not necessarily to eliminate a risk, but rather to manage the risk to an approved level to generate an outcome that reinforces the strategic direction of the ABC.

We have in place and regularly test our broadcast, transmission and business continuity processes to ensure that we can be relied upon by our audiences at all times.

The ABC adopts what is commonly referred to as the 'three lines of defence' model for the management and assessment of risk.

The first line of defence is that all ABC employees own the responsibility for identifying and managing risks within Board-approved limits of authority and expenditure.

The second line of defence is the management and ongoing refinement of a robust risk framework and the development of efficient and effective internal controls by central support functions and an oversight management committee.

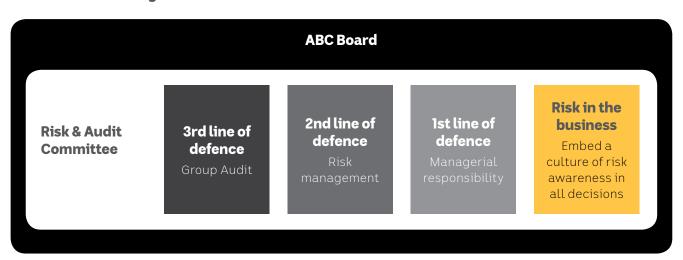
The third line of defence is the independent assurance by the ABC's internal audit team (Group Audit) of the existence, efficiency and effectiveness of internal controls relating to key risks.

The appropriateness and effectiveness of the risk management framework is overseen by the ABC Board and the Audit & Risk Committee.

The ABC risk team is responsible for the continued refinement of the ABC risk management framework. This includes providing counsel to the Board and management on how to identify, assess and manage risk.

As the ABC continues to evolve, the risk management framework will continue to be improved.

The ABC's Risk Management Framework



Principal Risks

Broadcast and digital service interruption

Preventing and minimising the impact of live broadcast interruption

Compliance

Ensuring compliance with editorial, contractual and regulatory requirements

Content relevance and value

Ensuring that content delivered is relevant and of value based on Charter and strong editorial decisions

Cyber security

Ensuring the robustness of ABC cyber defences and responses

Funding

Funding to deliver on the ABC Charter

Reputational damage

Managing the ABC's brand and reputation

Stewardship of public funds

Wise use of public funds

Strategic planning and communication

Ensuring the ABC responds to the rapidly changing media and technology environment

Workforce capability and management

The attraction, development and retention of a skilled workforce

Workplace health and safety

Delivering effective workplace health and safety practices including protective security

Ongoing Improvement

A defining element of any risk management framework is that it operates in an environment of ongoing iterative improvement. The ABC's Board has an expectation that each year there will be a significant improvement in how the ABC identifies, assesses and manages key risks. Over the lifecycle of the ABC's Corporate Plan strategies for improvement include:

- Continually enhancing the way we monitor and report risk.
- Undertaking root cause analysis through the ongoing recording and analysis of risk incidents. This forms the basis for close to real-time insights to the Board and management on the effectiveness of the risk management framework.
- The further development of a comprehensive program of risk-related learning and development for all employees which will support the enhancement of a positive risk culture and help maintain risk management capability across the ABC.

Greater focus is also being afforded to how the ABC adequately, and in a timely manner, gauges risk-focused cultural themes in areas such as risk awareness, managerial ownership of risk and proactive engagement in the management of risk. Disclaimer

This plan contains various long-range plans, projections, high-level estimates and other forward-looking information (Estimates). Those Estimates are based on the best considered professional assessment of present economic and operating conditions, present Australian Government policy and a number of assumptions regarding future events and actions which, at the date of this document, are expected to take place. The Estimates involve known and unknown risks, uncertainties and other factors beyond control that may cause the ABC's actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by the Estimates. Other than as required according to Reporting Obligations, the ABC is under no obligation to update the Estimates based on circumstances, developments or events occurring after the publication date of this document.





GPO Box 9994 in your state/territory capital

Phone 13 9994 Fax 02 8333 5344 TTY 1800 627 854 abc.net.au



code of practice 2011

(revised in 2016)

code of practice

l.	Regulatory Framework	1
II.	Scope of the Code	2
III.	Resolved Complaints	3
IV.	Principles and Standards	
	1. Interpretation	4
	2. Accuracy	4
7	3. Corrections and clarifications	5
/	4. Impartiality and diversity of perspectives	5
	5. Fair and honest dealing	7
	6. Privacy	8
	7. Harm and offence	8
	8. Children and young people	9
V.	Associated Standard:	

ABC Code of Practice 2011 (revised in 2016)

© Australian Broadcasting Corporation 2016
ISBN: 978-1-921832-06-2
700 Harris Street, Ultimo NSW 2007
abc.net.au



I. Regulatory Framework

The ABC Board is required, under section 8(1)(e) of the ABC Act, to develop a code of practice relating to its television and radio programming, and to notify this code to the Australian Communications and Media Authority ("the ACMA").

A complaint alleging the ABC has acted contrary to its Code of Practice in its television or radio programming may be made to the ABC. A complainant is entitled under section 150 of the *Broadcasting Services Act 1992* (Cth) ("the BSA") to take their complaint to the ACMA if, after 60 days, the ABC fails to respond to the complainant or the complainant considers the ABC's response is inadequate.

Section 150 of the BSA empowers the ACMA to investigate a complaint alleging the ABC has, in providing a national broadcasting service, breached its Code of Practice. The ACMA can decline to investigate the complaint under section 151 of the BSA if it is satisfied that the complaint does not relate to the ABC Code of Practice, or that the complaint is frivolous or vexatious or was not made in good faith.

The ACMA's jurisdiction under sections 150-151 does not encompass the ABC's print content or content disseminated by the ABC over the internet or through mobile devices. However, the ACMA has separate jurisdiction under Schedule 7 of the BSA in relation to content hosted on websites or transmitted through mobile services where that content is either "prohibited content" or "age-restricted content". The ACMA is empowered under Schedule 7 to require content service providers and content hosts to remove or prevent access to these types of content.

The ABC voluntarily complies with the *Content Services Code* developed by the Internet Industry Association and registered as an industry code with the ACMA under clause 85 of Schedule 7 of the BSA. The *Content Services Code* does not apply to content delivered through online or mobile services where that content has been previously transmitted on radio or television.

Except as expressly provided by the BSA, the regulatory regime established by the BSA does not apply to the ABC: section 13(5) of the BSA, and section 79 of the ABC Act.

¹ Prohibited content essentially involves content that is classified either as RC (Refused Classification) or X18+. This includes real depictions of actual sexual activity, child pornography, detailed instruction in crime, violence or drug use; and age-restricted content.

² Age-restricted content involves content classified as R18+ or MA15+ that is delivered through a mobile device or through a service that provides audio or video content for a fee. This type of content must be subject to a restricted access system, i.e. measures put in place to protect children under the age of 15 from exposure to unsuitable material. This category of content includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse language, and other material that is strong in impact.

II. Scope of the Code

The requirements of this Code are set out in the sections dealing with Interpretation and Standards in Part IV and the Associated Standard in Part V. The Standards in Part IV apply to radio and television programs broadcast by the ABC on its free-to-air television or radio broadcasting services. The Associated Standard in Part V applies only to television programs broadcast by the ABC on its domestic free-to-air television services.

This Code does not apply to any complaint which the ABC had decided not to investigate or, having accepted it for investigation, decided not to investigate further, where the ABC was satisfied that:

- the complaint concerns content which is or becomes the subject of legal proceedings;
- the complaint was frivolous or vexatious or not made in good faith;
- the complaint was lodged with the ABC more than six weeks after the date when
 the program was last broadcast by the ABC on its free-to-air radio or television
 services, unless the ABC accepted the complaint for investigation after being satisfied
 that it was appropriate to do so, having regard to:
 - the interests of the complainant in the subject matter of the complaint:
 - the seriousness of the alleged breach;
 - the reason(s) for the delay;
 - the availability of the program content which is the subject of the complaint; and
 - any prejudice the delay may otherwise have on the ABC's ability to investigate and determine the matter fairly; or
- the complainant does not have a sufficient interest in the subject matter of the complaint, where the complaint alleges a breach of Fair and honest dealing (Standards 5.1-5.8) or Privacy (Standard 6.1).

To avoid any doubt, the ABC intends that any complaint falling within the terms of any one of the above categories is not relevant to the ABC Code of Practice, for the purposes of section 151(2)(b) of the BSA. In effect, this means that only complaints which the ABC has accepted for investigation in accordance with the above criteria are eligible under this Code to be reviewed and investigated by the ACMA.



III. Resolved Complaints

The ABC seeks to comply fully with the Code and to resolve complaints as soon as practicable.

A failure to comply will not be a breach of the Code if the ABC has, prior to the complaint being made to the ACMA, taken steps which were adequate and appropriate in all the circumstances to redress the cause of the complaint.

To illustrate, a failure to comply with Standards 2.1 or 2.2 (Accuracy) will not be taken to be a breach of the Code if a correction or clarification, which is adequate and appropriate in all the circumstances, is made prior to or within 30 days of the ABC receiving the complaint.

IV. Principles and Standards

1. Interpretation

In this Code, the Standards must be interpreted and applied in accordance with the Principles applying in each Section. From time to time, the ABC publishes Guidance Notes which do not in themselves impose obligations on the ABC, but which may be relevant in interpreting and applying the Code.

The Standards in Parts IV and V are to be interpreted and applied with due regard for the nature of the content under consideration in particular cases. The ABC is conscious that its dual obligations – for accountability and for high quality – can in practice interact in complex ways. It can be a sign of strength not weakness that journalism enrages or art shocks. The Standards are to be applied in ways that maintain independence and integrity, preserve trust and do not unduly constrain journalistic enquiry or artistic expression.

2. Accuracy

Principles: The ABC has a statutory duty to ensure that the gathering and presentation of news and information is accurate according to the recognised standards of objective journalism. Credibility depends heavily on factual accuracy.

Types of fact-based content include news and analysis of current events, documentaries, factual dramas and lifestyle programs. The ABC requires that reasonable efforts must be made to ensure accuracy in all fact-based content. The ABC gauges those efforts by reference to:

- the type, subject and nature of the content;
- the likely audience expectations of the content;
- the likely impact of reliance by the audience on the accuracy of the content; and
- the circumstances in which the content was made and presented.

The ABC accuracy standard applies to assertions of fact, not to expressions of opinion. An opinion, being a value judgement or conclusion, cannot be found to be accurate or inaccurate in the way facts can. The accuracy standard requires that opinions be conveyed accurately, in the sense that quotes should be accurate and any editing should not distort the meaning of the opinion expressed.

The efforts reasonably required to ensure accuracy will depend on the circumstances. Sources with relevant expertise may be relied on more heavily than those without. Eyewitness testimony usually carries more weight than second-hand accounts. The passage of time or the inaccessibility of locations or sources can affect the standard of verification reasonably required.



The ABC should make reasonable efforts, appropriate in the context, to signal to audiences gradations in accuracy, for example by querying interviewees, qualifying bald assertions, supplementing the partly right and correcting the plainly wrong.

Standards:

- 2.1 Make reasonable efforts to ensure that material facts are accurate and presented in context
- **2.2** Do not present factual content in a way that will materially mislead the audience. In some cases, this may require appropriate labels or other explanatory information.

3. Corrections and clarifications

Principles: A commitment to accuracy includes a willingness to correct errors and clarify ambiguous or otherwise misleading information. Swift correction can reduce harmful reliance on inaccurate information, especially given content can be quickly, widely and permanently disseminated. Corrections and clarifications can contribute to achieving fairness and impartiality.

Standards:

- **3.1** Acknowledge and correct or clarify, in an appropriate manner as soon as reasonably practicable:
 - a. significant material errors that are readily apparent or have been demonstrated; or
 - b. information that is likely to significantly and materially mislead.

4. Impartiality and diversity of perspectives

Principles: The ABC has a statutory duty to ensure that the gathering and presentation of news and information is impartial according to the recognised standards of objective journalism.

Aiming to equip audiences to make up their own minds is consistent with the public service character of the ABC. A democratic society depends on diverse sources of reliable information and contending opinions. A broadcaster operating under statute with public funds is legitimately expected to contribute in ways that may differ from commercial media, which are free to be partial to private interests.

Judgements about whether impartiality was achieved in any given circumstances can vary among individuals according to their personal and subjective view of any given matter of contention. Acknowledging this fact of life does not change the ABC's obligation to apply its impartiality standard as objectively as possible. In doing so, the ABC is guided by these hallmarks of impartiality:

- a balance that follows the weight of evidence:
- fair treatment:

- open-mindedness: and
- opportunities over time for principal relevant perspectives on matters of contention to be expressed.

The ABC aims to present, over time, content that addresses a broad range of subjects from a diversity of perspectives reflecting a diversity of experiences, presented in a diversity of ways from a diversity of sources, including content created by ABC staff, generated by audiences and commissioned or acquired from external content-makers.

Impartiality does not require that every perspective receives equal time, nor that every facet of every argument is presented.

Assessing the impartiality due in given circumstances requires consideration in context of all relevant factors including:

- the type, subject and nature of the content;
- the circumstances in which the content is made and presented:
- the likely audience expectations of the content;
- the degree to which the matter to which the content relates is contentious;
- the range of principal relevant perspectives on the matter of contention; and
- the timeframe within which it would be appropriate for the ABC to provide opportunities for the principal relevant perspectives to be expressed, having regard to the public importance of the matter of contention and the extent to which it is the subject of current debate.

Standards:

- **4.1** Gather and present news and information with due impartiality.
- 4.2 Present a diversity of perspectives so that, over time, no significant strand of thought or belief within the community is knowingly excluded or disproportionately represented.
- 4.3 Do not state or imply that any perspective is the editorial opinion of the ABC. The ABC takes no editorial stance other than its commitment to fundamental democratic principles including the rule of law, freedom of speech and religion, parliamentary democracy and equality of opportunity.
- **4.4** Do not misrepresent any perspective.
- **4.5** Do not unduly favour one perspective over another.

5. Fair and honest dealing

Principles: Fair and honest dealing is essential to maintaining trust with audiences and with those who participate in or are otherwise directly affected by ABC content. In rare circumstances, deception or a breach of an undertaking may be justified. Because of the potential damage to trust, deception or breach of an undertaking must be explained openly afterwards unless there are compelling reasons not to do so.



Standards:

Dealing with participants

- 5.1 Participants in ABC content should normally be informed of the general nature of their participation.
- **5.2** A refusal to participate will not be overridden without good cause.

Opportunity to respond

5.3 Where allegations are made about a person or organisation, make reasonable efforts in the circumstances to provide a fair opportunity to respond.

Attribution and sources

- **5.4** Aim to attribute information to its source.
- 5.5 Where a source seeks anonymity, do not agree without first considering the source's motive and any alternative attributable sources.
- **5.6** Do not misrepresent another's work as your own.

Undertakings

5.7 Assurances given in relation to conditions of participation, use of content, confidentiality or anonymity must be honoured except in rare cases where justified in the public interest.

Secret recording and other types of deception

- 5.8 Secret recording devices, misrepresentation or other types of deception must not be used to obtain or seek information, audio, pictures or an agreement to participate except where:
 - (a) justified in the public interest and the material cannot reasonably be obtained by any other means; or
 - (b) consent is obtained from the subject or identities are effectively obscured; or
 - (c) the deception is integral to an artistic work. In all cases, the potential for harm must be taken into consideration.

6. Privacy

Principles: Privacy is necessary to human dignity and every person reasonably expects that their privacy will be respected. But privacy is not absolute. The ABC seeks to balance the public interest in respect for privacy with the public interest in disclosure of information and freedom of expression.

Standards:

6.1 Intrusion into a person's private life without consent must be justified in the public interest and the extent of the intrusion must be limited to what is proportionate in the circumstances.

7 Harm and offence

Principles: The ABC broadcasts comprehensive and innovative content that aims to inform, entertain and educate diverse audiences. This involves a willingness to take risks, invent and experiment with new ideas. It can result in challenging content which may offend some of the audience some of the time. But it also contributes to diversity of content in the media and to fulfilling the ABC's function to encourage and promote the musical, dramatic and other performing arts. The ABC acknowledges that a public broadcaster should never gratuitously harm or offend and accordingly any content which is likely to harm or offend must have a clear editorial purpose.

The ABC potentially reaches the whole community, so it must take into account community standards. However, the community recognises that what is and is not acceptable in ABC content largely depends upon the particular context, including the nature of the content, its target audience, and any signposting that equips audiences to make informed choices about what they see, hear or read. Applying the harm and offence standard, therefore, requires careful judgement. What may be inappropriate and unacceptable in one context may be appropriate and acceptable in another. Coarse language, disturbing images or unconventional situations may form a legitimate part of reportage, debate, documentaries or a humorous, satirical, dramatic or other artistic work.

Standards:

- 7.1 Content that is likely to cause harm or offence must be justified by the editorial context.
- **7.2** Where content is likely to cause harm or offence, having regard to the context, make reasonable efforts to provide information about the nature of the content through the use of classification labels or other warnings or advice.
- **7.3** Ensure all domestic television programs with the exception of news, current affairs and sporting events are classified and scheduled for broadcast in accordance with the ABC's Associated Standard on Television Program Classification.
- 7.4 If inadvertent or unexpected actions, audio or images in live content are likely to cause harm or offence, take appropriate steps to mitigate.
- 7.5 The reporting or depiction of violence, tragedy or trauma must be handled with extreme sensitivity. Avoid causing undue distress to victims, witnesses or bereaved relatives. Be sensitive to significant cultural practices when depicting or reporting on recently deceased persons.
- 7.6 Where there is editorial justification for content which may lead to dangerous imitation or exacerbate serious threats to individual or public health, safety or welfare, take appropriate steps to mitigate those risks, particularly by taking care with how content is expressed or presented.
- **7.7** Avoid the unjustified use of stereotypes or discriminatory content that could reasonably be interpreted as condoning or encouraging prejudice.



8. Children and young people

Principles: The ABC aims to provide children and young people (under the age of 18) with enjoyable and enriching content, as well as opportunities for them to express themselves. Children and young people participate and interact with the ABC in various ways – as actors, presenters, interviewees, subjects, content makers and audience members.

The ABC has a responsibility to protect children and young people from potential harm that might arise during their engagement with the ABC and its content. The ABC shares this responsibility with parents/guardians and with the child or young person him/herself. In particular, the ABC recommends that parents/guardians supervise children and young people's access to content, their participation in interactive services, and their exposure to news and current affairs. It is not always possible to avoid presenting content that may be distressing to some audience members.

Standards:

- **8.1** Take due care over the dignity and physical and emotional welfare of children and young people who are involved in making, participating in and presenting content produced or commissioned by the ABC.
- **8.2** Before significant participation of a child or young person in content produced or commissioned by the ABC, or in interactive services offered by the ABC, consider whether it is appropriate to obtain the consent of both the child/young person and the parent/quardian.
- **8.3** Adopt appropriate measures wherever practicable to enable children and young people, or those who supervise them, to manage risks associated with the child/young person's participation with, use of and exposure to ABC content and services designed for them.
- **8.4** Take particular care to minimise risks of exposure to unsuitable content or inappropriate contact by peers or strangers.

V. Associated Standard:Television Program Classification

Status of Associated Standard

This Associated Standard is approved by the ABC Board and is binding. It is for consideration by relevant editorial decision-makers when providing advice on compliance and by complaints bodies when dealing with complaints. The Associated Standard is provided to assist interpretation of or otherwise supplement the standard in the Editorial Policies to which the Associated Standard relates

This Associated Standard forms part of the Code of Practice notified to the Australian Communications and Media Authority under section 8(1)(e) of the Australian Broadcasting Corporation Act 1983.

Key Editorial Standard

7.3 Ensure all domestic television programs – with the exception of news, current affairs and sporting events – are classified and scheduled for broadcast in accordance with the ABC's Associated Standard on Television Program Classification.

Principles:

The ABC applies the classifications listed below to the broadcast of all its domestic television programs with the exception of news, current affairs and sporting events. The ABC classifications are adapted from the Guidelines for the Classification of Films and Computer Games issued by the Classification Board made under the Classification (Publications, Films and Computer Games) Act 1995.

The guiding principle in the application of the following classifications is context. What is inappropriate and unacceptable in one context may be appropriate and acceptable in another. Factors to be taken into account include: the artistic or educational merit of the production, the purpose of a sequence, the tone, the camera work, the intensity and relevance of the material, the treatment, and the intended audience.

Standards:

7.3.1 Television Classifications

G-GENERAL

G programs may be shown at any time. G programs, which include programs designed for pre-school and school-aged children, are suitable for children to watch on their own. Some G programs may be more appropriate for older children.



The G classification does not necessarily indicate that the program is one that children will enjoy. Some G programs contain themes or storylines that are not of interest to children.

Whether or not the program is intended for children, the treatment of themes and other classifiable elements will be careful and discreet

Themes: The treatment of themes should be discreet, justified by context, and very mild in impact. The presentation of dangerous, imitable behaviour is not permitted except in those circumstances where it is justified by context. Any depiction of such behaviour must not encourage dangerous imitation.

Violence: Violence may be very discreetly implied, but should:

- have a light tone, or
- have a very low sense of threat or menace, and
- be infrequent, and
- not be gratuitous.

Sex: Sexual activity should:

- only be suggested in very discreet visual or verbal references, and
- be infrequent, and
- not be gratuitous.

Artistic or cultural depictions of nudity in a sexual context may be permitted if the treatment is discreet, justified by context, and very mild in impact.

Language: Coarse language should:

- be very mild and infrequent, and
- not be gratuitous.

Drug Use: The depiction of the use of legal drugs should be handled with care. Illegal drug use should be implied only very discreetly and be justified by context.

Nudity: Nudity outside of a sexual context should be:

- infrequent.and
- not detailed, and
- not gratuitous.

PG - PARENTAL GUIDANCE

(Parental Guidance recommended for people under 15 years)
Subject to the Implementation Guidelines at 7.3.2, PG programs may be shown in accordance with Time Zone Charts at 7.3.5.

PG programs may contain themes and concepts which, when viewed by those under 15 years, may require the guidance of an adult. The PG classification signals to parents that material in this category contains depictions or references which could be confusing or upsetting to children without adult guidance. Material classified PG will not be harmful or disturbing to children.

Parents may choose to preview the material for their children. Some may choose to watch the material with their children. Others might find it sufficient to be accessible during or after the viewing to discuss the content.

Themes: The treatment of themes should be discreet and mild in impact. More disturbing themes are not generally dealt with at PG level. Supernatural or mild horror themes may be included.

Violence: Violence may be discreetly implied or stylised and should also be:

- mild in impact, and
- not shown in detail.

Sex: Sexual activity and nudity in a sexual context may be suggested, but should:

- be discreet, and
- be infrequent, and
- not be gratuitous.

Verbal references to sexual activity should be discreet.

Language: Coarse language should be mild and infrequent.

Drug Use: Discreet verbal references and mild, incidental visuals of drug use may be included, but these should not promote or encourage drug use.

Nudity: Nudity outside of a sexual context should not be detailed or gratuitous.

M - MATURE

(Recommended for people aged 15 years and over)

Subject to the Implementation Guidelines at 7.3.2, M programs may be shown in accordance with the Time Zone Charts at 7.3.5.

The M category is recommended for people aged over 15 years. Programs classified M contain material that is considered to be potentially harmful or disturbing to those under 15 years. Depictions and references to classifiable elements may contain detail. While most themes may be dealt with, the degree of explicitness and intensity of treatment



will determine what can be accommodated in the M category – the less explicit or less intense material will be included in the M classification and the more explicit or more intense material, especially violent material, will be included in the MA15+ classification.

Themes: Most themes can be dealt with, but the treatment should be discreet and the impact should not be strong.

Violence: Generally, depictions of violence should:

- not contain a lot of detail, and
- not be prolonged.

In realistic treatments, depictions of violence that contain detail should:

- be infrequent, and
- not have a strong impact, and
- not be gratuitous.

In stylised treatments, depictions of violence may contain more detail and be more frequent if this does not increase the impact.

Verbal and visual references to sexual violence may only be included if they are:

- discreet and infrequent, and
- strongly justified by the narrative or documentary context.

Sex: Sexual activity may be discreetly implied.

Nudity in a sexual context should not contain a lot of detail, or be prolonged.

Verbal references to sexual activity may be more detailed than depictions if this does not increase the impact.

Language: Coarse language may be used.

Generally, coarse language that is stronger, detailed or very aggressive should:

- be infrequent, and
- not be gratuitous.

Drug Use: Drug use may be discreetly shown.

Drug use should not be promoted or encouraged.

Nudity: Nudity outside of a sexual context may be shown but depictions that contain any detail should not be gratuitous.

MA15+ - MATURE AUDIENCE

(Not suitable for people under 15 years)

Subject to the Implementation Guidelines at 7.3.2, MA15+ programs may be shown in accordance with the Time Zone Charts at 7.3.5

MA15+ programs, because of the matter they contain or because of the way it is treated, are not suitable for people aged under 15 years.

Material classified MA15+ deals with issues or contains depictions which require a more mature perspective. This is because the impact of individual elements or a combination of elements is considered likely to be harmful or disturbing to viewers under 15 years of age. While most themes may be dealt with, the degree of explicitness and intensity of treatment will determine what can be accommodated in the MA15+ category – the more explicit or more intense material, especially violent material, will be included in the MA15+ classification and the less explicit or less intense material will be included in the M classification.

Themes: The treatment of themes with a high degree of intensity should not be gratuitous.

Violence: Generally, depictions of violence should not have a high impact.

In realistic treatments, detailed depictions of violence with a strong impact should:

- be infrequent, and
- not be prolonged, and
- not be gratuitous.

Depictions of violence in stylised treatments may be more detailed and more frequent if this does not increase the impact.

Depictions of sexual violence are permitted only if they are not frequent, prolonged, gratuitous or exploitative.

Sex: Sexual activity may be implied.

Depictions of nudity in a sexual context which contain detail should not be exploitative.

Verbal references may be more detailed than depictions, if this does not increase the impact.

Language: Coarse language may be used.

Coarse language that is very strong, aggressive or detailed should not be gratuitous.

Drug Use: Drug use may be shown, but should not be promoted or encouraged.



207

More detailed depictions should not have a high degree of impact.

Nudity: Nudity should be justified by context.

7.3.2 Implementation Guidelines

The time zones for each program classification are guides to the most likely placement of programs within that classification. They are not hard and fast rules and there will be occasions on which programs or segments of programs appear in other time zones.

There must be sound reasons for any departure from the time zone for a program classification. Possible reasons might include, for example, the need to schedule programs which are serious presentations of moral, social or cultural issues, in timeslots most suitable for their target audiences.

Programs, including those having a particular classification under the Classification Board's Guidelines for the Classification of Films and Computer Games, may be modified so that they are suitable for broadcast or suitable for broadcast at particular times.

Broken Hill in New South Wales shares a time zone with South Australia but ordinarily receives the ABC's New South Wales TV services. Given the time zone difference, some programs are broadcast outside their classification time zone.

7.3.3 Television Classification Symbols

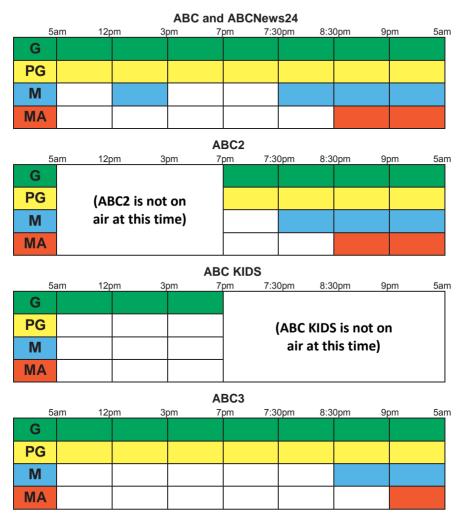
The classification symbol of the PG, M or MA15+ program (except for news, current affairs or sporting events) being shown will be displayed at the beginning of the program.

The classification symbol of the PG, M or MA15+ program (except for news, current affairs or sporting events) being promoted will be displayed during the promotion.

7 3 4 Consumer Advice

Audio and visual consumer advice on the reasons for an M or MA15+ classification will be given prior to the beginning of an M or MA15+ program.

7.3.5 Time Zone Charts



How to make a complaint

If you are concerned that a radio or television program broadcast by the ABC does not comply with this Code of Practice, you are entitled to make a complaint.

The law requires that you first make your complaint to the ABC. You can do so by completing the online Complaint Form at www.abc.net.au/contact/complain.htm or by writing to:

Audience and Consumer Affairs
Australian Broadcasting Corporation
GPO Box 9994. in the capital city of your State or Territory

Your complaint should:

- include your name and an address where you can be contacted (this can be an email address):
- specify the ABC program which concerned you;
- include the time, date and channel/station of the broadcast:
- be made within six weeks of the date of broadcast or, if made after six weeks, explain why you believe the ABC should nevertheless investigate the matter;
- provide a short summary of what concerned you, including any relevant Standard of the Code you believe may have been breached (see the section "Principles and Standards"):
- if you are complaining about a breach of the Standards relating to Privacy, or to Fair and Honest Dealing, indicate your interest in the subject matter (e.g., was your personal privacy affected, or were you a participant in a program and believe you were unfairly or dishonestly treated?).

If you are dissatisfied with the ABC's response, or if you have not received a response within 60 days of making your complaint to the ABC, then you are entitled to complain to the Australian Communications and Media Authority (the ACMA). You can write to the ACMA at:

Australian Communications and Media Authority

PO Box Q500, Queen Victoria Building

Sydney NSW 2000 Fax: 02 9334 7799

Email: broadcasting@acma.gov.au

If you make a complaint to the ACMA, you should provide:

- a copy of your complaint to the ABC
- a copy of the ABC's response to you, if received
- the reasons you consider the ABC's response to be inadequate.

Note: ABC complaints procedures do not form part of the ABC Code of Practice.



211

CODE OF PRACTICE

(& associated standards)

January 15, 2019

I. Regulatory Framework

The ABC Board is required, under paragraph 8(1)(e) of the ABC Act, to develop a code of practice relating to its television and radio programming, and to notify this code to the Australian Communications and Media Authority ("the ACMA").

A complaint alleging the ABC has acted contrary to its Code of Practice in its television or radio programming may be made to the ABC. A complainant is entitled under section 150 of the Broadcasting Services Act 1992 (Cth) ("the BSA") to take their complaint to the ACMA if, after 60 days, the ABC fails to respond to the complainant or the complainant considers the ABC's response is inadequate.

The ACMA has a discretionary power to investigate a complaint alleging the ABC has, in providing a national broadcasting service, breached its Code of Practice. Section 151 of the BSA provides that the ACMA may investigate the complaint if it thinks that it is desirable to do so.

The ACMA's jurisdiction under sections 150-151 does not encompass the ABC's print content or content disseminated by the ABC over the internet or through mobile devices.

However, the eSafety Commissioner has separate jurisdiction under Schedule 7 to the BSA in relation to content hosted on websites or transmitted through mobile services where that content is either "prohibited content" or "age-restricted content".

The eSafety Commissioner is empowered under Schedule 7 to require content service providers and content hosts to remove or prevent access to these types of content.

The ABC voluntarily complies with the Content Services Code, which is registered as an industry code with the eSafety Commissioner under clause 85 of Schedule 7 to the BSA.

The Content Services Code does not apply to content delivered through online or mobile services where that content has been previously transmitted on radio or television.

Except as expressly provided by the BSA, the regulatory regime established by the BSA does not apply to the ABC: subsection 13(5) of the BSA, and section 79 of the ABC Act.

¹ Prohibited content essentially involves content that is classified either as RC (Refused Classification) or X18+. This includes real depictions of actual sexual activity, child pornography, detailed instruction in crime, and violence or drug use.

² Age-restricted content involves content classified as R18+ or MA15+ that is delivered through a mobile device or through a service that provides audio or video content for a fee. This type of content must be subject to a restricted access system, i.e. measures put in place to protect children under the age of 15 from exposure to unsuitable material. This category of content includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse language, and other material that is strong in impact.

II. Scope of the Code

The requirements of this Code are set out in the sections dealing with Interpretation and Standards in Part IV and the Associated Standard in Part V. The Standards in Part IV apply to radio and television programs broadcast by the ABC on its free-to-air television or radio broadcasting services. The Associated Standard in Part V applies only to television programs broadcast by the ABC on its domestic free-to-air television services.

Complaints about content on the services named above fall within the scope of the Code except where:

- the complaint concerns content which is or becomes the subject of legal proceedings;
- the complaint was frivolous or vexatious or not made in good faith;
- the complainant does not have a sufficient interest in the subject matter of the complaint, where the complaint alleges a breach of Fair and honest dealing (Standards 5.1-5.8) or Privacy (Standard 6.1).
- the complaint was lodged with the ABC more than six weeks after the date when the program was last broadcast by the ABC on its free-to-air radio or television services, unless the complaint is accepted for investigation on the grounds that is appropriate to do so, having regard to:
 - the interests of the complainant in the subject matter of the complaint;
 - the seriousness of the alleged breach;
 - the reason(s) for the delay;
 - the availability of the program content which is the subject of the complaint; and
 - any prejudice the delay may otherwise have on the ability to investigate and determine the matter fairly.

III. Resolved Complaints

The ABC seeks to comply fully with the Code and to resolve complaints as soon as practicable.

A failure to comply will not be a breach of the Code if the ABC has, prior to the complaint being made to the ACMA, taken steps which were adequate and appropriate in all the circumstances to redress the cause of the complaint.

To illustrate, a failure to comply with Standards 2.1 or 2.2 (Accuracy) will not be taken to be a breach of the Code if a correction or clarification, which is adequate and appropriate in all the circumstances, is made prior to or within 30 days of the ABC receiving the complaint.

IV. Principles and Standards

Preamble

The ABC belongs to the Australian people.

Earning and retaining their trust is essential to fulfilling the ABC's charter and its responsibilities under the ABC Act to provide innovative and comprehensive services of a high standard to Australian and international audiences.

The principles and standards set out below are the means by which the ABC seeks to meet these obligations.

They uphold the fundamental journalistic principles of accuracy and impartiality, to protect the ABC's independence and integrity.

They recognise that ABC content must be created in a way that is respectful towards audiences and mindful of community standards in areas like harm and offence.

At the same time, they recognise that the ABC needs to be adventurous, brave and creative:

Adventurous in encouraging new and sometimes confronting forms of art and entertainment.

Brave in reporting without fear or favour, even when that might be uncomfortable or unpopular; and

Creative in finding new ways of telling Australian stories, reflecting Australian culture and sharing in the Australian conversation.

By holding to these principles and standards, the ABC seeks to be accountable to the Australian people who fund us.

1. Interpretation

In this Code, the Standards must be interpreted and applied in accordance with the Principles applying in each Section. From time to time, the ABC publishes Guidance Notes which do not in themselves impose obligations on the ABC, but which may be relevant in interpreting and applying the Code.

The Standards in Parts IV and V are to be interpreted and applied with due regard for the nature of the content under consideration in particular cases. The ABC is conscious that its dual obligations – for accountability and for high quality – can in practice interact in complex ways. It can be a sign of strength not weakness that journalism enrages or art shocks. The Standards are to be applied in ways that maintain independence and integrity, preserve trust and do not unduly constrain journalistic enquiry or artistic expression.

2. Accuracy

Principles: The ABC has a statutory duty to ensure that the gathering and presentation of news and information is accurate according to the recognised standards of objective journalism. Credibility depends heavily on factual accuracy. Types of fact-based content include news and analysis of current events, documentaries, factual dramas and lifestyle programs. The ABC requires that reasonable efforts must be made to ensure accuracy in all fact-based content. The ABC gauges those efforts by reference to:

- the type, subject and nature of the content;
- the likely audience expectations of the content;
- the likely impact of reliance by the audience on the accuracy of the content; and
- the circumstances in which the content was made and presented.

The ABC accuracy standard applies to assertions of fact, not to expressions of opinion. An opinion, being a value judgement or conclusion, cannot be found to be accurate or inaccurate in the way facts can. The accuracy standard requires that opinions be conveyed accurately, in the sense that quotes should be accurate and any editing should not distort the meaning of the opinion expressed.

The efforts reasonably required to ensure accuracy will depend on the circumstances. Sources with relevant expertise may be relied on more heavily than those without. Eyewitness testimony usually carries more weight than second-hand accounts. The passage of time or the inaccessibility of locations or sources can affect the standard of verification reasonably required.

The ABC should make reasonable efforts, appropriate in the context, to signal to audiences gradations in accuracy, for example by querying interviewees, qualifying bald assertions, supplementing the partly right and correcting the plainly wrong.

Standards:

- 2.1 Make reasonable efforts to ensure that material facts are accurate and presented in context.
- 2.2 Do not present factual content in a way that will materially mislead the audience. In some cases, this may require appropriate labels or other explanatory information.

3. Corrections and clarifications

Principles: A commitment to accuracy includes a willingness to correct errors and clarify ambiguous or otherwise misleading information. Swift correction can reduce harmful reliance on inaccurate information, especially given content can be quickly, widely and permanently disseminated. Corrections and clarifications can contribute to achieving fairness and impartiality.

Standards:

- 3.1 Acknowledge and correct or clarify, in an appropriate manner as soon as reasonably practicable:
- a. significant material errors that are readily apparent or have been demonstrated; or

b. information that is likely to significantly and materially mislead.

4. Impartiality and diversity of perspectives

Principles: The ABC has a statutory duty to ensure that the gathering and presentation of news and information is impartial according to the recognised standards of objective journalism.

Aiming to equip audiences to make up their own minds is consistent with the public service character of the ABC. A democratic society depends on diverse sources of reliable information and contending opinions. A broadcaster operating under statute with public funds is legitimately expected to contribute in ways that may differ from commercial media, which are free to be partial to private interests.

Judgements about whether impartiality was achieved in any given circumstances can vary among individuals according to their personal and subjective view of any given matter of contention. Acknowledging this fact of life does not change the ABC's obligation to apply its impartiality standard as objectively as possible. In doing so, the ABC is guided by these hallmarks of impartiality:

- a balance that follows the weight of evidence;
- fair treatment;
- open-mindedness; and
- opportunities over time for principal relevant perspectives on matters of contention to be expressed.

The ABC aims to present, over time, content that addresses a broad range of subjects from a diversity of perspectives reflecting a diversity of experiences, presented in a diversity of ways from a diversity of sources, including content created by ABC staff, generated by audiences and commissioned or acquired from external content-makers.

Impartiality does not require that every perspective receives equal time, nor that every facet of every argument is presented.

Assessing the impartiality due in given circumstances requires consideration in context of all relevant factors including:

- the type, subject and nature of the content;
- the circumstances in which the content is made and presented;
- the likely audience expectations of the content;
- the degree to which the matter to which the content relates is contentious;
- the range of principal relevant perspectives on the matter of contention; and
- the timeframe within which it would be appropriate for the ABC to provide opportunities for the principal relevant perspectives to be expressed, having regard to the public importance of the matter of contention and the extent to which it is the subject of current debate.

Standards:

- 4.1 Gather and present news and information with due impartiality.
- 4.2 Present a diversity of perspectives so that, over time, no significant strand of thought or belief within the community is knowingly excluded or disproportionately represented.
- 4.3 Do not state or imply that any perspective is the editorial opinion of the ABC. The ABC takes no editorial stance other than its commitment to fundamental democratic principles including the rule of law, freedom of speech and religion, parliamentary democracy and equality of opportunity.
- 4.4 Do not misrepresent any perspective.
- 4.5 Do not unduly favour one perspective over another.

5. Fair and honest dealing

Principles: Fair and honest dealing is essential to maintaining trust with audiences and with those who participate in or are otherwise directly affected by ABC content. In rare circumstances, deception or a breach of an undertaking may be justified. Because of the potential damage to trust, deception or breach of an undertaking must be explained openly afterwards unless there are compelling reasons not to do so.

Standards:

Dealing with participants

- 5.1 Participants in ABC content should normally be informed of the general nature of their participation.
- 5.2 A refusal to participate will not be overridden without good cause.

Opportunity to respond

5.3 Where allegations are made about a person or organisation, make reasonable efforts in the circumstances to provide a fair opportunity to respond.

Attribution and sources

- 5.4 Aim to attribute information to its source.
- 5.5 Where a source seeks anonymity, do not agree without first considering the source's motive and any alternative attributable sources.
- 5.6 Do not misrepresent another's work as your own.

Undertakings

5.7 Assurances given in relation to conditions of participation, use of content, confidentiality or anonymity must be honoured except in rare cases where justified in the public interest.

Secret recording and other types of deception

5.8 Secret recording, misrepresentation or other types of deception must not be used by the ABC or its co-production partners to obtain or seek information, audio, pictures or an agreement to participate except where:

- (a) justified in the public interest and the material cannot reasonably be obtained by any other means; or
- (b) consent is obtained from the subject or identities are effectively obscured; or
- (c) the deception is integral to an artistic work.

In all cases, the potential for harm must be taken into consideration.

6. Privacy

Principles: Privacy is necessary to human dignity and every person reasonably expects that their privacy will be respected. But privacy is not absolute. The ABC seeks to balance the public interest in respect for privacy with the public interest in disclosure of information and freedom of expression.

Standards:

6.1 Intrusion into a person's private life without consent must be justified in the public interest and the extent of the intrusion must be limited to what is proportionate in the circumstances.

7. Harm and offence

Principles: The ABC broadcasts comprehensive and innovative content that aims to inform, entertain and educate diverse audiences. This involves a willingness to take risks, invent and experiment with new ideas. It can result in challenging content which may offend some of the audience some of the time. But it also contributes to diversity of content in the media and to fulfilling the ABC's function to encourage and promote the musical, dramatic and other performing arts. The ABC acknowledges that a public broadcaster should never gratuitously harm or offend and accordingly any content which is likely to harm or offend must have a clear editorial purpose.

The ABC potentially reaches the whole community, so it must take into account community standards. However, the community recognises that what is and is not acceptable in ABC content largely depends upon the particular context, including the nature of the content, its target audience, and any signposting that equips audiences to make informed choices about what they see, hear or read. Applying the harm and offence standard, therefore, requires careful judgement. What may be inappropriate and unacceptable in one context may be appropriate and acceptable in another. Coarse language, disturbing images or unconventional situations may form a legitimate part of reportage, debate, documentaries or a humorous, satirical, dramatic or other artistic work.

Standards:

- 7.1 Content that is likely to cause harm or offence must be justified by the editorial context.
- 7.2 Where content is likely to cause harm or offence, having regard to the context, make reasonable efforts to provide information about the nature of the content through the use of classification labels or other warnings or advice.

- 7.3 Ensure all domestic television programs with the exception of news, current affairs and sporting events are classified and scheduled for broadcast in accordance with the ABC's Associated Standard on Television Program Classification.
- 7.4 If inadvertent or unexpected actions, audio or images in live content are likely to cause harm or offence, take appropriate steps to mitigate.
- 7.5 The reporting or depiction of violence, tragedy or trauma must be handled with extreme sensitivity. Avoid causing undue distress to victims, witnesses or bereaved relatives. Be sensitive to significant cultural practices when depicting or reporting on recently deceased persons.
- 7.6 Where there is editorial justification for content which may lead to dangerous imitation or exacerbate serious threats to individual or public health, safety or welfare, take appropriate steps to mitigate those risks, particularly by taking care with how content is expressed or presented.
- 7.7 Avoid the unjustified use of stereotypes or discriminatory content that could reasonably be interpreted as condoning or encouraging prejudice.

8. Children and young people

Principles: The ABC aims to provide children and young people (under the age of 18) with enjoyable and enriching content, as well as opportunities for them to express themselves.

Children and young people participate and interact with the ABC in various ways – as actors, presenters, interviewees, subjects, content makers and audience members.

The ABC has a responsibility to protect children and young people from potential harm that might arise during their engagement with the ABC and its content. The ABC shares this responsibility with parents/guardians and with the child or young person him/herself.

In particular, the ABC recommends that parents/guardians supervise children and young people's access to content, their participation in interactive services, and their exposure to news and current affairs. It is not always possible to avoid presenting content that may be distressing to some audience members.

Standards:

- 8.1 Take due care over the dignity and physical and emotional welfare of children and young people who are involved in making, participating in and presenting content produced or commissioned by the ABC.
- 8.2 Before significant participation of a child or young person in content produced or commissioned by the ABC, or in interactive services offered by the ABC, consider whether it is appropriate to obtain the consent of both the child/young person and the parent/guardian.
- 8.3 Adopt appropriate measures wherever practicable to enable children and young people, or those who supervise them, to manage risks associated with the child/young person's participation with, use of and exposure to ABC content and services designed for them.

8.4 Take particular care to minimise risks of exposure to unsuitable content or inappropriate contact by peers or strangers.

V. Associated Standard:

Television Program Classification

Status of Associated Standard

This Associated Standard is approved by the ABC Board and is binding. It is for consideration by relevant editorial decision-makers when providing advice on compliance and by complaints bodies when dealing with complaints. The Associated Standard is provided to assist interpretation of or otherwise supplement the standard in the Editorial Policies to which the Associated Standard relates.

This Associated Standard forms part of the Code of Practice notified to the Australian Communications and Media Authority under section 8(1)(e) of the Australian Broadcasting Corporation Act 1983.

Key Editorial Standard

7.3 Ensure all domestic television programs – with the exception of news, current affairs and sporting events – are classified and scheduled for broadcast in accordance with the ABC's Associated Standard on Television Program Classification.

Principles:

The ABC applies the classifications listed below to the broadcast of all its domestic television programs with the exception of news, current affairs and sporting events.

The ABC classifications are adapted from the Guidelines for the Classification of Films and Computer Games issued by the Classification Board made under the Classification (Publications, Films and Computer Games) Act 1995.

The guiding principle in the application of the following classifications is context. What is inappropriate and unacceptable in one context may be appropriate and acceptable in another. Factors to be taken into account include: the artistic or educational merit of the production, the purpose of a sequence, the tone, the camera work, the intensity and relevance of the material, the treatment, and the intended audience.

Standards:

7.3.1 Television Classifications

G – GENERAL

G programs may be shown at any time. G programs, which include programs designed for pre-school and school-aged children, are suitable for children to watch on their own.

Some G programs may be more appropriate for older children.

The G classification does not necessarily indicate that the program is one that children will enjoy. Some G programs contain themes or storylines that are not of interest to children.

Whether or not the program is intended for children, the treatment of themes and other classifiable elements will be careful and discreet.

Themes: The treatment of themes should be discreet, justified by context, and very mild in impact. The presentation of dangerous, imitable behaviour is not permitted except in those circumstances where it is justified by context. Any depiction of such behaviour must not encourage dangerous imitation.

Violence: Violence may be very discreetly implied, but should:

- have a light tone, or
- have a very low sense of threat or menace, and
- be infrequent, and
- not be gratuitous.

Sex: Sexual activity should:

- only be suggested in very discreet visual or verbal references, and
- be infrequent, and
- not be gratuitous.

Artistic or cultural depictions of nudity in a sexual context may be permitted if the treatment is discreet, justified by context, and very mild in impact.

Language: Coarse language should:

- be very mild and infrequent, and
- not be gratuitous.

Drug Use: The depiction of the use of legal drugs should be handled with care. Illegal drug use should be implied only very discreetly and be justified by context.

Nudity: Nudity outside of a sexual context should be:

- infrequent, and
- not detailed, and
- not gratuitous.

PG – PARENTAL GUIDANCE

(Parental Guidance recommended for people under 15 years)

Subject to the Implementation Guidelines at 7.3.2, PG programs may be shown in accordance with Time Zone Charts at 7.3.5.

PG programs may contain themes and concepts which, when viewed by those under 15 years, may require the guidance of an adult. The PG classification signals to parents that material in this category contains depictions or references which could be confusing or upsetting to children without adult guidance. Material classified PG will not be harmful or disturbing to children.

Parents may choose to preview the material for their children. Some may choose to watch the material with their children. Others might find it sufficient to be accessible during or after the viewing to discuss the content.

Themes: The treatment of themes should be discreet and mild in impact. More disturbing themes are not generally dealt with at PG level. Supernatural or mild horror themes may be included.

Violence: Violence may be discreetly implied or stylised and should also be:

- mild in impact, and
- not shown in detail.

Sex: Sexual activity and nudity in a sexual context may be suggested, but should:

- be discreet, and
- be infrequent, and
- not be gratuitous.

Verbal references to sexual activity should be discreet.

Language: Coarse language should be mild and infrequent.

Drug Use: Discreet verbal references and mild, incidental visuals of drug use may be included, but these should not promote or encourage drug use.

Nudity: Nudity outside of a sexual context should not be detailed or gratuitous.

M – MATURE

(Recommended for people aged 15 years and over)

Subject to the Implementation Guidelines at 7.3.2, M programs may be shown in accordance with the Time Zone Charts at 7.3.5.

The M category is recommended for people aged over 15 years. Programs classified M contain material that is considered to be potentially harmful or disturbing to those under 15 years.

Depictions and references to classifiable elements may contain detail.

While most themes may be dealt with, the degree of explicitness and intensity of treatment will determine what can be accommodated in the M category – the less explicit or less intense material

will be included in the M classification and the more explicit or more intense material, especially violent material, will be included in the MA15+ classification.

Themes: Most themes can be dealt with, but the treatment should be discreet and the impact should not be strong.

Violence: Generally, depictions of violence should:

- not contain a lot of detail, and
- not be prolonged.

In realistic treatments, depictions of violence that contain detail should:

- be infrequent, and
- not have a strong impact, and
- not be gratuitous.

In stylised treatments, depictions of violence may contain more detail and be more frequent if this does not increase the impact.

Verbal and visual references to sexual violence may only be included if they are:

- discreet and infrequent, and
- strongly justified by the narrative or documentary context.

Sex: Sexual activity may be discreetly implied.

Nudity in a sexual context should not contain a lot of detail or be prolonged.

Verbal references to sexual activity may be more detailed than depictions if this does not increase the impact.

Language: Coarse language may be used.

Generally, coarse language that is stronger, detailed or very aggressive should:

- be infrequent, and
- not be gratuitous.

Drug Use: Drug use may be discreetly shown.

Drug use should not be promoted or encouraged.

Nudity: Nudity outside of a sexual context may be shown but depictions that contain any detail should not be gratuitous.

MA15+ - MATURE AUDIENCE

(Not suitable for people under 15 years)

Subject to the Implementation Guidelines at 7.3.2, MA15+ programs may be shown in accordance with the Time Zone Charts at 7.3.5.

MA15+ programs, because of the matter they contain or because of the way it is treated, are not suitable for people aged under 15 years.

Material classified MA15+ deals with issues or contains depictions which require a more mature perspective. This is because the impact of individual elements or a combination of elements is considered likely to be harmful or disturbing to viewers under 15 years of age. While most themes may be dealt with, the degree of explicitness and intensity of treatment will determine what can be accommodated in the MA15+ category – the more explicit or more intense material, especially violent material, will be included in the MA15+ classification and the less explicit or less intense material will be included in the M classification.

Themes: The treatment of themes with a high degree of intensity should not be gratuitous.

Violence: Generally, depictions of violence should not have a high impact.

In realistic treatments, detailed depictions of violence with a strong impact should:

- be infrequent, and
- not be prolonged, and
- not be gratuitous.

Depictions of violence in stylised treatments may be more detailed and more frequent if this does not increase the impact.

Depictions of sexual violence are permitted only if they are not frequent, prolonged, gratuitous or exploitative.

Sex: Sexual activity may be implied.

Depictions of nudity in a sexual context which contain detail should not be exploitative.

Verbal references may be more detailed than depictions if this does not increase the impact.

Language: Coarse language may be used.

Coarse language that is very strong, aggressive or detailed should not be gratuitous.

Drug Use: Drug use may be shown but should not be promoted or encouraged.

More detailed depictions should not have a high degree of impact.

Nudity: Nudity should be justified by context.

7.3.2 Implementation Guidelines

The time zones for each program classification are guides to the most likely placement of programs within that classification. They are not hard and fast rules and there will be occasions on which programs or segments of programs appear in other time zones.

There must be sound reasons for any departure from the time zone for a program classification. Possible reasons might include, for example, the need to schedule programs which are serious presentations of moral, social or cultural issues, in timeslots most suitable for their target audiences.

Programs, including those having a particular classification under the Classification Board's Guidelines for the Classification of Films and Computer Games, may be modified so that they are suitable for broadcast or suitable for broadcast at particular times.

Broken Hill in New South Wales shares a time zone with South Australia but ordinarily receives the ABC's New South Wales TV services. Given the time zone difference, some programs are broadcast outside their classification time zone.

7.3.3 Television Classification Symbols

The classification symbol of the PG, M or MA15+ program (except for news, current affairs or sporting events) being shown will be displayed at the beginning of the program.

The classification symbol of the PG, M or MA15+ program (except for news, current affairs or sporting events) being promoted will be displayed during the promotion.

7.3.4 Consumer Advice

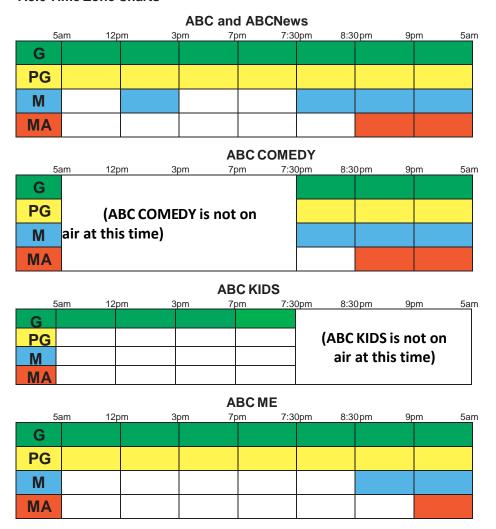
Audio and visual consumer advice on the reasons for an M or MA15+ classification will be given prior to the beginning of an M or MA15+ program.

7.3.5 Classification of Live Content

Many live programs fall into the classification exemption categories (news, current affairs and sporting events). Some, such as live music or comedy programs, do not fall into the exemption categories and pose a particular challenge to classify accurately. The ABC makes reasonable efforts to classify these programs accurately by reviewing scripts, lyrics, outlines, and any pre-recorded material, and briefing program makers and talent as required.

A failure to provide an accurate classification symbol or consumer advice prior to a live (or as-live) program will not be regarded as a breach of standards as long as reasonable efforts were made to classify it and appropriate steps are taken to mitigate any harm or offence.

7.3.6 Time Zone Charts



How to make a complaint

If you are concerned that a radio or television program broadcast by the ABC does not comply with this Code of Practice, you are entitled to make a complaint.

The law requires that you first make your complaint to the ABC. You can do so by completing the online Complaint Form at www.abc.net.au/contact/complain.htm or by writing to:

Audience and Consumer Affairs

Australian Broadcasting Corporation

GPO Box 9994, in the capital city of your State or Territory

Your complaint should:

- include your name and an address where you can be contacted (this can be an email address);
- specify the ABC program which concerned you;
- include the time, date and channel/station of the broadcast;
- be made within six weeks of the date of broadcast or, if made after six weeks, explain why you believe the ABC should nevertheless investigate the matter;
- provide a short summary of what concerned you, including any relevant Standard of the Code you believe may have been breached (see the section "Principles and Standards");
- if you are complaining about a breach of the Standards relating to Privacy, or to Fair and Honest Dealing, indicate your interest in the subject matter (e.g., was your personal privacy affected, or were you a participant in a program and believe you were unfairly or dishonestly treated?).

If you are dissatisfied with the ABC's response, or if you have not received a response within 60 days of making your complaint to the ABC, then you are entitled to complain to the Australian Communications and Media Authority (the ACMA). You can write to the ACMA at: Australian Communications and Media Authority

PO Box Q500, Queen Victoria Building

Sydney NSW 2000

Fax: 02 9334 7799

Email: broadcasting@acma.gov.au

If you make a complaint to the ACMA, you should provide:

- a copy of your complaint to the ABC
- a copy of the ABC's response to you, if received
- the reasons you consider the ABC's response to be inadequate.

Note: ABC complaints procedures do not form part of the ABC Code of Practice.



ABC EDITORIAL POLICIES

Principles and Standards

Updated 15 January 2019

1	Independence, integrity and responsibility	4
2	Accuracy	5
3	Corrections and clarifications	6
4	Impartiality and diversity of perspectives	7
5	Fair and honest dealing	9
6	Privacy	11
7	Harm and offence	12
8	Children and young people	14
9	Public access and participation	15
10	Announcements about ABC programs and activities	17
11	Advertising and sponsorship restrictions	19
12	Commercial references	21
13	External funding and relationshins	22



Preamble

The ABC belongs to the Australian people.

Earning and retaining their trust is essential to fulfilling the ABC's charter and its responsibilities under the ABC Act to provide innovative and comprehensive services of a high standard to Australian and international audiences.

The Editorial Policies set out the key areas where the ABC seeks to meet these obligations. They are the primary tool for content-makers to ensure that the ABC's reputation is maintained to a high standard.

They uphold the fundamental journalistic principles of accuracy and impartiality, to protect the ABC's independence and integrity. They recognise that ABC content must be created in a way that is respectful towards audiences and mindful of community standards in areas like harm and offence.

At the same time, they recognise that the ABC needs to be adventurous, brave and creative:

Adventurous in encouraging new and sometimes confronting forms of art and entertainment.

Brave in reporting without fear or favour, even when that might be uncomfortable or unpopular; and

Creative in finding new ways of telling Australian stories, reflecting Australian culture and sharing in the Australian conversation.

By holding to the principles and standards contained in the Editorial Policies, the ABC seeks to be accountable to the Australian people who fund us.



Note on interpretation

The Principles set out the ABC's approach to each of the main issues to be addressed by an independent public broadcaster that regulates itself. The Standards which follow each statement of principle are enforceable under internal management processes and under the ABC Complaints Handling Procedures. The Principles are intended to assist the interpretation and application of the Standards. More detailed advice is available in non-binding Guidance Notes.

The Editorial Policies are intended to be applied with due regard for the nature of the content under consideration in particular cases. The ABC is conscious that its dual obligations – for accountability and for high quality – can in practice interact in complex ways. It can be a sign of strength not weakness that journalism enrages or art shocks.

The Standards are to be applied in ways that maintain independence and integrity, preserve trust and do not unduly constrain journalistic enquiry or artistic expression. However, all who are involved with content for the ABC are required to act with integrity and take account of likely harms in exercising their power and responsibility.



Scope

The ABC Editorial Policies apply to all content produced, commissioned, acquired or otherwise obtained by the ABC for broadcast or publication by the ABC on platforms and through services operated by the ABC, or by the ABC on platforms and through services operated by third parties.

The ABC Editorial Policies do not apply to the activities of ABC Commercial except to the extent that ABC Commercial exercises editorial control over content for broadcast or publication by the ABC which has not been already broadcast or published by the ABC. In all its activities, ABC Commercial must operate in a manner consistent with maintaining the independence and integrity of the ABC.



1 Independence, integrity and responsibility

Principles

The trust and respect of the community depend on the ABC's editorial independence and integrity. Independence and responsibility are inseparable. The Managing Director is the Editor-in-Chief who has ultimate editorial power and responsibility.

Editorial decision-making at the ABC is based on upward referral. Those **who create, acquire, commission or oversee ABC content** are responsible for ensuring that it complies with the Editorial Policies, but they are also required to upwardly refer any editorial matter where they are in doubt. Editorial content that is controversial or likely to have an extraordinary impact should also be upwardly referred, even if there is no doubt, to allow closer consideration of any editorial policy issues.

Upward referral is made to line managers and to appropriately senior people within Divisions who are designated with responsibility. In addition, editorial advisers are available and should be consulted for advice and guidance.

Where an editorial issue is being upwardly referred to the Managing Director, it must first be referred to the Editorial Director for input and advice.

Standards

- 1.1 Maintain the independence and integrity of the ABC.
- 1.2 Exercise ABC editorial control over the content the ABC broadcasts or publishes.



- 1.3 Ensure that editorial decisions are not improperly influenced by political, sectional, commercial or personal interests.
- 1.4 External activities of individuals undertaking work for the ABC must not undermine the independence and integrity of the ABC's editorial content.
- 1.5 Exercise editorial independence as authorised and accept responsibility for it. When in doubt about an editorial matter, refer it up to the next most senior person for advice or decision.
- 1.6 When any editorial matter, including an editorial matter not being referred up for advice or decision, is likely to cause controversy or have an extraordinary impact, give proper notice of it to the most appropriate senior manager.
- 1.7 Any editorial matter which is considered by a Divisional Director to be sufficiently significant to be referred to the Managing Director for information or decision must first be referred to the Editorial Director. If a Director is in doubt as to whether an editorial matter is sufficiently significant, advice should be sought from the Editorial Director.



2 Accuracy

Principles

The ABC has a statutory duty to ensure that the gathering and presentation of news and information is accurate according to the recognised standards of objective journalism. Credibility depends heavily on factual accuracy.

Types of fact-based content include news and analysis of current events, documentaries, factual dramas and lifestyle programs. The ABC requires that reasonable efforts must be made to ensure accuracy in all fact-based content. The ABC gauges those efforts by reference to:

- the type, subject and nature of the content;
- the likely audience expectations of the content;
- the likely impact of reliance by the audience on the accuracy of the content; and
- the circumstances in which the content was made and presented.

The ABC accuracy standard applies to assertions of fact, not to expressions of opinion. An opinion, being a value judgement or conclusion, cannot be found to be accurate or inaccurate in the way facts can. The accuracy standard requires that opinions be conveyed accurately, in the sense that quotes should be accurate and any editing should not distort the meaning of the opinion expressed.

The efforts reasonably required to ensure accuracy will depend on the circumstances. Sources with relevant expertise may be relied on more heavily than those without. Eyewitness testimony usually carries more weight than



second-hand accounts. The passage of time or the inaccessibility of locations or sources can affect the standard of verification reasonably required.

The ABC should make reasonable efforts, appropriate in the context, to signal to audiences gradations in accuracy, for example by querying interviewees, qualifying bald assertions, supplementing the partly right and correcting the plainly wrong.

Standards

- 2.1 Make reasonable efforts to ensure that material facts are accurate and presented in context.
- 2.2 Do not present factual content in a way that will materially mislead the audience. In some cases, this may require appropriate labels or other explanatory information.



3 Corrections and clarifications

Principles

A commitment to accuracy includes a willingness to correct errors and clarify ambiguous or otherwise misleading information. Swift correction can reduce harmful reliance on inaccurate information, especially given content can be quickly, widely and permanently disseminated. Corrections and clarifications can contribute to achieving fairness and impartiality.

Standards

- 3.1 Acknowledge and correct or clarify, in an appropriate manner as soon as reasonably practicable:
 - (a) significant material errors that are readily apparent or have been demonstrated; or
 - (b) information that is likely to significantly and materially mislead.



4 Impartiality and diversity of perspectives

Principles

The ABC has a statutory duty to ensure that the gathering and presentation of news and information is impartial according to the recognised standards of objective journalism.

Aiming to equip audiences to make up their own minds is consistent with the public service character of the ABC. A democratic society depends on diverse sources of reliable information and contending opinions. A broadcaster operating under statute with public funds is legitimately expected to contribute in ways that may differ from commercial media, which are free to be partial to private interests.

Judgements about whether impartiality was achieved in any given circumstances can vary among individuals according to their personal and subjective view of any given matter of contention. Acknowledging this fact of life does not change the ABC's obligation to apply its impartiality standard as objectively as possible. In doing so, the ABC is guided by these hallmarks of impartiality:

- a balance that follows the weight of evidence;
- fair treatment;
- open-mindedness; and
- opportunities over time for principal relevant perspectives on matters of contention to be expressed.

The ABC aims to present, over time, content that addresses a broad range of subjects from a diversity of perspectives reflecting a diversity of experiences,



presented in a diversity of ways from a diversity of sources, including content created by ABC staff, generated by audiences and commissioned or acquired from external content-makers.

Impartiality does not require that every perspective receives equal time, nor that every facet of every argument is presented.

Assessing the impartiality due in given circumstances requires consideration in context of all relevant factors including:

- the type, subject and nature of the content;
- the circumstances in which the content is made and presented;
- the likely audience expectations of the content;
- the degree to which the matter to which the content relates is contentious;
- the range of principal relevant perspectives on the matter of contention; and
- the timeframe within which it would be appropriate for the ABC to provide opportunities for the principal relevant perspectives to be expressed, having regard to the public importance of the matter of contention and the extent to which it is the subject of current debate.



Standards

- 4.1 Gather and present news and information with due impartiality.
- 4.2 Present a diversity of perspectives so that, over time, no significant strand of thought or belief within the community is knowingly excluded or disproportionately represented.
- 4.3 Do not state or imply that any perspective is the editorial opinion of the ABC. The ABC takes no editorial stance other than its commitment to fundamental democratic principles including the rule of law, freedom of speech and religion, parliamentary democracy and equality of opportunity.
- 4.4 Do not misrepresent any perspective.
- 4.5 Do not unduly favour one perspective over another.



5 Fair and honest dealing

Principles

Fair and honest dealing is essential to maintaining trust with audiences and with those who participate in or are otherwise directly affected by ABC content. In rare circumstances, deception or a breach of an undertaking may be justified. Because of the potential damage to trust, deception or breach of an undertaking must be explained openly afterwards unless there are compelling reasons not to do so.

Standards

Dealing with participants

- 5.1 Participants in ABC content should normally be informed of the general nature of their participation.
- 5.2 A refusal to participate will not be overridden without good cause.

Opportunity to respond

5.3 Where allegations are made about a person or organisation, make reasonable efforts in the circumstances to provide a fair opportunity to respond.

Attribution and sources

- 5.4 Aim to attribute information to its source.
- 5.5 Where a source seeks anonymity, do not agree without first considering the source's motive and any alternative attributable sources.
- 5.6 Do not misrepresent another's work as your own.

Undertakings



5.7 Assurances given in relation to conditions of participation, use of content, confidentiality or anonymity must be honoured except in rare cases where justified in the public interest.

Secret recording and other types of deception

- 5.8 Secret recordings, misrepresentation or other types of deception must not be used by the ABC or its co-production partners to obtain or seek information, audio, pictures or an agreement to participate except where:
 - (a) justified in the public interest and the material cannot reasonably be obtained by any other means; or
 - (b) consent is obtained from the subject or identities are effectively obscured; or
 - (c) the deception is integral to an artistic work.

In all cases, the potential for harm must be taken into consideration.

Mandatory referral

- 5.9 An appropriately senior ABC person designated for the purpose must approve in advance, having consulted ABC Legal, and considered the applicable editorial standards (such as 5.5, 5.7 or 5.8) and any other relevant factors, any proposal:
 - (a) to use secret recording during the production of content commissioned, produced or co-produced by the ABC; or
 - (b) to broadcast or publish material obtained by deception; or



- (c) to broadcast or publish without attribution information that forms the basis of a report and the ABC is to be committed to protect the identity of the source of the information; or
- (d) not to honour an assurance given in relation to conditions of participation, use of content, confidentiality or anonymity.



6 Privacy

Principles

Privacy is necessary to human dignity and every person reasonably expects that their privacy will be respected. But privacy is not absolute. The ABC seeks to balance the public interest in respect for privacy with the public interest in disclosure of information and freedom of expression.

Standards

6.1 Intrusion into a person's private life without consent must be justified in the public interest and the extent of the intrusion must be limited to what is proportionate in the circumstances.



7 Harm and offence

Principles

The ABC broadcasts and publishes comprehensive and innovative content that aims to inform, entertain and educate diverse audiences. This involves a willingness to take risks, invent and experiment with new ideas. It can result in challenging content which may offend some of the audience some of the time. But it also contributes to diversity of content in the media and to fulfilling the ABC's function to encourage and promote the musical, dramatic and other performing arts. The ABC acknowledges that a public broadcaster should never gratuitously harm or offend and accordingly any content which is likely to harm or offend must have a clear editorial purpose.

The ABC potentially reaches the whole community, so it must take into account community standards. However, the community recognises that what is and is not acceptable in ABC content largely depends on the particular context, including the nature of the content, its target audience, and any signposting that equips audiences to make informed choices about what they see, hear or read. Applying the harm and offence standard, therefore, requires careful judgement. What may be inappropriate and unacceptable in one context may be appropriate and acceptable in another. Coarse language, disturbing images or unconventional situations may form a legitimate part of reportage, debate, documentaries or a humorous, satirical, dramatic or other artistic work.

Standards

7.1 Content that is likely to cause harm or offence must be justified by the editorial context.



- 7.2 Where content is likely to cause harm or offence, having regard to the context, make reasonable efforts to provide information about the nature of the content through the use of classification labels or other warnings or advice.
- 7.3 Ensure all domestic television programs with the exception of news, current affairs and sporting events are classified and scheduled for broadcast in accordance with the ABC's <u>Associated Standard on</u> Television Program Classification.
- 7.4 If inadvertent or unexpected actions, audio or images in live content are likely to cause harm or offence, take appropriate steps to mitigate.
- 7.5 The reporting or depiction of violence, tragedy or trauma must be handled with extreme sensitivity. Avoid causing undue distress to victims, witnesses or bereaved relatives. Be sensitive to significant cultural practices when depicting or reporting on recently deceased persons.
- 7.6 Where there is editorial justification for content which may lead to dangerous imitation or exacerbate serious threats to individual or public health, safety or welfare, take appropriate steps to mitigate those risks, particularly by taking care with how content is expressed or presented.
- 7.7 Avoid the unjustified use of stereotypes or discriminatory content that could reasonably be interpreted as condoning or encouraging prejudice.



8 Children and young people

Principles

The ABC aims to provide children and young people (under the age of 18) with enjoyable and enriching content, as well as opportunities for them to express themselves. Children and young people participate and interact with the ABC in various ways – as actors, presenters, interviewees, subjects, content makers and audience members.

The ABC has a responsibility to protect children and young people from potential harm that might arise during their engagement with the ABC and its content. The ABC shares this responsibility with parents/guardians and with the child or young person him/herself. In particular, the ABC recommends that parents/guardians supervise children and young people's access to content, their participation in interactive services, and their exposure to news and current affairs. It is not always possible to avoid presenting content that may be distressing to some audience members.

Standards

- 8.1 Take due care over the dignity and physical and emotional welfare of children and young people who are involved in making, participating in and presenting content produced or commissioned by the ABC.
- 8.2 Before significant participation of a child or young person in content produced or commissioned by the ABC, or in interactive services offered by the ABC, consider whether it is appropriate to obtain the consent of both the child/young person and the parent/guardian.



- 8.3 Adopt appropriate measures wherever practicable to enable children and young people, or those who supervise them, to manage risks associated with the child/ young person's participation with, use of and exposure to ABC content and services designed for them.
- 8.4 Take particular care to minimise risks of exposure to unsuitable content or inappropriate contact by peers or strangers.



9 Public access and participation

Principles

The ABC provides opportunities for individuals and organisations to engage with the ABC, its audiences and each other consistent with the ABC's public service purposes to inform, entertain, educate and encourage and promote the arts.

Public access and participation can take many forms, for example: musicians and artists submit work for broadcast or online presentation; audience members question ABC presenters and their guests by phone or through online interactive services; organisers of concerts and other activities inform local communities through event diaries; political parties are granted broadcast time to convey their policies directly to the electorate; and community service announcements support charities and other activities in the public interest.

The ABC seeks both to draw audiences to the platforms it controls and to reach audiences using suitable services that third parties control. The ABC takes editorial responsibility in proportion to its control of the media environment in which it operates. The ABC expects those who participate also to exercise responsibility for what they can control.

In fostering engagement, the ABC seeks to maintain its independence and integrity, preserve trust and cultivate respect among participants. The ABC may establish conditions for participation with which participants are expected to comply, such as the ABC's Terms of Use relating to users' interactivity on abc.net.au. The ABC will exercise appropriate oversight over participants' contributions, for example through appropriate moderation of its interactive services.

The ABC does not require content generated and submitted by individuals and organisations to meet the standard of accuracy required of content generated by the ABC. However, where the ABC is satisfied that it is appropriate to do so, the



ABC may decline to broadcast or publish, or may edit, remove, correct or clarify content generated by public participants that contains error or is otherwise false, misleading or harmful.

Individuals and organisations who generate and submit content are not required to be impartial. The ABC recognises that social and political activity, including robust debate, is a necessary and desirable aspect of a healthy democratic community.

Standards

- 9.1 Free broadcast time or publication space may be provided to enable individuals or organisations to communicate directly with the ABC, the audience and each other, provided that:
 - (a) the content is broadcast or published as a public service;
 - (b) the content is relevant and suitable in the context in which it appears;
 - (c) the ABC maintains editorial control; and
 - (d) ABC independence and integrity are maintained.
- 9.2 Opportunities to participate must be administered fairly and respectfully.
- 9.3 Do not knowingly mislead audiences about the nature of the content.
- 9.4 Clearly distinguish content generated and submitted to the ABC from content produced, commissioned or acquired by the ABC.
- 9.5 Do not accept money or other benefit in exchange for broadcasting or publishing the content generated through public access and participation.



10 Announcements about ABC programs and activities

Principles

The ABC is permitted by the ABC Act to publicise its programs, products, services, events and other activities. The ABC is conscious that its audiences value the ABC's role as a non-commercial broadcaster and its non-commercial style. To that end, the ABC will ensure that announcements about ABC activities are produced, scheduled and broadcast or published in a style consistent with the tone and approach of the ABC's various content strands. ABC program promotions should not misrepresent original content and should be scheduled so as to be consistent with the nature of the surrounding content.

Standards

- 10.1 Ensure program promotions and announcements about other ABC activities are produced, scheduled and broadcast or published in a style consistent with the tone and approach of the surrounding content and appropriately take into consideration the likely composition of the audience.
- 10.2 Program promotions must not misrepresent the content they promote.
- 10.3 Announcements about specific ABC commercial products, services or other activities may be broadcast or published provided that:
 - (a) the product, service or activity is directly related to ABC content or to content or services that bear an ABC logo or trademark;



- (b) prior approval has been obtained from an appropriately senior person designated for the purpose within the Division(s) editorially responsible for the surrounding content or from the Managing Director;
- (c) where the product, service or other activity involves sponsorship, any reference to the sponsor must be relevant to informing the audience and not simply a promotion of the sponsor; and
- (d) the announcement is not broadcast or published within news content, content designed for preschool children, or any television program.
- 10.4 Generic announcements about ABC commercial products, services or other activities may be made provided that:
 - (a) prior approval has been obtained from an appropriately senior person designated for the purpose within the Division(s) editorially responsible for the surrounding content or from the Managing Director; and
 - (b) the announcement is not broadcast within news content, content designed for preschool children, or any television program.
- 10.5 Except where permitted by law, do not accept payment or other benefit to broadcast an announcement relating to any program, product, service or other activity which has been produced, published or otherwise created or made available by the ABC in association with an external organisation.



11 Advertising and sponsorship restrictions

Principles

The absence of advertisements and commercial sponsorship is one of the distinctive features of the ABC's domestic television and radio services. It has been reinforced by statute since the ABC was first established in 1932. The ABC is conscious that its audiences value the ABC's distinctive role and style as a non-commercial broadcaster.

The ABC Act was amended in 2013 to recognise the provision of "digital media services" by the ABC. These are non-broadcasting services provided by the ABC to deliver content using digital technology and include online, mobile and social media services. Equivalent restrictions on advertising and commercial sponsorship that apply to ABC broadcasts also apply to the ABC's digital media services.

The ABC is permitted by law to augment its public funding through advertising and sponsorship in relation to certain of its activities, for example its international television service. The ABC may also include advertisements in its commercial products and services where permitted under the ABC Act, for example in its print or related digital magazines.

The restriction on advertising or sponsorship for online content or services provided by the ABC is not intended to limit the ABC's ability to link, where editorially justified, from ABC sites to non-ABC sites which are supported by advertising or sponsorship, or to sites which are operated by the ABC's international television service or by ABC Commercial.

This is also not intended to limit the ABC's ability to establish official presences on advertising-supported sites or services where these are provided by a third party.



The decision as to whether or in what form the ABC establishes such an official presence is an editorial one.

Where permissible advertising or sponsorship occurs, the ABC is committed to maintaining the audience members' trust in the honesty and integrity of what they see, hear and read. Advertisements and sponsored content must be readily recognisable as such. Advertisers and sponsors must have no influence over editorial content or scheduling decisions.

In all decisions relating to advertising and sponsorship, the ABC's independence and integrity are paramount.

Standards

- 11.1 Do not accept advertising or sponsorship in relation to content or services offered on:
 - (a) the ABC's domestic free-to-air television and its domestic and international radio services; or
 - (b) the ABC's online, mobile, social media or other digital media services other than as are associated with the ABC's international television service or as permitted under the ABC Act in respect of certain of ABC Commercial's activities.
- 11.2 Do not accept sponsorship for news content or content designed for preschool children.
- 11.3 Ensure advertising is not broadcast within news content or content designed for preschool children.



- 11.4 Ensure sponsored content is identified as such and in a manner that informs but does not promote.
- 11.5 References to a sponsor or a sponsor's product or service must not be a condition of the sponsorship arrangement. Any sponsorship reference must be editorially justified.
- 11.6 Ensure advertising is readily distinguishable from editorial content.
- 11.7 Product placement and other forms of embedded or surreptitious advertising are prohibited. In exceptional cases, the ABC may use content that already contains product placement provided:
 - (a) the ABC played no role in the commissioning or production of the content;
 - (b) the content has intrinsic editorial value;
 - (c) the product placement is not unduly frequent or unduly prominent; and
 - (d) the ABC's editorial independence and integrity are not undermined.
- 11.8 Do not enter into any advertising or sponsorship arrangement if it would be likely to undermine the ABC's independence and integrity or could be reasonably perceived to do so.



12 Commercial references

Principles

The ABC needs to be able to reflect the world as it is, and this involves referring appropriately to commercial organisations, products and services, while maintaining the ABC's editorial independence and integrity.

Standards

- 12.1 References to trade names, brand names, and logos may be made provided that:
 - (a) the references are editorially relevant in the context; and
 - (b) the ABC's editorial independence or integrity is not undermined.
- 12.2 Commercial references must not be unduly frequent or unduly prominent.
- 12.3 Take particular care to minimise commercial references in content designed for children.
- 12.4 Do not state or imply that the ABC endorses any commercial organisation, product or service.



13 External funding and relationships

Principles

The ABC relies on public funding from Parliament to fulfil its charter obligations and carry out its functions under the ABC Act. The ABC is permitted to supplement its public funding and work collaboratively with others to extend the variety and reach of content offered to the community. The ABC is permitted to accept direct external funding from public sources and enter into funding arrangements with bona fide producers and publishers of content.

The production of content by independent producers, including co-production arrangements, regularly involves funding from the public sector, bona fide industry funding sources and other permitted sources some of which the ABC may not be able to access directly. The ABC is also able to accept free or discounted products, services or facilities to support the creation of content where that does not undermine the ABC's independence and integrity.

External funding sources for ABC produced, commissioned or co-produced content must be scrutinised by the ABC to ensure the ABC's editorial independence and integrity are maintained. Contentiousness alone is not a reason to reject a proposal. The ABC Act requires innovative services of a high standard. The Editorial Policies require the ABC to present a diversity of perspectives over time on contentious matters. Innovation, high quality, diversity and contentiousness can travel together, so long as risks are properly managed.

In these Standards, "external partners" includes funders, producers, publishers and distributors.



Standards

- 13.1 Before the ABC enters into an arrangement for external funding or coproduction of content, the arrangement must be scrutinised by an appropriately senior ABC person designated for the purpose who must reject the arrangement unless satisfied that the independence and integrity of the ABC are fully protected. Factors to consider include:
 - (a) whether the arrangement is permissible under the ABC Act;
 - (b) whether the content is something that the ABC would consider producing for broadcast or publication without external funding;
 - (c) the nature of the external partners' interest in the subject matter of the content and in broadcast or publication of the content by the ABC, and how that interest whether it be political, commercial, sectional, personal or otherwise is likely to be perceived;
 - (d) the extent to which the making, promotion or scheduling of the content will be influenced by any funder and how that influence is likely to be perceived;
 - the reputations of the external partners, including where relevant whether they have editorial standards similar to the ABC's;
 - (f) the willingness of external partners to contract to comply with the Editorial Policies and to assist the ABC to comply;
 - (g) how the ABC will exercise an appropriate level of editorial control that is commensurate with the ABC's contribution and



- consistent with its obligations under the ABC Act and Editorial Policies; and
- (h) the degree to which the subject matter or proposed treatment of the subject matter or scheduling of the content is likely to be contentious, and ways to manage that contentiousness consistent with obligations under the ABC Act and Editorial Policies.
- 13.2 A record of the reasons for acceptance or rejection of external funding proposals must be kept.
- 13.3 The sources of funds obtained by external partners must be disclosed to the ABC before an external funding or co-production arrangement is formalised.
- 13.4 Do not accept public funding from Commonwealth, State or Territory governments or their authorities for the production and broadcast or publication of content which is or appears to be party political.
- 13.5 Free or discounted products, services or facilities may be accepted to support the creation of content provided that:
 - there is no obligation imposed on or accepted by the ABC to structure or present any matter with a particular editorial perspective;
 - (b) prior approval is obtained from an appropriately senior ABC person designated for the purpose;
 - (c) the independence and integrity of the ABC are fully protected; and
 - (d) accurate records are kept of what is accepted.



- 13.6 Any credits acknowledging creative, managerial and financial contributions must be editorially justified and not unduly prominent.
- 13.7 Ensure appropriate disclosure of any external funding arrangement, and any acceptance of free or discounted products, services or facilities, where the arrangement or acceptance, if it were not disclosed but later became public, may reasonably be perceived to distort the editorial content or otherwise undermine the ABC's independence or integrity.





ABC Values & Standards of Workplace Behaviour

ABC employees are expected to demonstrate ABC Values and to conduct themselves in accordance with specified standards of behaviour. Those Values and Standards are outlined below. ABC employees must also comply with ABC policies.

Values

The ABC is an independent media organisation providing broadcasting and digital media services within and outside Australia.

Our Values are the foundation of our work. ABC employees are expected to demonstrate the following ABC Values:

Integrity

We act with trustworthiness, honesty and fairness. We deliver on our commitments and are accountable.

Respect

We treat our audiences and each other with consideration and dignity. We embrace diversity.

Collegiality

We work together willingly. We cooperate and share in the ABC's challenges and successes.

Innovation

We foster creativity and distinctiveness. We encourage new thinking and strive to achieve quality in all that we do.

Standards

ABC employees must:

- 1. demonstrate ABC Values in all aspects of work
- 2. work and act with professionalism, care and diligence
- 3. comply with any lawful and reasonable direction given by a person in the ABC who has authority to give such a direction
- 4. treat colleagues and the public with respect and courtesy
- 5. demonstrate ethical behaviour consistent with the best interests and good name of the ABC
- 6. act in good faith, for a proper purpose and only use ABC resources and information for legitimate ABC purposes
- 7. advise the ABC of criminal charge or conviction which is related to or impacts on the employee's ability to perform the inherent requirements of their job

- 8. meet appropriate standards of personal hygiene and appearance and dress appropriately for the workplace and the tasks to be undertaken on any particular day
- 9. comply with all relevant legal and administrative requirements, including ABC Policies and Procedures.

Conduct or behaviour which does not meet these standards may constitute misconduct (including serious misconduct) and lead to disciplinary action, including termination of employment.

5 Issued: January 20, 2010 Revised: March 1, 2016

5 FAIR AND HONEST DEALING

Principles

Fair and honest dealing is essential to maintaining trust with audiences and with those who participate in or are otherwise directly affected by ABC content. In rare circumstances, deception or a breach of an undertaking may be justified. Because of the potential damage to trust, deception or breach of an undertaking must be explained openly afterwards unless there are compelling reasons not to do so.

Standards

Dealing with participants

- **5.1** Participants in ABC content should normally be informed of the general nature of their participation.
- **5.2** A refusal to participate will not be overridden without good cause.

Opportunity to respond

5.3 Where allegations are made about a person or organisation, make reasonable efforts in the circumstances to provide a fair opportunity to respond.

Attribution and sources

- **5.4** Aim to attribute information to its source.
- **5.5** Where a source seeks anonymity, do not agree without first considering the source's motive and any alternative attributable sources.
- **5.6** Do not misrepresent another's work as your own.

Undertakings

5.7 Assurances given in relation to conditions of participation, use of content, confidentiality or anonymity must be honoured except in rare cases where justified in the public interest.

Secret recording and other types of deception

- **5.8** Secret recording devices, misrepresentation or other types of deception must not be used to obtain or seek information, audio, pictures or an agreement to participate except where:
 - a justified in the public interest and the material cannot reasonably be obtained by any other means; or

- **b** consent is obtained from the subject or identities are effectively obscured; or
- **c** the deception is integral to an artistic work.

In all cases, the potential for harm must be taken into consideration.

Mandatory referral

- **5.9** An appropriately senior ABC person designated for the purpose must approve in advance, having consulted ABC Legal, any proposal:
 - **a** to use secret recording during the production of content commissioned, produced or co-produced by the ABC; or
 - **b** to broadcast or publish material obtained by deception; or
 - **c** to broadcast or publish without attribution information that forms the basis of a report and the ABC is to be committed to protect the identity of the source of the information; or
 - **d** not to honour an assurance given in relation to conditions of participation, use of content, confidentiality or anonymity.

Related Guidance Notes

Interviewing

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/interviewing/)

Filming with a Remotely Piloted Aircraft (RPA) or drone

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/filming-with-aremotely-piloted-aircraft-rpa-or-drone/)

ABC Indigenous Content

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/abc-indigenous-content/)

<u>Use in News Reports of Pictures from Social Networking Sites</u>

 $\underline{(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/use-in-news-reports-of-pictures-from-social-networking-sites/)}$

Secret Recording Devices in News, Current Affairs and Other Factual Content

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/secret-recording-devices-in-news-current-affairs-and-other-factual-content/)

<u>Impartiality</u>

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/impartiality/)

Fair opportunity to respond

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/fair-opportunity-to-respond/)

Elections (https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/elections/)

Consulting ABC Legal and Handling External Requests for Access to Contentious Program Material (https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/consulting-abc-legal-and-handling-external-requests-for-access-to-contentious-program-material/)

Attribution / Anonymity of Sources

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/attribution-anonymity-of-sources/)

Quick Links

Browse Editorial Policies

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/policies/)

Editorial Guidance Documents

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/)

Visit the full Editorial Policy site

(https://web.archive.org/web/20180123173231/http://about.abc.net.au/how-the-abc-is-run/what-guides-us/abc-editorial-standards/)

Feedback (https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/feedback)

Scope and Note on Interpretation

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/https://edpols.abc.net.au/home/note-on-interpretation-and-scope/)

Recently Added Policy & Guidance

Complaints Handling

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/complaints-handling/)

Interviewing

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/interviewing/)

External Funding of Australia Plus Content

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/external-funding-of-australia-plus-content/)

External Work and Editorial Conflicts

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/external-work-and-editorial-conflicts/)

Domestic Violence

(https://web.archive.org/web/20180123173231/https://edpols.abc.net.au/guidance/domestic-violence/).

Conditions of Use (https://web.archive.org/web/20180123173231/http://www.abc.net.au/conditions.htm) Privacy Policy (https://web.archive.org/web/20180123173231/http://www.abc.net.au/privacy.htm)



(https://web.archive.org/web/20180123173231/http://www.abc.net.au/)

Issued: April 11, 2011 No revision as yet

ATTRIBUTION / ANONYMITY OF SOURCES

Status of Guidance Note

This Guidance Note, authorised by the Managing Director, is provided to assist interpretation of the Editorial Policies to which the Guidance Note relates. Guidance notes provide advice to assist in the interpretation of the Editorial Policies, which contain the standards enforceable under the ABC's internal management processes and under the ABC's complaints handling procedures.

It is expected that staff will normally act in accordance with the advice contained in Guidance Notes. In a given situation there may be good reasons to depart from the advice. This is permissible so long as the standards of the Editorial Policies are met. In such situations, the matter should ordinarily be referred upwards. Any mandatory referrals specified in Guidance Notes must be complied with.

Key Editorial Standards

Excerpts of key editorial standards relevant to this Guidance Note are set out below. Other editorial standards may also be relevant, depending on the specific circumstances applying in each case.

1 Independence, integrity and responsibility

- **1.5** Exercise editorial independence as authorised and accept responsibility for it. When in doubt about an editorial matter, refer it up to the next most senior person for advice or decision.
- **1.6** When any editorial matter, including an editorial matter not being referred up for advice or decision, is likely to cause controversy or have an extraordinary impact, give proper notice of it to the most appropriate senior manager.

5 Fair and honest dealing

Dealing with participants

- **5.1** Participants in ABC content should normally be informed of the general nature of their participation.
- **5.2** A refusal to participate will not be overridden without good cause.

Attribution and sources

- **5.4** Aim to attribute information to its source.
- **5.5** Where a source seeks anonymity, do not agree without first considering the source's motive and any alternative attributable sources.

Undertakings

5.7 Assurances given in relation to conditions of participation, use of content, confidentiality or anonymity must be honoured except in rare cases where justified in the public interest.

Mandatory referral

5.9 An appropriately senior ABC person designated for the purpose must approve in advance, having consulted ABC Legal, any proposal:

..

- **c** to broadcast or publish without attribution information that forms the basis of a report and the ABC is to be committed to protect the identity of the source of the information; or
- **d** not to honour an assurance given in relation to conditions of participation, use of content, confidentiality or anonymity.

Mandatory referrals

The Editorial Standards require (at section 5.9) that an appropriately senior ABC person designated for the purpose must approve in advance, having consulted ABC Legal –

- any proposal to broadcast or publish without attribution information that forms
 the basis of a report and the ABC is to be committed to protect the identity of
 the source of the information; or
- any proposal not to honour an assurance given in relation to conditions of participation, use of content, confidentiality or anonymity.

It is mandatory to disclose a source's identity, if sought, to an appropriately senior ABC person designated for the purpose.

Any proposal not to comply with a lawful order to disclose, or any proposal not to honour an assurance, must be referred to the responsible Divisional Director.

Presumption of attribution

Aim to attribute information to its source [Editorial Standard 5.4]

When media provide information without attribution, audience members are denied an opportunity to consider the source for themselves and to decide how much weight to give to the information in light of who the source is.

Through agreements with media professionals, anonymous sources exercise the power of widespread disclosure of information without having to share responsibility for its reliability and for consequences of its disclosure. That responsibility lies solely with the media professionals and the outlet through which their work is disseminated.

When the ABC carries unattributed information it is, in effect, vouching for the information to the audience. The ABC is asking its audience to take the information on trust and in that way the ABC is investing some of its own credibility in the material.

Negotiating about anonymity

A democratic society protects itself through the free flow of information. Timely public disclosure of information nourishes the formal and informal checks and balances by which such societies hold the powerful to account and debate matters affecting the common good.

There are circumstances in which the public interest is served by media disclosure of information that is not attributed to its source. An example of such a circumstance is the disclosure of official corruption. Disclosure serves the public interest in at least two ways. It can prevent specific consequences harmful to the public interest, such as planning or environmental harms resulting from approvals obtained by bribes. More generally, disclosure serves the public interest because when corrupted official processes are exposed they are more likely to be addressed, and perhaps remedied. Disclosure, by itself or in combination with resulting public opinion, may cause more formal checks and balances to come into operation, such as police, commissions of inquiry, statutory regulators, prosecutors and parliaments.

In some circumstances, if the identity of the source of significant information were to be revealed, the source would be at risk of various types of harm to reputation, livelihood, property or person. Those close to the source, such as family members, may also be at risk. If those who reveal information that serves a significant public interest suffer unjustly, they and other actual or potential sources may be deterred from providing information in future. In this way, the free flow of information may be impeded beyond the context of a specific case.

While anonymity for sources is justifiable in some cases, it should be the exception not the rule. Circumstances in which a source is given a commitment that his or her identity will be protected should involve the public interest in the free flow of information. It is not enough that anonymity merely serves the source's convenience. The information the source is conveying should have genuine public interest value.

Timeliness may also be a factor. In each case, consider whether it is in the public interest that the information, unattributed but corroborated, be disclosed sooner rather than later, even though it may be possible later to disclose with attribution.

Key terms

In negotiating with sources, be clear with them about key terms including —

- On the record, meaning both parties agree that the information conveyed may be disclosed and attributed to the source by name.
- On background, meaning both parties agree that the information conveyed may be disclosed but not attributed in a way that would be likely to identify the source.
- Off the record, meaning both parties agree that the information conveyed is not to be disclosed, with or without attribution.

Harm can result from sources and media professionals having different understandings of what they have agreed to. Misunderstandings may damage mutual trust and confidence between the two individuals involved. The source's attitude to media professionals in general may be adversely affected. Other sources (actual and potential) who observe the consequences of such misunderstandings may be deterred from future dealings. Clarity about the terms of agreements is of

heightened importance when controversies develop, the stakes rise and scrutiny intensifies. Confusion about the terms of an agreement can affect reputations of individuals and media organisations.

Individual staff members will have established and continuing relationships with their own sources. They may use particular terms that are clearly understood between them. Certain terms may be understood by both parties to be synonymous with the definitions given above. Whatever language is used with particular sources when obtaining information, staff should be clear with sources about the terms of agreement prior to disclosure by the ABC of information obtained from the source.

In its own decision-making, the ABC will apply the definitions given above and will reasonably expect that staff have communicated clearly with sources.

Reconsidering the status of the information

Once you have clearly identified yourself as working for the ABC, the information a source conveys is on the record unless agreed otherwise.

Sometimes, a source will attempt retrospectively to place on background or off the record information which he or she conveyed after you identified yourself as working for the ABC. This can be an awkward discussion, especially for the inexperienced. You are not obliged to agree to such requests.

Having identified yourself and your employer, you are entitled to report what the person says. A person may, on reflection, wish to resile from taking responsibility in public for what they have told a media professional. But attribution serves the public best, and you may often need to remain firm and explain that the information is properly on the record.

However, in some circumstances it may be appropriate to negotiate. In making a judgement, factors to consider include —

- The circumstances prevailing at the time the information was conveyed. The
 on the record nature of the exchange may not have been sufficiently clear from
 the outset. Circumstances may be that the source has been drinking or has
 recently woken from sleep, is reeling from serious news just conveyed, or is
 otherwise vulnerable or incapacitated.
- The nature of the information. For example, in the course of an on the
 record exchange the source may convey sensitive information that has low
 public interest value but may unreasonably affect others if disclosed with
 attribution. For example it may infringe the privacy of a member of the
 source's family and neither the information nor its disclosure may be
 material to the story.
- The nature of the source. It may be appropriate to negotiate retrospectively with people who are inexperienced in dealing with media, especially young people, to ensure they are treated fairly. A different type of source, usually highly experienced with media, may be such a significant ongoing source of information of value in serving the public interest that retrospective negotiation may be judged to be a necessary aspect of maintaining the relationship.

Clear understandings, clear purpose

When sources seek to convey information off the record, tell them beforehand that if the information warrants disclosure in the public interest you will try to confirm it through other sources and disclose it.

When a source is told this in advance, it is then up to the source to decide how much to convey. This approach is straightforward and conducive to maintaining trust between you and your source.

Agreements to accept information off the record may include time limits, or be conditional on certain other factors. For instance, you may negotiate that the information that the source wants to convey off the record may change status to 'on background' or even 'on the record' for you if it becomes public through circumstances beyond your control. It may be agreed that the change of status would be automatic, or the agreement may require that you and the source have another conversation if circumstances change.

It can be tempting to agree in advance to receive information off the record in order to become 'in the know'. But it is necessary to be cautious about going into an agreement not to disclose information before you know the precise information. It may be that, having learned what the information is and considering prevailing circumstances, it is in the public interest for the ABC to disclose the information as promptly as possible.

Faced with an offer of information conditional on you being unable to do anything with it, test the source's reasons for wanting to lock you – and through you the ABC – into silence, even temporary silence. In considering the proffered reasons, weigh the seriousness, likelihood and imminence of any harms that could flow from independent efforts by you to corroborate and disclose the information.

Keep in mind that your professional purpose is, at its core, to disclose reliable information in the public interest. Others may have different professional purposes which may be easier for them to accomplish by controlling what information is disclosed to the public. Those purposes may be legitimate, but they are not your purpose.

Considering motive

Where a source seeks anonymity, do not agree without first considering the source's motive and any alternative attributable sources [Editorial Standard 5.5].

A source's motives need not be pure. Long experience teaches that the public interest in the disclosure of information can be served by media professionals cultivating sources who may have mixed motives for seeing the information they provide made public.

Some sources are genuinely altruistic whistleblowers at risk of various types and degrees of harm if their identity as a source is disclosed. The mixed motives of sources who seek anonymity may include: spinning, kite-flying, strewing red

herrings, undermining rivals, salvaging prestige, dampening/heating expectations, avenging defeats, and trading favours.

Acknowledging that sources may have mixed motives does not change the media's need to cultivate sources and gather information, but it does underscore the importance of journalists giving careful consideration to the motives of a source before granting anonymity.

Test whether the source has first-hand knowledge of the matters he or she is conveying.

Seek to confirm the information through independent sources (persons or documents).

Avoid reliance solely on sources to which you are referred by the original source.

Other factors to consider

In negotiating with sources, also consider the following factors —

- **The public interest:** Whether the disclosure of the information unattributed would serve a sufficiently important public interest.
- **Personal attack only?:** Whether disclosure of the information unattributed would amount only to a personal attack made on another person by the source under cover of anonymity provided by you.
- **Timeliness:** Whether the information can be obtained from an attributable source of comparable reliability for disclosure to occur within a time period that would allow the public interest to be adequately served.
- Form of attribution: A form of attribution which, while preserving anonymity, would give the audience an opportunity to weigh the reliability of the information, at least to some extent. Phrases like 'sources said' are unhelpful. The following advice adapts the New York Times' guidance on this point to the Australian context:'Australian diplomat' is better than 'Western diplomat', which is better than 'diplomat'. Still better is 'an Australian diplomat who took part in the meeting'. The phrase 'a person familiar with the case' is vague enough to include the reporter. Better are 'an executive from the plaintiff company' and 'a staff member who has read the draft'.
- No misleading descriptors: Anonymity for the source requires an investment
 of trust in you by the audience (and your colleagues) as well as by the source.
 Do not say 'sources', plural, if there is only one source. Do not give false forms of attribution in order to throw people off
 the scent of the real source:
 for example, 'a parliamentary source' when actually the source works in a
 - department of executive government. Such actions can undermine the story as a whole and may affect the subsequent willingness of others to invest trust.
- Agreed limitations that take effect if circumstances change: Terms of
 agreement can be specific to what is appropriate to the circumstances of the
 case and can include agreed limitations to the anonymity. Limitations may include an express understanding between you
 and the source that if the disclosure of the information supplied by the source causes certain consequences, then the
 source waives the commitment to maintain anonymity. Consequences that may lead to a source agreeing to come forward
 and be identified as the source may include —

- legal proceedings in which you and/or the ABC are lawfully compelled to provide information; or
- the establishment of a process under law, such as a royal commission or parliamentary inquiry, with the capacity to address the issue that the source was trying to bring to light through the media; or
- o an investigation under law by an authority, such as a statutory anticorruption body, with the capacity to protect the source from adverse effects of being identified as the source.

Shared risks and responsibilities

It is not mandatory to refer upwards before approaching sources and obtaining information from sources.

It is obviously impracticable to refer upwards before contacting sources, cultivating them, obtaining information from them and sharing information with them. Multiple such exchanges are desirable and routine in the practice of journalism.

Information gleaned this way may provide leads for further investigation, allow media professionals to acquire fuller background knowledge of events and issues, confirm information obtained elsewhere, and reinforce relationships of trust and confidence.

Individual staff members have broad discretion in dealings with their sources up to the point that the staff member proposes that the ABC disclose, without attribution, information obtained.

The act of disclosure on an ABC platform creates risks and responsibilities for the ABC as well as for the staff member and the source in relation to potential consequences of disclosure.

Among those responsibilities are —

- the support you may expect from the ABC for yourself and your source after the disclosure; and
- the support the ABC may expect from you and your source to prepare and to respond should the ABC be called to account for the disclosure and its consequences.

Shared risks and responsibilities are the basis for the requirements of this part of the Editorial Policies.

Using unattributed information

An appropriately senior ABC person designated for the purpose must approve in advance, having consulted ABC Legal, any proposal ... to broadcast or publish without attribution information that forms the basis of a report and the ABC is to be committed to protect the identity of the source of the information [Editorial Standard 5.9(c)].

This part attempts to ensure that the work of the staff member with the direct relationship with a source is tested through consultation with colleagues before the source's information is disclosed by the ABC without attribution.

Upward referral before an anonymous source is used as the basis of a story has been a requirement of the News Division's Style Guide for some years. It is a common feature of the published standards of many respected media outlets.

The practical effect of this section is to compel consultation that should, and often does, occur as a matter of course when disclosures of significance are being contemplated on the basis of information from an anonymous source.

First, the consultation among colleagues is a check on the natural tendency for journalists to get close to their contacts. They may develop an empathy that clouds their judgement. Colleagues, being at arm's-length, can be more dispassionate. They bring their own knowledge and experience to methods of negotiation, analysis of sources' motives, forms of attribution, reasonable limitations on commitments, and practical protection of sources.

The ABC may seek the identity of a source

Before unattributed disclosure by the ABC of information obtained from a source, the source's identity must, if sought, be made known to an appropriately senior ABC person designated for the purpose.

Mandatory disclosure of an anonymous source's identity to a more senior person has been a requirement of the News Division's Style Guide for several years. The phrase 'designated for the purpose' is intended to give flexibility to the different divisions of the ABC, each of which will have various organisational structures and reporting lines.

A risk that has caused some media outlets very serious harm in the past and would gravely harm the ABC if it eventuated is the risk that a staff member fabricates information, claims the identity of the 'source' can be known to the staff member alone, and claims the 'source' must stay anonymous after disclosure of the information.

Identities of sources may not be sought on every occasion. The requirement relates to disclosures of unattributed information that forms the basis of reports, and to cases in which the ABC is to be committed to protect the identity of the source. It is a matter for the judgement of the designated senior person whether he or she seeks to be told the name of the anonymous source, or is satisfied about the existence and reliability of the source on the basis of other factors including: the particular staff member's reputation; corroboration from independent alternative sources; and the terms of the agreement negotiated with the source in the specific circumstances.

Staff members should ensure that their sources understand that the identity of a source may be required to be shared by the staff member with an appropriately senior ABC person before information is disclosed by the ABC without attribution.

Ensuring practical protection

When committed to protect a source, take care with the precautions necessary to make the protection effective in practice.

A basic rule of journalism is to protect the identity of sources when committed to do so.

Any failure to uphold the rule can result in serious potential costs in loss of trust and reduced information flow, both from the source affected and from potential sources who may be deterred.

Generally speaking, the more significant the information provided by an anonymous source, the greater the risk to the source of retribution or other adverse consequences, and the more intense the efforts by others to discover the source's identity. Some sources may risk reputation, livelihood or even personal safety to provide information for public disclosure in the media.

In striving to maintain protection in practice —

- avoid exposing the source when cross-checking the information the source supplied;
- minimise and keep secure any notes, email exchanges, phone records, drafts and other material which may expose the source's identity;
- consider whether any retained notes can be written in ways that do not identify sources;
- be aware of the risks to the source arising from original documents, photocopies, disks, USB data storage devices and other items supplied by the source;
- be aware that some taxi-payment records show GPS-derived location data about pick-up and drop-off addresses;
- be aware that date/time-stamped CCTV footage in offices may be aligned with dated/timed phone records to indicate who was using a particular phone at the time of a particular call;
- if using vision of the source in the report that is broadcast, blur rather than pixelate (which can be reversed);
- for voiceovers of the source, use another person's voice rather than distort
 by technological means the actual source's voice; consider the potential for details other than face or voice to identify a source
 - for example, clothing, landmarks, street names, vehicle registration number;
- be vigilant to maintain the security of a source even when the source is geographically remote from the place in which the report based on the source's information is first broadcast or published.

Handling hard cases

Experience shows that in this context of source protection, 'hard cases' can and do happen from time to time. In such cases, basic values can clash and choices must be made between promise-keeping and another basic value such as truth-telling.

An appropriately senior ABC person designated for the purpose must approve in advance, having consulted ABC Legal, any proposal ... not to honour an assurance given in relation to conditions of participation, use of content, confidentiality or anonymity [Editorial Standard 5.9(d)].

Where circumstances arise in which a decision needs to be made about whether to maintain a commitment to a source —

- it is mandatory to refer upwards to the Division's Director;
- consult Legal;
- consider whether a release from some or all of the commitment can be negotiated with the source in light of circumstances that have developed since the original commitment was made;
- gather and verify the facts needed to make the decision;
- · identify the competing values;
- analyse the impact of the various options and how to minimise foreseeable harm.

Having taken these steps, decide whether, in the circumstances, substantial advancement of the public interest or the risk of substantial harm to people justifies overriding promise-keeping in order to serve another basic value.

Explain the decision publicly.

Dilemmas can arise in two very distinct settings.

Setting 1

Following a commitment to protect the identity of the source, the information from the source is disclosed but not attributed. Among the consequences of disclosure is a legal process – e.g., defamation action, royal commission, statutory regulator's corruption investigation – in which an enforceable demand is made for the identity of the source to be provided, notwithstanding the source's continuing wish to remain anonymous and notwithstanding the media professionals' objection to identifying the source.

Setting 2

Following a commitment to protect the identity of the source, the information from the source is disclosed but not attributed. Among the consequences of disclosure is a change in circumstances which suggests to the media professionals that the identity of the source ought to be made public, notwithstanding the source's continuing wish to remain anonymous.

Decision-making in either setting requires great care. This Guidance Note sets out a structure for making such decisions. The structure does not pre-determine the outcome of any particular case. The facts of every case will be different. Note that in every case upward referral is mandatory.

By including the decision-making structure in this Guidance Note, and by being willing to explain decisions publicly, the ABC demonstrates that it —

- understands the gravity of each such decision;
- has prepared itself for dealing with such cases responsibly; and
- accepts for itself the public accountability that the ABC's staff routinely require of others.

Further guidance

For further details and reference materials about source protection issues, see the report <u>Sources and Conflicts (http://about.abc.net.au/wp-</u>

<u>content/uploads/2012/06/SourcesAndConflictsReportJuly2008.pdf)</u> and the resources listed in it. See also the ABC News Division Style

Guide. Consult colleagues, learn from their experience, and be willing to share your own.

Related Editorial Policies

<u>5 Fair and honest dealing (https://edpols.abc.net.au/policies/5-fair-and-honest-dealing/)</u>

<u>1 Independence, integrity and responsibility (https://edpols.abc.net.au/policies/1-independence-integrity-and-responsibility/)</u>

Quick Links

Browse Editorial Policies (/policies/)

Editorial Guidance Documents (/guidance/)

<u>Visit the full Editorial Policy site (http://about.abc.net.au/how-the-abc-is-run/what-guides-us/abc-editorial-standards/)</u></u>

Feedback (/feedback)

Editorial Guidance Index

ABC Indigenous Content (https://edpols.abc.net.au/guidance/abc-indigenous-content/)

Accuracy (https://edpols.abc.net.au/guidance/accuracy/)

<u>Advertising and Sponsorship ABC Commercial (https://edpols.abc.net.au/guidance/advertising-and-sponsorship-abc-commercial/)</u>

<u>Advertising and Sponsorship on Australia Plus (https://edpols.abc.net.au/guidance/advertising-and-sponsorship-on-australia-plus/)</u>

Attribution / Anonymity of Sources (https://edpols.abc.net.au/guidance/attribution-anonymity-of-sources/)

<u>Chequebook Journalism / Paying for Interviews (https://edpols.abc.net.au/guidance/chequebook-journalism-paying-for-interviews/)</u>

<u>Children and Young People: Managing their Participation in Broadcast (https://edpols.abc.net.au/guidance/children-and-young-people-managing-their-participation-in-broadcast/)</u>

<u>Children and Young People: Managing their Participation Online (https://edpols.abc.net.au/guidance/children-and-young-people-managing-their-participation-online/)</u>

<u>Competitions and Prizes (https://edpols.abc.net.au/guidance/competitions-and-prizes/)</u>

Complaints Handling (https://edpols.abc.net.au/guidance/complaints-handling/)

Consulting ABC Legal and Handling External Requests for Access to Contentious Program Material (https://edpols.abc.net.au/guidance/consulting-abc-legal-and-handling-external-requests-for-access-to-contentious-program-material/)

<u>Corrections & Clarifications (https://edpols.abc.net.au/guidance/corrective-actions/)</u>

<u>Credits (https://edpols.abc.net.au/guidance/credits/)</u>

<u>Differentiating between factual reporting, analysis and opinion (https://edpols.abc.net.au/guidance/differentiating-between-factual-reporting-analysis-and-opinion/)</u>

<u>Domestic Violence (https://edpols.abc.net.au/guidance/domestic-violence/)</u>

<u>Elections (https://edpols.abc.net.au/guidance/elections/)</u>

External Funding of Australia Plus Content (https://edpols.abc.net.au/guidance/external-funding-of-australia-plus-content/)

External Work and Editorial Conflicts (https://edpols.abc.net.au/guidance/external-work-and-editorial-conflicts/)

Factual Drama (https://edpols.abc.net.au/guidance/factual-drama/)

Fair opportunity to respond (https://edpols.abc.net.au/guidance/fair-opportunity-to-respond/)

<u>Filming with a Remotely Piloted Aircraft (RPA) or drone (https://edpols.abc.net.au/guidance/filming-with-a-remotely-piloted-aircraft-rpa-or-drone/)</u>

Free or discounted products, services or facilities (https://edpols.abc.net.au/guidance/83/).

<u>Guidelines for personal use of social media (https://edpols.abc.net.au/guidance/guidelines-for-personal-use-of-social-media/)</u>

Harm and offence (https://edpols.abc.net.au/guidance/84/)

<u>Impartiality (https://edpols.abc.net.au/guidance/impartiality/)</u>

<u>Interviewing (https://edpols.abc.net.au/guidance/interviewing/)</u>

<u>Managing External Funding in Broadcast Television (https://edpols.abc.net.au/guidance/managing-external-funding-in-broadcast-television/)</u>

<u>Moderating User Generated Content (https://edpols.abc.net.au/guidance/moderating-user-generated-content/)</u>

<u>Operating Official ABC Social Media Accounts (https://edpols.abc.net.au/guidance/operating-official-abc-social-media-accounts/)</u>

Removing Online Content (https://edpols.abc.net.au/guidance/removing-online-content/)

<u>Secret Recording Devices in News, Current Affairs and Other Factual Content (https://edpols.abc.net.au/guidance/secret-recording-devices-in-news-current-affairs-and-other-factual-content/)</u>

Suicide and Self-Harm (https://edpols.abc.net.au/guidance/suicide-and-self-harm/)

<u>Use in News Reports of Pictures from Social Networking Sites (https://edpols.abc.net.au/guidance/use-in-news-reports-of-pictures-from-social-networking-sites/)</u>

Recently Added Policy & Guidance

Reporting and portraying disability in ABC content
(https://edpols.abc.net.au/guidance/reporting-and-portraying-disability-in-abc-content/)

Advertising and Sponsorship ABC Magazines

(https://edpols.abc.net.au/guidance/advertising-and-sponsorship-abc-magazines/)

Accessibility

(https://edpols.abc.net.au/guidance/accessibility/)

Complaints Handling

(https://edpols.abc.net.au/guidance/complaints-handling/)

Interviewing

(https://edpols.abc.net.au/guidance/interviewing/)

ABC Home (http://www.abc.net.au/) About the ABC (http://www.abc.net.au/corp/) Careers (http://www.abc.net.au/careers/) ABC Services (http://www.abc.net.au/services/) ABC Contacts (http://www.abc.net.au/contact/)

© 2014 ABC (http://www.abc.net.au/copyright.htm) Conditions of Use (http://www.abc.net.au/conditions.htm) Privacy Policy (http://www.abc.net.au/privacy.htm)





Our code is now the benchmark for professional ethical behaviour across the industry. MEAA continues to campaign for self-regulation of news media, free from interference by the state.

MEAA is a member of the Australian Press Council and advocates for an all-media self-regulating body.

MEAA Journalist Code of Ethics

Respect for truth and the public's right to information are fundamental principles of journalism. Journalists describe society to itself. They convey information, ideas and opinions, a privileged role. They search, disclose, record, question, entertain, suggest and remember. They inform citizens and animate democracy. They give a practical form to freedom of expression. Many journalists work in private enterprise, but all have these public responsibilities. They scrutinise power, but also exercise it, and should be accountable. Accountability engenders trust. Without trust, journalists do not fulfil their public responsibilities.

MEAA members engaged in journalism commit themselves to

- Honesty
- Fairness
- Independence
- Respect for the rights of others

Journalists will educate themselves about ethics and apply the following standards:

- Report and interpret honestly, striving for accuracy, fairness and disclosure of all essential facts. Do not suppress relevant
 available facts, or give distorting emphasis. Do your utmost to give a fair opportunity for reply.
- 2. Do not place unnecessary emphasis on personal characteristics, including race, ethnicity, nationality, gender, age, sexual orientation, family relationships, religious belief, or physical or intellectual disability.
- Aim to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source. Where confidences are accepted, respect them in all circumstances.
- 4. Do not allow personal interest, or any belief, commitment, payment, gift or benefit, to undermine your accuracy, fairness or independence.
- 5. Disclose conflicts of interest that affect, or could be seen to affect, the accuracy, fairness or independence of your journalism. Do not improperly use a journalistic position for personal gain.
- 6. Do not allow advertising or other commercial considerations to undermine accuracy, fairness or independence.

PHONE

1300 656 513

MEAA.org



- 7. Do your utmost to ensure disclosure of any direct or indirect payment made for interviews, pictures, information or stories.
- 8. Use fair, responsible and honest means to obtain material. Identify yourself and your employer before obtaining any interview for publication or broadcast. Never exploit a person's vulnerability or ignorance of media practice.
- 9. Present pictures and sound which are true and accurate. Any manipulation likely to mislead should be disclosed.
- 10. Do not plagiarise.
- 11. Respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude.
- 12. Do your utmost to achieve fair correction of errors.

Guidance Clause

Basic values often need interpretation and sometimes come into conflict. Ethical journalism requires conscientious decision-making in context. Only substantial advancement of the public interest or risk of substantial harm to people allows any standard to be overridden.

If you feel a MEAA member is in breach of the code, you can lodge a complaint using the process outlined in the *How to Make a Complaint* form.

[129VFED: Incorporates alterations of 06/04/2017 in matter R2017/45]
I CERTIFY under section 161 of the Fair Work (Registered Organisations) Act 2009 that the pages herein numbered 1 to 63 both inclusive contain a true and correct copy of the registered rules of the Media, Entertainment and Arts Alliance.
DELEGATE OF THE GENERAL MANAGER FAIR WORK COMMISSION
[IMPORTANT: Enquiries about these rules or other rules relating to this organisation which are currently in force may be directed to any office of the Fair Work Commission.]

Rules of the Media, Entertainment and Arts Alliance Contents

SECTION 1	1
1 - NAME	1
2. OBJECTS	1
3 - INDUSTRY	4
Part A:	4
Part B:-	
Part C:-	
Part D:	
Part E:-	
Part F:-	
4 - ELIGIBILITY FOR MEMBERSHIP	
Part A:	
Part B:	7
Part C:	8
Part D:	<u>G</u>
Part E:	
Part F:	
Part G:	
Part H:	
5 - DEFINITIONS	
6 - REGISTERED OFFICE	
SECTION 2 - MEMBERSHIP	
7 - ADMISSION TO MEMBERSHIP	
7A – ASSOCIATE MEMBERSHIP	
8 - TEMPORARY & INTERNATIONAL MEMBERSHIP	
9 - ENTRANCE FEES	
10 - SUBSCRIPTIONS	
11 - RIGHTS OF MEMBERS	
12 - DUTIES OF MEMBERS	
13 - MEMBERSHIP HONOURS	
14 - UNFINANCIAL MEMBERS	
15 - TEMPORARY SUSPENSION OF MEMBERSHIP	
16 - RESIGNATION FROM MEMBERSHIP	
17 - REMOVAL FROM THE ROLL OF MEMBERS	
SECTION 3 - BRANCHES	20
18 - BRANCHES	20
19 - BRANCH COUNCIL	20
20 - DELETED	21
22 - DELETED	22
23 - CONTROL OF BRANCH COUNCIL BY MEMBERS	22
24 - DELETED	23
25 - BRANCH OFFICERS	23
26 - BRANCH PRESIDENT	23
27 - BRANCH VICE-PRESIDENTS	23
28 - POWERS & DUTIES OF BRANCH SECRETARIES AND REGIONAL DIRECTORS	23
29 - DELETED	
30 - GENERAL MEETINGS	
31 - ROLL OF MEMBERSHIP	
32 - DELETED	
SECTION 4 - SECTIONS	
33- PROTECTION OF SECTION PROFESSIONAL INTERESTS	
55 TROTLETION OF SECTION TROTESSIONAL INTERESTS	2

34 - SECTIONS	26
35 - SECTIONS 35 - SECTION COMMITTEES.	
36 - DELETED	
37 - DELETED	
38 - DELETED	
39 - SECTION PLEBISCITES.	
SECTION 5 - FEDERAL ORGANISATION	
40 - CONSTITUTION OF FEDERAL COUNCIL	
41 - POWERS AND DUTIES OF THE FEDERAL COUNCIL	
42 - ORDINARY MEETINGS OF FEDERAL COUNCIL	
43 - ORDER OF BUSINESS AT FEDERAL COUNCIL MEETINGS	
44 - EXTRAORDINARY MEETINGS OF FEDERAL COUNCIL	
45 - MEETINGS AND/OR DECISIONS OF FEDERAL COUNCIL MAY BE CONDUCT	
BY FACSIMILE, TELEPHONIC VOTES ETC	
46 - CONTROL OF FEDERAL COUNCIL BY MEMBERS	
47 - FEDERAL OFFICERS	
48 - FEDERAL PRESIDENT	
49 - FEDERAL SECTION PRESIDENTS AND FEDERAL VICE-PRESIDENTS	
50 - POWERS AND DUTIES OF CHIEF EXECUTIVE	
51 - DELETED	
52 - BOARD - POWERS AND DUTIES	
53 - MEETINGS OF THE BOARD	
54 - DELETED	
55 - NATIONAL GENERAL MEETINGS	
56 - DELETED	
SECTION 6 - INDUSTRIAL MATTERS	
57 - INDUSTRIAL DISPUTES	
58 - PROSECUTIONS ON BEHALF OF THE ASSOCIATION	
59 - AGREEMENTS WITH STATE UNIONS	
SECTION 7 - ADMINISTRATION	
60 - SEAL AND EXECUTION OF DOCUMENTS	
61 - AUDITOR	
62 - FINANCIAL YEAR	
63A - DISCLOSURE AND ACCOUNTABILITY	
SECTION 8 - JOURNALISTS' CODE OF ETHICS	
64 - RESTRICTED APPLICATION OF SECTION 8	
65 - AUSTRALIAN JOURNALISTS ASSOCIATION CODE OF ETHICS	
66 - OFFENCES AND COMPLAINTS AGAINST THE CODE OF ETHICS	
67 - ETHICS PANEL	
68 - COMPLAINTS	
69 - APPEALS PANEL	
70A - NATIONAL STUNT COMMITTEE	
SECTION 9 - OFFENCES AND BREACHES OF THE RULES	
71 - OFFENCES AND COMPLAINTS	
72 - REMOVAL FROM OFFICE	
74 - DELETED	
SECTION 10 - RULES	
75 - NEW RULES AND ALTERATIONS OF RULES	
76 - INTERPRETATION OF RULES	
SECTION 11 - AFFILIATION & REPRESENTATION	
77 - AFFILIATION AND REPRESENTATION	
SECTION 12 - ELECTIONS	
78 - TERMS OF OFFICE	
79 - ELECTIONS	56

Contents

Nominations	57
Contested Election	
80 - FORMULA FOR ELECTION OF FEDERAL, BRANCH AND SECTION DELEGATE	S AND
VOTING AT FEDERAL COUNCIL	61
81 - AVOIDANCE OF IRREGULARITIES	62
82 - OFFICERS ILLEGALLY ELECTED.	62
83 - MEMBERS RIGHT TO VOTE IN BALLOT	62
84 - TRANSITIONAL RULES	

SECTION 1

1 - NAME

The name of the Association shall be the Media, Entertainment and Arts Alliance.

2. OBJECTS

The objects of the Association shall be:-

Members

- (a) To regulate, improve and protect the wages and conditions of work welfare and rights of all members including by advancing and protecting the professional interests status and rights of members and the usages and customs of callings covered by the Association, and where considered necessary by the Federal Council of the Association, of persons entitled to become members, and to improve and foster the interests of members of the Association.
- (b) To secure the membership in the Association of all persons who are entitled to become members in accordance with these rules.
- (c) To secure preference in employment and in all aspects of that employment for members of this Association.
- (d) To provide effective representation (including legal representation) to member(s) or any section or group of members in connection with any matter where such representation is considered desirable by the Federal Council or a Branch Council.
- (e) To provide services generally to members (including legal assistance) to member(s) or any section or group of members or access to such services at special or discounted rates in connection with any matter where such services are considered desirable by the Federal Council or a Branch Council.
- (f) To attain sex and racial equality in all spheres of the Association's activity and to oppose all discrimination on the grounds of race, sex, colour, religion, political beliefs, sexual preference or disability.
- (g) To regulate and decide all questions of professional conduct, including, to prescribe and enforce a Code of Ethics to ensure and maintain ethical standards in all areas of journalism.

Education and Training

- (h) To take all steps considered necessary or desirable by the Federal Council or a Branch Council to further and promote the opportunities for training and education of members especially where such training and education has a direct vocational benefit including by the establishment and fostering of schemes of industry training, apprenticeship and the like.
- (h) To ensure that the Association's financial policies and practices accord with all relevant standards and laws and that key financial and operating decisions are disclosed to members in a timely and transparent manner.
- (i) To foster and promote trade union training among the membership.

Benevolent activities

- (j) To provide financial and other assistance at the discretion of the Federal Council of the Association to members in case of accident, death, sickness unemployment or other distress.
- (k) To establish a Benevolent Fund and/or Funds for the benefit of members or former members of the Association.
- (l) To establish funeral, sick, accident, unemployment or other insurance or assurance funds or benefits for the assistance of members of the Association.

Industry Matters

- (m) To ensure that not less than a minimum proportion of resident members as decided by the Federal Council are employed in any film, television or theatrical production.
- (n) To maximise the use of Australian creative resources in all aspects of the media, entertainment and amusement industries and ensure that not less than a minimum proportion of all radio and television programs broadcast in Australia are produced in Australia.
- (o) To promote and attain the use of standard contracts of engagement of the members throughout the industries with which the Association is associated.
- (p) To seek the regulation and control by appropriate legislation if necessary, of the operation of theatrical and other employment and engagement booking agencies and the business methods of theatrical and/or other employment agencies who arrange employment for the members of the Association.
- (q) To issue to members from time to time a list which contains the name of any employer, theatrical agent or employment agent or other person who in the opinion of the Federal Council of the Association has acted in an unfair manner in connection with the employment of any member or members.
- (r) To protect the welfare and rights, including the intellectual property rights, of members including by:
 - (i) seeking appropriate legislation and/or industrial regulation to protect the welfare and rights, including the intellectual property rights, and moral rights, of members and similar rights such as residual, secondary usage, or re-use fees and/or royalties
 - (ii) acting as agent and/or licensor for members in all respects in relation to the authorisation of uses of copyright material and the collection and distribution of copyright fees and similar fees; and
 - (iii) seeking appropriate legislation and/or industrial regulation to protect the welfare and rights of outdoor amusement and recreation workers.

Public Education and Publicity

(s) To promote the objects policies and activities of the Association by means of publications and the media generally.

Co-operation with other Bodies

(t) To co-operate with any other person, for the defence and improvement of theatrical, radio, film and television performances and productions generally, and for the promotion of the arts of the theatre, film, radio and television in all their spheres and to further the establishment and advancement of Australian art and culture within the theatre, live entertainment and in film, radio and television generally.

- (u) To amalgamate with, absorb, affiliate to, or co-operate (including by providing financial assistance thereto) or otherwise combine with, any trade or industrial union or association or associations of trade unions including any international federation of trade unions or similar international bodies, or any other organisations having objects similar in whole or in part to the objects of the Association and to be represented on other bodies and organisations.
- (v) To provide financial or other assistance to and/or participate in the activities of any other union or unions, including any international federation of trade unions or similar international bodies, or any other organisations having objects similar in whole or in part to the objects of the Association.

Trade Union Rights

- (w) To assist members to obtain a fair remuneration for their labour and to assist other trade unions, whether in Australia or overseas to maintain, preserve and advance the interests of labour.
- (x) To uphold the right of all workers to combine for the preservation and advancement of their interests.
- (y) To promote industrial peace by amicable means and to foster and promote means of conciliation to settle industrial disputes.

Management & other Activities of the Association

- (z) To adopt & promote such other objects which are from time to time considered desirable by the Federal Council.
 - (aa) To provide the necessary and reasonable expenses of management of the Association.
 - (bb) To raise funds for the carrying out of the objects, policies and activities of the Association, including by the striking of levies upon members or sections or groups of members for the benefit of those members or sections or groups of members.
 - (cc) To take all steps necessary or desirable to organise and represent the members including by the establishment of sections, sub branches, delegates committees, and delegates, however described.
 - (dd) To hold, purchase, sell, lease, mortgage, borrow or otherwise deal in real property and to enter into agreements in connection with same and to do all such other things as may be deemed necessary in connection therewith.
 - (ee) To initiate and carry into effect in any way considered necessary or advisable by the Federal Council and/or the Board, authorised as herein provided, all or any of the provisions of any statute, state or federal, relating to industrial disputes and arbitration and for all or any such purposes to employ legal or other assistance.
 - (ff) To enforce the rules of the Association.

Cultural Activities

- (za) To promote culture through undertaking activities that advance the professional and industry development of cultural pursuits including literature, music, media, performing arts, visual arts, design, film, video, television, radio, community arts, Indigenous arts and movable cultural heritage.
- (zb) To promote cultural development through activities and industry seminars, forums, workshops, discussion papers and other activities.

Overseas Aid

- (zc) To undertake charitable overseas development and/or relief activities including:
 - (i) to provide support to journalists, media, entertainment and arts workers facing intimidation, discrimination or physical violence;
 - (ii) to provide financial relief to journalists, media, entertainment and arts workers and/or their families:
 - (iii) to provide legal assistance to journalists, media, entertainment and arts workers:
 - (iv) to support human rights advocacy and other collective action by journalists, media, entertainment and arts workers and their unions in support of press freedom and media and journalists rights;
 - (v) to provide support with particular priority to the Asia and Pacific region;
 - (vi) to take any steps thought appropriate to advance the interests of professional and ethical journalism;
 - (vii) to raise funds from members and the public through donations and fund raising activities.

3 - INDUSTRY

Part A:

The industry in connection with which the Association is registered shall be the industry of the employment of every person employed or likely to be employed in or in connection with any of the following industries or callings, namely:

Employees employed in or in connection with, including selling tickets by any means in connection therewith, or in or about, any kind of amusement, whether indoor or outdoor, including:-

- (a) cultural complexes, theatres, halls, racecourses, sports, exhibitions, agricultural shows, planetaria, animal parks, puppet shows and film exchanges, but excluding any person employed in or about the foregoing in any capacity in or in connection with the provision, sale, service or preparation of food or drink;
- (b) Clubs, licensed clubs and discotheques, but only insofar as such employees are employed as set and property carpenters and painters, stage crews, mechanists, projectionists, audio and lighting technicians, flymen, props persons, scenic artists, wardrobe including dressers, costume and property workers, stage managers, make-up artists, hairdressers, wigmakers and wig dressers, directors, choreographers and designers;
- (c) Casinos, but only insofar as such employees are employed as supervisors, pit bosses, inspectors, croupiers, dealers, bankers, cashiers and change clerks, but excluding such persons employed at the Wrest Point Casino, Tasmania;
- (d) In all aspects of Motion Picture Film, Video and Television Production and Processing, the Australian Film Commission and the Australian Film and Television School, including but without limiting the generality of the foregoing Producers, Directors, Production or Studio Unit Managers, Assistant Directors, Production Accountants, Dialogue and/or Commentary Writers, Script and/or Continuity Recordists, Location and/or Talent Scouts, Contact Men, Make-up Artists, Casting Directors, Art Directors, Chief Cameramen, Operative Cameramen, Special and/or Process Cameramen, Title and/or Cartoon Cameramen, Camera Dolly and/or Rotambulation Operators,

Slate Operators, Studio Gripmen, Studio Mechanists, Chief Sound Engineers, Sound Engineers, Sound Recordists, Microphone Boom Operators, Sound Mixers, Film Editors, Film Cutters, Specialist Film Cutters, Film Librarians, Film Vault Keepers, Film Splicers, Laboratory and/or Studio Maintenance Men, Film Stock Keepers, Film Laboratory Managers, Film Laboratory Chemists, Film Printing Operators, Film By- Product Recovery Chemists, Film Timers, Film Cleaners and/or Waxers, Film Checkers, Laboratory and/or Studio Projectionists, Film Processors, Film Graders, Film Despatchers, Film Packers and Film Examiners, Supervising and other classes of Technician involved in Maintenance, Installation, Videotape, Lighting, Telecine or Audio Departments, Cinecameramen, Videocameramen, Set Designers, Graphic Artists, Co-ordinators, Stills Photographers, Floor Managers, Film Sound Recordists, Wardrobe Supervisors and Assistants, Set and Property Carpenters and Painters, Property men/ women, Scenic Artists, Producers/ Directors Assistants, Vision Switchers, Set Dressers, Hairdressers, Film Department Assistants, Studio Hands, Film/Videotape and Record Librarians, Property and Scenery Storemen, and all trainees and inexperienced adults employed in or in connection with television or videotape production houses;

- (e) In film and television distribution, persons employed in film release and control, statistics and contracts, film despatch, (other than officers in charge), projectionists, assistant projectionists, film packers, film checkers, film examiners, film cleaners and film splicers; and
- (f) Cinemas;
- (h) All persons employed or to be employed at World Congress Centre Melbourne and/or the Melbourne Exhibition Centre, other than the employees of contractors providing cleaning, carparking, or food and drink services.

together with such other persons, whether so employed or not as have been elected Officers and Industrial Staff of the Association and have been admitted as members thereof.

and:-

Part B:-

In or in connection with journalism, public relations or authorship in or in connection with the printed media, radio, television, satellite, cable transmission or broadcast or electronic data bases and Hansard, law or other reporting.

and:-

Part C:-

In or in connection with the industry of commercial and industrial art which without limiting the generality of the foregoing includes any business, trade, manufacture, undertaking, calling, service, employment, handicraft or industrial occupation or avocation in the industry or in any branch of the industry including concept visualisation, art direction, art buying, layout, illustration, photography, decorative set and prop design, three dimension and surface packaging design, lettering, typographic design, photo-retouching, video, film graphics, cartooning, finished art and assembly of all design elements including type, provided that it has been set in a recognised trade house and production supervision, book brochure design, map drawing, display and exhibition design, and development of corporate image provided that persons shall not be eligible to join the Association who are employees in or in connection with the printing industry.

Part D:-

The industry of entertaining the public in any place which could reasonably be construed to be a place of entertainment; and of acting, rehearsing or otherwise appearing in cinematographic films and of entertaining and providing and or preparing commercial advertising and/or entertainment, and/or making announcements, and/or devising entertainment for transmission by short or long wave or frequency modulated broadcasting (wireless) transmitters, or televisors or for gramophone recordings.

Part E:-

The Association shall also consist of such independent contractors who, if they were employees performing work of the kind which they usually perform as independent contractors, would be employees eligible for membership of the Association.

Part F:-

Part to reflect orders made under the Industrial Relations Act 1988 (now the Workplace Relations Act 1996) and recorded in Print N5128

Notwithstanding anything elsewhere contained in this rule and without limiting Parts A, B, C, D and E of this rule and without in any way being limited by parts A, B, C, D or E, for the purpose of giving effect to the orders made on 18 September 1996 and recorded in Print N5128 and subject to further order of the Commission to vary or set aside the orders, with effect from 4 July 1997 the industry in connection with which the Association is registered shall include the industry of every person employed or likely to be employed in or in connection with the Live Theatre and Concert Industry which, for the purposes of this rule, shall mean all activities undertaken in or in connection with producing, presenting, or otherwise undertaking live theatrical, performance art, operatic, orchestral, dance, variety, revue, comedy, multimedia, choral, or musical performances, productions, presentations, workshops, rehearsals or concerts, including the provision, sale, service or preparation of food or drink and also including selling tickets by any means, for or in or in connection with any such performances, productions, presentations, workshops, rehearsals or concerts, and including the operation of venues or other facilities, whether permanent or temporary, utilised for such performances, productions, presentations, workshops, rehearsals or concerts, whether or not such performances, productions, presentations, workshops, rehearsals or concerts are performed or presented in the presence of an audience, or are recorded by any means.

4 - ELIGIBILITY FOR MEMBERSHIP

Part A:

the following persons shall be eligible for membership:

Without limiting parts B, C, D or G of this rule and without in any way being limited by parts B, C, D or G:

The Association shall consist of an unlimited number of persons employed on any contractual, (i) weekly, daily or other basis of employment as actors, actresses, singers, choristers, dancers, variety, revue and/or vaudeville artists, circus artists, supernumeraries, extras, understudies, showgirls, models, nudes, mannequins, stand-ins, skaters, aquatic performers, comperes, announcers, narrators and stunt men or women or persons employed for the purpose of commercial display in the theatrical, concert, cabaret, ballroom, hotel, restaurant, club, circus or skating branches of the entertainment industry or in any other place which could be construed to be a place of entertainment, or who are employed as entertainers in any other place, or who are employed in the cinematographic film, television, television film, wireless broadcast recording, commercial wireless broadcasting, or other wireless broadcasting stations, or any other sections of the wireless broadcasting industry, or in the production of gramophone recordings, and all persons employed by or at commercial or other wireless broadcasting stations, or in the production of transcribed radio programs or transcribed commercial announcements for use in wireless broadcasting as monitors, comperes, narrators, members of general information or quiz programs, announcers, monitors of international broadcasts for the purpose of gathering material, translators, checkers, and other persons engaged in the presentation and/or preparation of foreign language broadcasts, and all writers who write specialised radio or television scripts and material as defined in Schedule A hereof, and writers of film scripts and/or scenarios and all persons who are employed at commercial wireless broadcasting stations or elsewhere in the production of transcribed wireless broadcast programs and/or commercial announcements or direct (live) wireless broadcast programs as members of the presentation, program, record library, and/or continuity staff, or in manual sound effects work, or employed as advertising copywriters by a commercial wireless broadcasting station together with such other persons whether employed in the industry or not as have been

appointed officers of the Association (including appointed as Organisers) and admitted as members thereof at present or in the future.

Provided however that an employee whose work in the main consists of writing news or similar commentaries or an employee whose work in the main consists of writing news and similar commentaries and who also verbally broadcasts these commentaries, instrumental musicians other than variety artists, copyists of music, persons engaged on technical and mechanical duties and included within the constitution of the Professional Radio Employees Institute of Australia, or the constitution of the Postal Telecommunication Technicians Association, or employees included within the constitution of the Federated Clerks Union or officers or employees of the Australian Broadcasting Commission who are qualified by the Constitution of the Australian Broadcasting Commission Staff Association to become other than Associate members of the Australian Broadcasting Commission Staff Association, employees engaged solely as clerks, telephonists, watchmen, caretakers, cleaners, or lift attendants or salesmen, copywriters employed by advertising agencies, shall not be eligible for membership.

Schedule A: A writer of specialised radio or television material is one who writes specialised radio or television material, irrespective of length, which is suitable only for radio or television presentation and is pre-designed for that purpose, such as comic or straight dramatic spots, straight plays, including drama, comedy, farce, burlesque & c., musical or variety performances, documentaries in dramatic, musical or other entertainment form and adaptations designed specifically for radio or television performances from an original play or book.

- (ii) Without limiting or in any way being limited by sub-rule (i) of this rule, the Association shall also consist of persons employed as:
 - (a) disc jockeys and discotheque comperes;
 - (b) bingo, housie callers;
 - (c) puppeteers excluding persons whose sole duties are the building, painting and finishing of puppets;
 - (d) stunt co-ordinators and stunt performers;
 - (e) performance artists.

Part B:

the following persons shall be also eligible for membership:

Without limiting parts A, C, D or G of this rule and without in any way being limited by parts A, C, D or G:

The Association shall also be composed of an unlimited number of employees employed in or in connection with, including selling tickets by any means in connection therewith, or in or about, any kind of amusement, whether indoor or outdoor, including:-

- (a) cultural complexes, theatres, halls, racecourses, sports, exhibitions, agricultural shows, planetaria, animal parks, puppet shows and film exchanges, but excluding any person employed in or about the foregoing in any capacity in or in connection with the provision, sale, service or preparation of food or drink;
- (b) Clubs, licensed clubs and discotheques, but only insofar as such employees are employed as set and property carpenters and painters, stage crews, mechanists, projectionists, audio and lighting technicians, flymen, props persons, scenic artists, wardrobe including dressers, costume and property workers, stage managers, make-up artists, hairdressers, wigmakers and wig dressers, directors, choreographers and designers;

- (c) Casinos, but only insofar as such employees are employed as supervisors, pit bosses, inspectors, croupiers, dealers, bankers, cashiers and change clerks, but excluding such persons employed at the Wrest Point Casino, Tasmania;
- In all aspects of Motion Picture Film, Video and Television Production and Processing, the (d) Australian Film Commission and the Australian Film and Television School, including but without limiting the generality of the foregoing Producers, Directors, Production or Studio Unit Managers, Assistant Directors, Production Accountants, Dialogue and/or Commentary Writers, Script and/or Continuity Recordists, Location and/or Talent Scouts, Contact Men, Make-up Artists, Casting Directors, Art Directors, Chief Cameramen, Operative Cameramen, Special and/or Process Cameramen, Title and/or Cartoon Cameramen, Camera Dolly and/or Rotambulation Operations, Slate Operations, Studio Gripmen, Studio Mechanists, Chief Sound Engineers, Sound Engineers, Sound Recordists, Microphone Boom Operators, Sound Mixers, Film Editors, Film Cutters, Specialist Film Cutters, Film Librarians, Film Vault Keepers, Film Splicers, Laboratory and/or Studio Maintenance Men, Film Stock Keepers, Film Laboratory Managers, Film Laboratory Chemists, Film Printing Operators, Film By- Product Recovery Chemists, Film Timers, Film Cleaners and/or Waxers, Film Checkers, Laboratory and/or Studio Projectionists, Film Processors, Film Graders, Film Despatchers, Film Packers and Film Examiners, Supervising and other classes of Technician involved in Maintenance, Installation, Videotape, Lighting, Telecine or Audio Departments, Cinecameramen, Videocameramen, Set Designers, Graphic Artists, Co-ordinators, Stills Photographers, Floor Managers, Film Sound Recordists, Wardrobe Supervisors and Assistants, Set and Property Carpenters and Painters, Property men/women, Scenic Artists, Producers/Directors Assistants, Vision Switchers, Set Dressers, Hairdressers, Film Department Assistants, Studio Hands, Film/Videotape and Record Librarians, Property and Scenery Storemen, and all trainees and inexperienced adults employed in or in connection with television or videotape production houses;
- (e) In film and television distribution, persons employed in film release and control, statistics and contracts, film despatch, (other than officers in charge), projectionists, assistant projectionists, film packers, film checkers, film examiners, film cleaners and film splicers; and
- (f) Cinemas;
- (h) All persons employed or to be employed at World Congress Centre Melbourne and/or the Melbourne Exhibition Centre, other than the employees of contractors providing cleaning, carparking, or food and drink services.

together with such other persons, whether so employed or not as have been elected Officers and Industrial Staff of the Association and have been admitted as members thereof.

The following persons, otherwise eligible for membership of the Association under Part B shall not be eligible for membership by reason of that Part:

All persons employed or to be employed by Kirby Banner Pty Ltd (collectively trading as Movie World Enterprises) at the Movie World Theme Park, Movie Studios (except where such employees are engaged directly in the production of film or television programmes) and Wet'N'Wild Water Slide Complex at Oxenford in the State of Queensland.

Part C:

the following persons shall be also eligible for membership:

Without limiting parts A, B, D or G of this rule and without in any way being limited by parts A, B, D or G:

(a) The Association shall also consist of persons employed or engaged -

Page 8 of 63 Pages

- 1. as journalists, authors, licensed or official shorthand writers, Hansard reporters and publicity and public relations officers;
- 2. in any branch of writing or drawing or photographic work for the press;
- 3. in the collection and/or preparation of news, and/or information on current events for broadcasting or radio transmission;
- 4. in any form of writing, collection and/or preparation of news and/or information on current events, or drawing or news photography for use in television services;
- 5. in any branch of writing or drawing or photographic work for publicity, published instructions or public relations purposes;
- 6. wholly or in major part as script writers, except those engaged solely, or in major part, in the preparation of advertising material for broadcasting or radio or television transmission;
- 7. in the Public Service of the Commonwealth or a State -
 - (a) as journalists in writing and/or preparing matter for publication in newspapers, magazines, books or pamphlets and/or broadcasting and persons performing work of a similar nature as publicity officers or public relations officers;
 - (b) as photographers, the greater part of whose duty is to take and prepare photographs for reproduction in newspapers and/or magazines.
- (b) Only those persons who constantly or regularly perform substantially the work specified in Clause (a) of this Rule, shall be eligible for membership.
- (c) Persons not eligible to be members of the Association are:
 - 1. the Editor-in-Chief and the Editor of a metropolitan daily newspaper;
 - 2. the chief of the general reporting staff permanently employed as such on a daily newspaper in a capital city;
 - 3. a proprietor or part-proprietor of a newspaper who does not derive the major part of his or her income from salary or other remuneration for journalistic work.
 - 4. Any person eligible for membership of the Theatre Managers' Association as at the 27th day of March, 1958.
 - 5. Any person who is a member, staff member or special member of the Australian Federal Police.

Part D:

the following persons shall be also eligible for membership:

Without limiting parts A, B, C or G of this rule and without in any way being limited by parts A, B or C:

The Association shall also consist of an unlimited number of persons

- (a) who are employees or whose occupation is that of an employee in or in connection with the industry as set out in Rule 3, part C;
- (b) who are employees engaged in an industrial pursuit in or connected with the industry as set out in Rule 3, part C;

Page 9 of 63 Pages

- who are employees qualified to be employed in or in connection with the industry or to be engaged as employees in an industrial pursuit connected with the industry as set out in Rule 3, part C;
- (d) who are officers of the Association and who have been admitted as members of the Association.

A person otherwise eligible under sub paragraph (c) of this part shall not be admitted as a member of the Association if such admission shall have the effect of causing the Association to cease being effectively representative of the members employed in or in connection with the industry and the members engaged in industrial pursuits in or connected with the industry.

Provided that persons who are eligible to be members of the Association of Architects Engineers Surveyors and Draughtsmen of Australia in accordance with the registered rules of Association of Architects Engineers Surveyors and Draughtsmen of Australia as at 24 October 1978 shall not be eligible for membership of the Association under this part.

Part E:

The Association shall also consist of such independent contractors who, if they were employees performing work of the kind which they usually perform as independent contractors, would be employees eligible for membership of the Association.

Part F:

No restriction or qualification under parts A B C D or G of this rule shall restrict or qualify eligibility for membership under any other parts of this rule.

Part G:

Part to reflect orders made under the Industrial Relations Act 1988 (now the Workplace Relations Act 1996) and recorded in Print N5128

For the purposes of this rule, the Live Theatre and Concert Industry shall mean all activities undertaken in or in connection with producing, presenting, or otherwise undertaking live theatrical, performance art, operatic, orchestral, dance, variety, revue, comedy, multi-media, choral, or musical performances, productions, presentations, workshops, rehearsals or concerts, including the provision, sale, service or preparation of food or drink and also including selling tickets by any means, for or in or in connection with any such performances, productions, presentations, workshops, rehearsals or concerts, and including the operation of venues or other facilities, whether permanent or temporary, utilised for such performances, productions, presentations, workshops, rehearsals or concerts, whether or not such performances, productions, presentations, workshops, rehearsals or concerts are performed or presented in the presence of an audience, or are recorded by any means.

Notwithstanding anything elsewhere contained in this rule and without limiting Parts A, B, C, D and F of this rule and without in any way being limited by parts A, B, C, D or F, for the purpose of giving effect to the orders made on 18 September 1996 and recorded in Print N5128 and subject to further order of the Commission to vary or set aside the orders, with effect from 4 July 1997 the Association shall also be composed of:

- 1. persons employed or to be employed in all States and Territories of Australia other than Queensland in the Live Theatre and Concert Industry,
- 2. persons employed or to be employed in Queensland in the Live Theatre and Concert Industry,
 - (i) who are eligible to be members of the Association by virtue of Part A, Part C or Part D of this Rule as at 1 January 1996; or

- (ii) who are employed at major performing arts venues in Queensland including but not limited to the Queensland Performing Arts Centre, and the Suncorp Theatre, or at companies or employers in receipt of subsidies from either Commonwealth or Queensland state arts funding bodies, including but not limited to the Queensland Theatre Company, the Queensland Opera, Queensland Ballet, and Dance North, or by companies engaged in the contracting of theatre technical and crewing services, or by the Tjapuki Dance Theatre; or
- (iii) who are employed at venues or by companies associated with institutions of higher learning and including persons employed by student unions or guilds; or
- (iv) who are employed in theatre restaurants; or
- (v) who are employed at the Gold Coast Arts Centre and at Jupiters Casino; or
- (vi) who are employed at venues or by employers in Queensland which are members of the National Association of Regional Performing Arts Centres other than at the NARPAC centre at Redcliffe Queensland.

Part H:

Notwithstanding the provisions of Part A, Part B, Part C, Part D, Part E and Part G of Rule 4, the following persons shall not be eligible for membership of the Union:

All persons employed or to be employed by Village Sea World Operations Pty Ltd and Warner Sea World Operations Pty Ltd (collectively trading as Sea World Enterprises) at the Sea World Theme Park, Gold Coast and its associated facilities; and

All persons employed or to be employed by Janola Dale Pty Ltd, its successors, assignees or transmittees at Dreamworld Theme Park, Coomera, Queensland.

5 - DEFINITIONS

Unless the context otherwise requires, the following construction shall be applied throughout these Rules:

(a)	Associate Member	means an individual or organisation whether incorporated or unincorporated which is not eligible for full membership of the Association
(b)	board	means a group of persons who supervise, govern or otherwise have oversight of a corporation, organisation, association or other like body including a Board of Directors
(c)	Chief Executive	means the senior employee appointed to administer on behalf of the Federal Council and the Board the overall operations of the Association.
(d)	disclosure period	For the purpose of these rules means the financial year unless a shorter period is specified.

- (e) declared person or body A person is a declared person or body if:
 - (i) an officer of the Association or a Branch of the Association has disclosed a material personal interest; and
 - (ii) the interest relates to, or is in, the person or body; and

- (iii) the officer has not notified the Association or a Branch of the Association that the officer no longer has the interest. (f) financial duties includes duties that relate to the financial management of the Association or a Branch of the Association non-cash benefit means property or services in any form other than money, but does not (g) include a computer, mobile phone or other electronic device that is used only or mainly for work purposes. (h) office has the same meaning as defined by section 9 of the Fair Work (Registered Organisations) Act 2009. officer has the same meaning as defined by section 6 of the Fair Work (Registered (i) Organisations) Act 2009. Regional Director means the employee appointed to administer the Association's operations (i) in states and/or territories has the same meaning as defined by section 9B of the Fair Work (k) related party Registered Organisations) Act 2009. relative (1) in relation to a person, means: (i) parent, step parent, child, stepchild, grandparent, grandchild, brother or sister of the person; or (ii) the spouse of the first mentioned person. (m) relevant remuneration in relation to an officer of the Association or Branch of the Association for a disclosure period is the sum of the following: (i) any remuneration disclosed to the Association or Branch of the Association by the officer during the disclosure period; (ii) any remuneration paid during the disclosure period, to the officer of the Association or Branch of the Association. in relation to an officer of the Association or Branch of the Association relevant non-cash (n) benefits for a disclosure period means the non-cash benefits provided to the officer, at any time during the disclosure period, in connection with the performance of the officer's duties as an officer, by the Association or Branch of the Association or by a related party of the Association or Branch of the Association. (o) remuneration (i) includes pay, wages, salary, fees, allowances, leave, benefits or or other entitlements; but (ii) does not include a non-cash benefit; and (iii) does not include the reimbursement or payment of reasonable expenses for the costs incurred in the course of the officer carrying out his or her duties.
- (p) "Member" means a duly admitted member of the Association other than an Associate Member.
- (q) "international member" means a member who is not ordinarily resident in Australia and who is employed in Australia on a temporary basis or pursuant to a contract for a specified duration and/or specified work [e.g. a theatrical or concert tour, film, radio or television programme].

Page 12 of 63 Pages

- (r) "Quarter" means those three month periods ending March 31, June 30, September 30 or December 31 in any year.
- (s) "Half-year" means those six month periods ending June 30 or December 31 in any year.
- (t) The "Association" means the Media, Entertainment and Arts Alliance.
- (u) "Officer" means any person who has been elected or appointed to the Federal Council or the Board or a Branch Council of the Association.
- (v) "Honorary Officer" shall be an office in the Association other than a full-time office provided that the Federal Council and/or the Board from time to time may decide to second such an officer to an employed position within the Association for a limited period or to work on a particular project or assignment.
- (w) "Federal Section Presidents" means Federal President [Media], Federal President [Actors Equity], Federal President [ECS] and Federal President [Musicians].
- (x) "Meeting" includes any meeting held by any means, including by telephone, post, email, on-line or any other electronic manner.
- (y) Senior employee means a person appointed to the position of Director.

Words of the singular number shall include the plural and vice versa. Words of the masculine gender shall include the feminine gender.

6 - REGISTERED OFFICE

The Registered Office of the Association shall be: 245 Chalmers Street Redfern NSW 2016.

The situation of the Registered Office may be altered at the discretion of the Federal Council and such alteration shall be notified immediately to the Federal Industrial Registrar by the Chief Executive.

In each state there shall be Association offices the location of which office may be altered by the Branch Council, with the approval of the Board.

SECTION 2 - MEMBERSHIP

7 - ADMISSION TO MEMBERSHIP

- (a) A person wishing to apply for membership of the Association shall complete an application form approved by the Association. Unless otherwise exempted by the Chief Executive, Branch Secretary or Regional Director, the applicant shall pay an entrance fee according to their category of membership as determined from time to time by the Board.
- (b) The Chief Executive, Branch Secretary or Regional Director shall examine the application and once satisfied that:
 - (i) the person is eligible for membership
 - (ii) the person has paid the required fees or has made arrangement to pay or has been exempted from paying all or part of the required fees

Page 13 of 63 Pages

8 - TEMPORARY & INTERNATIONAL MEMBERSHIP

the Chief Executive, Branch Secretary or Regional Director shall approve the application or refer the application to the next meeting of the Branch Council.

- (c) No error, omission or want of form in connection with any application for or admission to membership shall invalidate membership.
- (d) Each member shall be deemed to be attached to the branch of the Association in which he or she resides and the section to which he or she is allocated by the Branch Council in accordance with the relevant policy regarding allocation to sectional membership then in force provided that where a member's employment is in a branch other than the branch where the member resides [e.g. in a border town or city] the Chief Executive, Branch Secretary or Regional Director may allocate that member to the branch where the member is employed. For the purposes of these Rules members residing in the Northern Territory shall be regarded as residing in South Australia.

And further provided that members of the Professional Sports Branch shall be attached to that Branch no matter where they may reside and shall not be members of any other Branch.

- (e) Each member when allocated to a section shall have the rights and responsibilities of a member of that section as determined by these rules and by the Federal Council. Members who wish to be allocated to more than one section will nominate, and be allocated to, a primary section and will be entitled to vote in sectional elections for that primary section only. Where a member wishes to be allocated to another section or sections or transfer to another section, he or she shall submit an application to that effect to the Chief Executive, Branch Secretary or Regional Director.
- (f) Where a member is admitted to another section or transfers her or his membership, the member shall be required to pay the difference between any entrance fee or subscriptions applicable to that section, unless the amount is waived by the Chief Executive, Branch Secretary or Regional Director.
- (g) Applicants for membership shall be advised by the Association in writing of:
 - (i) the financial obligations arising from membership of the Association; and
 - (ii) the circumstances, and the manner, in which a member may resign from the Association.

7A - ASSOCIATE MEMBERSHIP

An Associate Member is an individual or organisation whether incorporated or not that supports the Association's aims and objectives. Associate Members are persons or entities that are not eligible to become full members under Rule 4. Associate Members can be invited to attend general meetings and speak where invited to do so or where a majority of members present support a request to address the meeting. Neither an Associate Member nor its representative shall be entitled to vote or hold office in the Association or to take part in any election under these Rules.

8 - TEMPORARY & INTERNATIONAL MEMBERSHIP

- (a) The Federal Council of the Association may create categories of temporary membership which will allow the enrolment of members for fixed periods of time.
- (b) International members shall be admitted for the period during which they are contracted to perform services in Australia pursuant to a valid visa. At the end of the such period the member shall cease to be a member of the Association.

Page 14 of 63 Pages

9 - ENTRANCE FEES

- (a) Entrance fees shall be determined by the Board.
- (b) Additional entrance fees shall be payable where a member moves from one category to another or from one section to another. Where this occurs, and the member is admitted to the new category or section, the member shall pay the difference between the entrance fee previously paid by him or her and the entrance fee payable by new applicants coming within the category or section to which he or she has moved. Failure to pay such difference to the Association not later than eight weeks after an account or other written demand for its payment has been forwarded to the member shall render the member unfinancial.
- (c) Payment of all or part of the entrance fee may be waived, reduced or deferred by the Chief Executive, Branch Secretary or Regional Director.

10 - SUBSCRIPTIONS

- (a) Unless relieved of the liability to do so by the Chief Executive, Branch Secretary or Regional Director under these rules, each member shall pay an annual subscription to the Association. Subscriptions shall be fixed each year by the Board no later than April 30 before the financial year in which the subscriptions are to be charged.
- (b) Subscriptions for members in any year shall fall due on the first day of July in that year and shall be payable in advance. They may be paid:
 - (i) yearly;
 - (ii) half-yearly;
 - (iii) by regular deductions from the member's pay;
 - (iv) by regular deductions from a member's bank or similar account or credit card; or
 - (v) by such other means as the Chief Executive, Branch Secretary or Regional Director may approve.
- (c) A member will become unfinancial:
 - (i) in the case of members paying yearly, if payments are not made within two calendar months of July 1 in each year;
 - (ii) in the case of half-yearly payments, if payments are not made within two calendar months of July 1 and/or January 1 in each year; or
 - (iii) in the case of a member paying by regular deductions from the member's pay or from a member's bank or similar account or credit card, if no payments are received for 93 days.
- (d) not certified
- (e) An unfinancial member shall become financial when:
 - (i) All outstanding monies are paid, or
 - (ii) The member enters into a scheme for periodic payments approved by the Branch Secretary.

11 - RIGHTS OF MEMBERS

- (f) The Chief Executive, Branch Secretary or Regional Director may make arrangements with employers or government departments for the deduction, on the signed authority of the member, of entrance fees and/or subscriptions from the members wages or other monies payable to the member, and for the forwarding of such amounts to the Association. Any such arrangements shall conform to any guidelines determined by the Board to apply to such deduction schemes. As long as such authority remains in force, the member shall be regarded as a financial member provided that if no subscriptions are received from a member in respect of employment for three months, the member shall be regarded as an unfinancial member as from the first day of the succeeding half year until such time as a further payment is received or action is taken under either Rule 15 or 17.
- (g) Additional subscriptions may be payable where a member moves from one category to another or from one area of employment or section to another. Where this occurs, and the member is admitted to the new category or section, the member shall pay the difference between the subscriptions previously paid by him or her and the subscriptions payable by new applicants coming within the category or section to which he or she has moved. Failure to pay such difference to the Association not later than eight weeks after an account or other written demand for its payment has been forwarded to the member shall render the member unfinancial.
- (h) Fines and Levies shall be the first charge on all payments by members.
- (i) Any member who fails to pay her/his subscriptions (and/or fines and levies) prior to or upon the due date may also be required thereafter to pay any additional costs incurred by the union in the recovery of the outstanding subscriptions (and/or fines and levies).
- (j) Payment of all subscriptions, entrance fees, levies and fines may be made to any person authorised by the Chief Executive to receive them.
- (k) Payment of any sum due by any member under these Rules may be postponed, reduced or waived by the Chief Executive, Branch Secretary or Regional Director if, in her or his view, it would be appropriate to do so.
- (l) Where payment of subscriptions is postponed by a decision under sub-rule (h), the member shall be regarded as a financial member as from the date of such decision until the date specified in the decision for payment of such postponed amount, provided that any other sums due by the member to the Association are paid in accordance with these Rules.
- (m) Where an amount is reduced or waived by a decision under this sub-rule, the financial status of the member shall be determined as though the amount reduced or waived had been paid by the member on the date of the decision or such other date as may be specified in the decision.
- (n) It shall be the duty of each member without the necessity for any request to do so, to pay his or her subscriptions when required to do so by these rules to any person authorised by the Association to receive such subscriptions.

11 - RIGHTS OF MEMBERS

- (a) Each financial member shall be entitled to all the rights and privileges of membership prescribed in these rules and to participate to the maximum degree possible in the activities of the Association under the Rules. Without limiting these rights, each member shall also be entitled to vote in any relevant election, plebiscite or ballot in accordance with these rules.
- (b) Each financial member shall be entitled to attend any Association, branch, sectional committee or branch council meeting to which he or she is attached as an observer. Provided that such member may be required to leave any such meeting where confidential information is being discussed.
- (c) Any financial member may at a reasonable time during office hours inspect the books and records of the Association or of a Branch upon giving the Chief Executive, Branch Secretary or Regional

Page 16 of 63 Pages

Director as the case may be, 72 hours' notice in writing of their wish to do so <u>provided that</u> the member shall not have the right to inspect any graded, staff or employment list other than that relating to his or her employment or to see any confidential record except that relating to the member personally.

12 - DUTIES OF MEMBERS

- (a) Each member shall be bound by the rules of the Association and each shall take all steps as are reasonable in the circumstances to ensure that the rules of the Association are observed.
- (b) Each member shall pay his or her dues and any other monies owing or due to be paid to the Association without a request to do so having to be made to the member.
- (c) Any member in attendance at a meeting of the Association which is to deal with a matter which affects that member's activity as an employer or agent of an employer shall, immediately prior to discussion of that matter, rise to declare his or her interest. Upon the objection of any other member, the Chair of the meeting shall exclude the member with a declared interest while the particular matter is dealt with.
- (d) Any member who believes that another member should declare his or her interest in a matter shall ask the Chair to give a ruling on whether a declaration of interest should be made. The member under challenge shall have the right to be heard. Upon an interest being found by the Chair, the member under challenge shall be excluded from the meeting during the debate and voting on a matter subject of a declared interest upon one member objecting in accordance with this sub-rule.
- (e) A member who is indebted for any sum of money to the Association in any way whatsoever notwithstanding that the member may not be unfinancial within the meaning of this Rule, shall pay within seven days of his or her receipt from the Chief Executive or Branch Secretary or Regional Director, a demand for payment of such sum of money.
- (f) Each member shall co-operate with the officers of the Association, representatives and workplace delegates.
- (g) A member changing her or his residence shall report this in writing to the Chief Executive, Branch Secretary or Regional Director within twenty-eight days of such change.

13 - MEMBERSHIP HONOURS

(1) Honorary Membership

- (a) The Branch Council may create an Honorary Membership and by resolution may transfer to such membership any financial member or former member who has been a member of the union for no less than 10 years and who has rendered valuable assistance in promoting the Objects of the Association and who is not employed on work defined in rule 4.
- (b) Honorary Members shall not pay any dues to the Association and shall not exercise any voting power. They shall be entitled only to receive notice of any General Meeting, to attend and speak at such meetings, to receive copies of the Association's journal and any report or document issued by the Association to the general membership.
- (c) Honorary Members shall not be included in the membership of the Branch, but a list of Honorary Members may be published in the annual report of the Branch.
- (d) Honorary Members on obtaining employment in work defined in Rule 4 may be readmitted to membership without entrance fee on making application.

(2) Gold Honour Badge

- (a) The Gold Honour Badge of the Association may be awarded by Federal Council to a member for meritorious services, which, in the opinion of the Council, were of conspicuous benefit to the Association.
- (b) The design of the Gold Honour Badge shall be determined by Federal Council.
- (c) Federal Council shall not make an award of the Gold Honour Badge unless at least 75 per cent of delegates vote in favour of such Award.
- (d) A record of the names of members awarded the Gold Honour Badge shall be kept by the Federal President on behalf of the Association.

(3) Honorary Life Membership

- (a) Honorary Life Membership of the Association may be conferred by Federal Council on any holder of the Gold Honour Badge who in the opinion of the Council has given long and outstanding meritorious services additional to those for which the Gold Honour Badge was awarded.
- (b) The Honorary Life Membership list shall be limited to a total of 20 recipients. When that number is reached, no further Honorary Life Memberships shall be bestowed until the number of living Honorary Life Members falls below 20.
- (c) The distinction of Honorary Life Membership shall be conferred only by the unanimous vote of Federal Council.
- (d) Honorary Life Members shall have all the rights and privileges of financial members of the Association.
- (e) A record of the names of members on whom the distinction of Honorary Life Membership has been conferred shall be kept by the Federal President on behalf of the Association.

(4) Honours Previously Granted

Members who immediately before the date of amalgamation enjoyed the status of life membership or long service life membership of the Australian Theatrical and Amusement Employees Association shall be deemed to have an award equivalent to the Gold Honour badge conferred under this rule. Persons conferred with such an honour shall not be required to pay subscriptions whether they are engaged in an occupation covered by Rule 4, part B, or not.

(5) The Federal Council in its discretion may confer upon members the distinction of Honorary Long Service Life Membership for those members who have at least 40 years of continuous membership in the Association. A member granted Honorary Long Service Life Membership shall retain all rights which accrue to financial members of the Association but shall not be required to pay any subscriptions or levy.

14 - UNFINANCIAL MEMBERS

(a) A member who has not paid subscriptions in accordance with rule 10 (or who is not an honorary life member), shall be deemed to be an unfinancial member and shall remain an unfinancial member until such time as all contributions including any fines, levies or other monies payable by the member have been paid.

Page 18 of 63 Pages

16 - RESIGNATION FROM MEMBERSHIP

- (b) An unfinancial member shall not be entitled to:-
 - (i) Any of the rights privileges and benefits of the Association,
 - (ii) Hold any office in the Association,
 - (iii) Nominate for, or vote in, an election to any office,
 - (iv) Nominate any candidate for election to any office,
 - (v) Have access to union records,
 - (vi) Receive notice of any meetings,
 - (vii) Take part in any meeting or proceedings connected with the Association,
 - (viii) Receive copies of any journals, reports or documents issued by the Association.
- (c) The Association may deduct any subscriptions not paid in accordance with rule 10 from any moneys the Association receives on behalf of the member.

15 - TEMPORARY SUSPENSION OF MEMBERSHIP

- (a) Any financial member who expects to be absent from Australia or who expects not to be employed for six months or more on work defined in rule 4 and who desires to retain some form of contact with the Association, may apply to the Chief Executive to be taken off the membership list and placed on a temporary suspension list. Unless the Chief Executive decides otherwise, only persons who agree to notify the Association when they resume employment in the industry shall be eligible to be placed on the temporary suspension list.
- (b) Persons who are placed on the temporary suspension list shall not pay any fees to the Association and shall not be members of the Association for the period of being on the temporary suspension list.
- (c) A person on the temporary suspension list on obtaining employment covered by Rule 4 shall again become a member entitled to all rights, privileges and benefits of membership provided they make themselves financial in accordance with Rule 10.
- (d) If a person whose membership is temporarily suspended takes up work and does not notify the Association the members' dues shall become payable as and from the date when the member so resumes work.
- (e) A person on the temporary suspension list shall, if he or she desires, receive copies of any relevant Association publication. The Board may require a subscription fee for any publication.
- (f) The Association may deduct an administrative charge from any moneys the Association receives on behalf of a member who has placed his/her membership on temporary suspension.

16 - RESIGNATION FROM MEMBERSHIP

(a) A member may resign her or his membership of the Association by notice in writing and such resignation shall take effect:

Page 19 of 63 Pages

19 - BRANCH COUNCIL

- (i) Where the member has ceased to be eligible to become a member of the Association on the day on which the notice of resignation is received or a later date if that later date is specified in the notice; or
- (ii) In any other case, at the end of two weeks after the day on which the notice of resignation is received or a later date if that later date is specified in the notice.
- (b) Notice of resignation shall be in writing, addressed and delivered to the Chief Executive, Branch Secretary or Regional Director.
- (c) For the purposes of this Rule, subscriptions payable shall be calculated on a quarterly basis. Nothing in this rule shall mean that any or all subscriptions, fines and levies owed by the member to the Association and payable on the date on which the resignation is to take effect and unpaid, shall not continue as a debt owed by the member to the Association.
- (d) The Association may deduct an administrative charge from any moneys the Association receives on behalf of a member who has resigned his/her membership of the Association.

17 - REMOVAL FROM THE ROLL OF MEMBERS

The Chief Executive may at any time purge the roll of membership by striking off the names of members:

- (i) who are in arrears of more than six months;
- (ii) who have ceased to be eligible to become a member of the Association;
- (iii) whose address is unknown; or
- (iv) who are deceased,

but such action shall not free any such discharged member from liability for the arrears at the time the member is removed from the roll.

The Association may deduct an administrative charge from any moneys the Association receives on behalf of a member whose membership has been purged from the roll.

SECTION 3 - BRANCHES

18 - BRANCHES

- (a) Federal Council may by resolution establish branches within the membership to reflect geographical locations and/or occupational groupings within the Association.
- (b) Provided that no branch shall be dissolved, amalgamated or have its boundaries altered without first being consulted by the Board, or where authorised by the Board, the Chief Executive and approved by the Branch Council of the affected Branch or by a vote of Federal Council carried by no fewer than 75% of the votes exercised by Federal Councillors.

19 - BRANCH COUNCIL

(a) Subject to these rules, the supreme governing body of each Branch of the Association shall be the Branch Council.

Page 20 of 63 Pages

- (b) The Branch Council shall be responsible for the general conduct and control of the Branch of the Association within the powers and decisions of the Federal Council and the Board.
- (c) Federal Council, in consultation with the Branch, shall determine that the Branch Council shall consist of either:
 - (1) (i) the Branch President
 - (ii) three Branch Vice-Presidents
 - (iii) the Branch Secretary (in those branches where Federal Council has approved the creation of a Branch Secretary)
 - (iv) Delegates from the sections of the Association as determined by Rule 80 [other than in those branches where Federal Council has determined that the number of delegates shall be zero].

Or

- (2) (i) the Branch President of each section that has more than 100 financial members within the Branch
 - (ii) the Branch Vice-President of each section that has more than 500 financial members within the Branch
 - (iii) the Branch Secretary (in those branches where Federal Council has approved the creation of a Branch Secretary)
 - (iv) Delegates from the sections of the Association as determined by Rule 80 [other than in those branches where Federal Council has determined that the number of delegates shall be zero].
- (d) The Branch Council shall meet whenever convened by the Branch President, or whenever determined by the Branch Council or the Board. Notice of any such meeting shall be given to all members of Branch Council by the officer convening the meeting. Where practicable, such notice shall be given in writing.
- (e) Notwithstanding any other rule precluding an officer being an employee of the Association, the Branch Council may, with the approval of the Board, in the case of absence of the Branch Secretary or Regional Director, appoint another member of the Association, eligible under the rules, to act as Branch Secretary or Regional Director for the period of such absence provided that no such appointment shall exceed 12 months. A member appointed under this rule may hold another office in the Association during such appointment.
- (f) The Branch Council shall decide all matters in accordance with these Rules. A decision of Branch Council shall be final and binding throughout the Branch and shall remain in force until superseded, amended or rescinded either at a subsequent meeting of the Branch Council, by the Board or Federal Council or by decision of the members reached by plebiscite of the Branch or Association.
- (g) The Branch President or in his or her absence, a Branch Vice-President shall preside at all Branch Council meetings or in the absence of these officers, a Chair shall be elected by the Council members present.
- (h) A quorum of members at a Branch Council meeting shall be a majority of the members, provided that the Board may approve a lesser quorum of no less than a third of the members.
- (i) If any member of Branch Council fails to attend three succeeding meetings without the leave of the Council, the Branch Council may declare the office vacant and seek to fill the office in accordance with rule 79(u).

20 - DELETED

21 - DELETED

22 - DELETED

23 - CONTROL OF BRANCH COUNCIL BY MEMBERS

- (a) All decisions of the Branch Council shall be subject to review by the members either by decision of a special general meeting or by the members voting in a plebiscite.
- (b) A special general meeting of members of the Branch may be called to consider a decision of the Branch Council where a petition of financial members signed by not fewer than 5% of the financial members of the Branch requests it.
- (c) The special general meeting so called may consider a resolution referring the decision of the Branch Council to the Federal Council. Where a resolution to that effect is carried, the Chief Executive shall take all necessary steps to refer the matter to the Federal Council for review of the decision of the Branch Council within eight weeks of the request of the special general meeting being made.
- (d) Alternatively, a Branch plebiscite shall be held to review a decision of the Branch Council where a petition of financial members signed by not fewer than 10% of the financial members of the Branch request it.
- (e) A request for a plebiscite must be made within eight weeks of the decision of Branch Council sought to be reviewed.
- (f) Where a valid request for a plebiscite is made, the Branch Council shall appoint a returning officer who shall:-
 - (i) Take all such steps and have all necessary authority to conduct such plebiscite;
 - (ii) Set out the question to appear on the ballot paper,
 - (iii) Fix a date and time for the issue of ballot papers by the returning officer and also a date and time for the closing of the plebiscite,
 - (iv) Ensure that a full and fair explanation as to the reason for the plebiscite, and the competing views as to whether members should vote for or against it, accompanies the ballot paper.
- (g) A ballot paper issued in relation to this rule, shall be in the following form:-

"Are you in favour of the following......".

Then follows the resolution of Branch Council on which the plebiscite is being taken.

YES() NO()

- (h) The Branch returning officer shall conduct such ballot in accordance with rule 79 of these rules and any member may arrange to attend to scrutinise the returning officer's activities. The returning officer shall conduct the plebiscite promptly.
- (i) The Branch Secretary or Regional Director shall submit the report of the Returning Officer to the next meeting of the Branch Council.

28 - POWERS & DUTIES OF BRANCH SECRETARIES AND REGIONAL DIRECTORS

(j) Any decision of the members voting in plebiscite shall be final and binding on the Branch of the union and its members until superseded by another plebiscite decision, or a decision of the Federal Council or, once a period of 25 years has elapsed, a decision of the Branch Council.

24 - DELETED

25 - BRANCH OFFICERS

The Branch Officers of the Association shall be in each branch the officers listed in either 19(c)(1)(i) and (ii) or 19(c)(2)(i) and (ii), and where determined by Federal Council, with the consent of the relevant Branch, Branch Secretary.

26 - BRANCH PRESIDENT

The Branch President shall:-

- (a) Be the senior officer of the branch and preside at all meetings of the branch and superintend the discussion of all business tabled for consideration.
- (b) Have a deliberative vote.
- (c) Be an ex-officio member of all sections, sub-branches, committees and sub-committees formed within the branch to advise the Association on matters concerning members or other Association matters and have the right to move and second motions, speak and vote at all meetings whether Council, Section, Committee or Sub-Committee or Special or General Meetings of members. The President may delegate this power, except the right to vote, to any member of the Branch Council to represent the President at any such meeting except at a meeting of the Branch Council.
- (d) Sign the Minutes of the proceedings of all meetings of the branch.
- (e) Where practicable, the Branch President shall be consulted by the Branch Secretary or Regional Director where urgent matters of substance arise between Branch Council meetings which require an urgent decision by the Branch Secretary or Regional Director. Any decisions so taken shall be reported to the Branch Council at the earliest opportunity by the Branch President, Branch Secretary or Regional Director.
- (f) The Branch President shall observe and cause to be observed all the rules, policies and decisions of the Association.

27 - BRANCH VICE-PRESIDENTS

- (a) There shall be three Branch Vice-Presidents. One of the Branch Vice- Presidents shall take the chair in the absence of the Branch President and thereupon shall have and may exercise all the powers of the Branch President.
- (b) In ordinary cases, one of the Branch Vice-Presidents shall assist the President in maintaining order at the meetings of the branch.

28 - POWERS & DUTIES OF BRANCH SECRETARIES AND REGIONAL DIRECTORS

The Branch Secretary or Regional Director (whichever is applicable) (and a person appointed to act as Branch Secretary or Regional Director in a temporary capacity in accordance with these Rules) shall conscientiously, efficiently and expeditiously do all things required to safeguard the interests of members and of the branch as a whole and:-

[129VFED: Incorporates alterations of 06/04/2017 in matter R2017/45] Page 23 of 63 Pages

30 - GENERAL MEETINGS

- (a) Attend all general meetings of the branch and Branch Council, keep the Minutes of such meetings (and send a copy of each set of minutes when completed, to the Chief Executive), and take note of all the necessary proceedings.
- (b) Be an ex-officio member of all sections, sub-branches, committees and sub-committees formed within the branch to advise the Association in matters concerning members or other Association matters and, in the case of Branch Secretaries, have the right to move and second motions, speak and vote at all meetings whether Council, Sub-branches, Section, Committee or Sub-Committee or Special or General Meetings of members.
- (c) On request of the Board or Federal Council or on a request signed by a majority of Branch Council members or on resolution of a General Meeting, hand over all books, documents and papers of the branch to a person named in such request within twenty-four hours of the receipt of such request, always provided that the provisions of these Rules relating to the removal of and/or suspension of officers shall prevail.
- (d) Obey the directions of the Branch Council regarding branch affairs.
- (e) Attend to all correspondence related to Branch affairs.
- (f) Take all such steps as are necessary and are required by the Branch Council, for the participation of the branch in a state industrial relation system.
- (g) Observe and cause to be observed all the rules, policies and decisions of the Association.

29 - DELETED

30 - GENERAL MEETINGS

- (a) Meetings which all the members of Branch are entitled to attend shall be known as Branch General Meetings. Meetings which all members of a section within a Branch are entitled to attend shall be known as Section General Meetings.
- (b) A general meeting may be convened at any time by:
 - (i) resolution of the Branch Council or Branch Sectional Committee as the case may be;
 - (ii) a request in writing signed by not less than five per cent of the financial members of the Branch or of the section as the case may be.
- (c) A general meeting shall be called by the Branch Secretary or Regional Director or in his or her absence, the Branch President, by notice giving at least 14 days notice either by:
 - (i) providing notice to each financial member at his or her last known address; or
 - (ii) forwarding a notice to all places of work where more than three members are employed and to theatrical and employment agents (where applicable).
- (d) The notice calling the meeting shall set out the place, date and time of the meeting and the nature of the business to be brought before the meeting.
- (e) The quorum necessary to transact business at general meetings shall be:
 - (i) At least 15 financial members in a branch with a financial membership not exceeding 200.

Page 24 of 63 Pages

33- PROTECTION OF SECTION PROFESSIONAL INTERESTS

- (ii) Two more financial members for each 100 financial members thereafter, provided that no quorum shall exceed 85.
- (iii) general meeting quorums shall be calculated by Branches according to the following table:

Financial Members	Quorum	Financial Members	Quorum
0-200	15	1501-1600	43
201-300	17	1601-1700	45
301-400	19	1701-1800	47
401-500	21	1801-1900	49
501-600	23	1901-2000	51
601-700	25	2001-2100	53
701-800	27	2101-2200	55
801-900	29	2201-2300	57
901-1000	31	2301-2400	59
1001-1100	33	2401-2500	61
1101-1200	35	2501-2600	63
1201-1300	37	2601-2700	65
1301-1400	39	2701-2800	67
1401-1500	41	2801-2900	69

and thereafter an extra 2 members for each additional 100 members of the Branch to a maximum of 85 members.

- (f) A general meeting shall be called not later than 14 days after the receipt by the Branch Secretary or Regional Director, or in his or her absence the Branch President, of a request in writing signed by not less than 5 per cent of the financial members of the Branch or section as the case may be.
- (g) A general meeting shall not be convened in accordance with sub-rule (f) hereof for the purpose of reviewing any action or resolution of a Branch Council or section committee unless such request is made within eight weeks of the action or resolution which it is proposed to review.
- (h) A general meeting shall have the power to require the Branch Council or Section Committee or in the case of a matter of federal importance, the Board or Federal Council, to deal with a matter. The relevant body shall deal with the matter promptly.

31 - ROLL OF MEMBERSHIP

A register of the names of the officers and members resident in each branch, their postal addresses, sections and place of work (as far as known), shall be kept at the office of the branch and shall be open for inspection at all convenient times to the Industrial Registrar or any persons appointed by him or her. The register may be kept in a computerised form.

32 - DELETED

SECTION 4 - SECTIONS

33- PROTECTION OF SECTION PROFESSIONAL INTERESTS

(a) Notwithstanding anything else contained in these rules, the policies adopted by the Association regarding the professional standards and interests of members of any section (and in relation to

Page 25 of 63 Pages

Journalists the establishment of a code of professional ethics) shall be determined exclusively by the section of the Association concerned. Such issues shall include the admission to membership of prospective members and approval of the entry to the country and the issue of permission to take up employment of those prospective members.

- (b) This rule shall only be altered with the consent of each of the sections of the Association and only after a plebiscite of each of the sections approves of any such alteration in accordance with the rule alterations rule 75.
- (c) For the purposes of this rule, professional standards and interests shall not include matters pertaining to wages and conditions of employment.

34 - SECTIONS

- (a) The Federal Council shall by resolution, establish sections within the membership to reflect occupational or industry groupings within the Association.
- (b) Upon the establishment of each section, the Federal Council shall issue a charter to the section, defining the scope of the section, and allocate members to each section.
- (c) Any dispute about the scope and membership of a section shall be determined by the Board, subject to appeal to the Federal Council.
- (d) New members shall be required to nominate a section which corresponds with their primary employment in the industry in accordance with Rule 7 of these rules. Once allocated to a section, a member shall not be reallocated without the approval of the Branch Council. A member shall be allocated to a primary section and may stand for any elective office and vote only as a member of that section.
- (e) The Federal Council shall have the power, subject to this sub-rule, to decide that a section shall be dissolved or amalgamated with another section. The size of a section shall be a factor to be taken into account by the Federal Council when making such a decision. No section shall be dissolved or amalgamated without first being consulted by the Federal President, and approved by the national sectional committee of the section concerned or by a vote of Federal Council carried by no fewer than 75% of votes exercised by Federal Councillors.

35 - SECTION COMMITTEES

- (a) Federal Council may approve the formation of a National Section Committee in any section.
- (b) The National Section Committee shall consist of all members of Federal Council who are members of that section and the vice-presidents of each branch entitled to three or more votes at Federal Council in accordance with Rule 80 where the holder of that office is member of the relevant section but not also a member of Federal Council.
- (c) Each member of the section committee shall exercise a single deliberative vote. Decisions shall be by a majority of votes cast.
- (d) A National Section Committee may adopt by-laws to govern its conduct and activities, subject to the approval of those by-laws by the Federal Council.
- (e) The National Section Committee may approve the formation of a State Section Committee in any State. A State Section Committee shall consist of all members of Federal Council who are members of the relevant section in that State together with all members of the Branch Council in that State who are members of the relevant section and such other members as are co-opted by the State Section Committee.

Page 26 of 63 Pages

39 - SECTION PLEBISCITES.

- (f) The National Section Committee shall have the power to make recommendations to the Board and Federal Council on all matters pertaining to that section especially those matters affecting the policies and industrial objectives to be adopted by the Association.
- (g) The State Section Committee shall have the power to make recommendations to the Branch Council and National Section Committee on all matters pertaining to that division especially those matters affecting the policies and industrial objectives to be adopted by the Association.
- (h) Each recommendation of a National Section Committee or a State Section Committee shall be considered by the relevant deliberative body at its next ordinary meeting except in cases of urgency.

36 - DELETED

37 - DELETED

38 - DELETED

39 - SECTION PLEBISCITES.

- (a) All decisions of a Section Committee shall be subject to review by the members of that section either by decision of a special general meeting or by the members of that section voting in a plebiscite.
- (b) A sectional plebiscite shall be held to review a decision of the National Sectional Committee or Branch Sectional Committee where a petition of financial members signed by not fewer than 5% of the financial members of the section or in the case of a Branch matter 10% of the financial members of the section attached to the branch in question requests it.
- (c) The Federal Council or a Branch Council with the approval of the Federal Council, may conduct a plebiscite on any question affecting a section or sections.
- (d) Where the plebiscite seeks to review a decision of the Association, a request for a plebiscite must be made to the Federal President or Branch President as the case may be within eight weeks of the decision sought to be reviewed.
- (e) Where a valid request or decision to hold a plebiscite is made, the Board or Branch Council (as the case may be) shall appoint a returning officer who shall:-
 - (i) Take all such steps and have all necessary authority to conduct such plebiscite;
 - (ii) Set out the question to appear on the ballot paper,
 - (iii) Fix a date and time for the issue of ballot papers by the returning officer and also a date and time for the closing of the plebiscite,
 - (iv) Ensure that a full and fair explanation as to the reason for the plebiscite, and the competing views as to whether members should vote for or against it, accompanies the ballot paper.
- (f) A ballot paper issued in relation to this rule, shall be in the following form:-

"Are you in favour of the following......?"

Then follows the question or matter on which the plebiscite is being taken.

 $YES() \qquad NO()$

Page 27 of 63 Pages

40 - CONSTITUTION OF FEDERAL COUNCIL

- (g) The returning officer shall conduct such ballot in accordance with rule 79 of these rules and any member may arrange to attend or to be represented by a scrutineer to scrutinise the returning officer's activities. The returning officer shall conduct the plebiscite promptly.
- (h) The Federal President or Branch President as appropriate, shall submit the report of the Returning Officer to the Board or the Branch Council.
- (i) Any decision of the members voting in plebiscite shall be final and binding on the section unless overturned by a subsequent plebiscite or by a decision of Federal Council or, once a period of 25 years has elapsed, a decision by the section committee.

SECTION 5 - FEDERAL ORGANISATION

40 - CONSTITUTION OF FEDERAL COUNCIL

- (a) Subject to these rules, the supreme governing body of the Association shall be the Federal Council.
- (b) The Federal Council shall consist of:
 - (i) All members of the Board in accordance with rule 52
 - (ii) Delegates from the sections as determined by rule 80
 - (iii) Delegates from Branches as determined by sub-rule (c) of this rule
- (c) Provided that, where Federal Council has approved a Branch to operate in any state, the delegates shall be:

In the case of NSW and Victoria, the Branch Officers.

In the case of any other Branch with officers determined by Rule 19(c)(1), the Branch President and, if applicable, the Branch Secretary.

In the case of any Branch with officers determined by Rule 19(c)(2), the Branch Officers.

- (cc) In any state where the Federal Council has not approved a Branch to operate, there shall be one delegate.
- (d) No member shall hold two positions on Federal Council.
- (e) Each member of Federal Council shall exercise a single vote.
- (f) No proceeding of the Federal Council shall be affected by or rendered void by reason only that one or more casual vacancies in the respective offices of those bodies has or have occurred and has or have not been filled.
- (g) Where a member of Federal Council is unable to attend a meeting of Federal Council, a financial member may be appointed as an alternative member of Federal Council to attend Federal Council in his or her place. A person so appointed shall exercise all the powers and duties of the person whom they are replacing. The appointment may be revoked at any time. The appointment shall be made by:
 - (i) the relevant Branch Council in the case of a branch representative
 - (ii) the relevant National Section Committee in the case of a sectional delegate
 - (iii) the Board in the case of a federal officer.
- (h) Any member of Federal Council may appoint another member of Federal Council as a proxy for the first member where that member is unable to attend all or part of the Council meeting and

Page 28 of 63 Pages

41 - POWERS AND DUTIES OF THE FEDERAL COUNCIL

where no alternate member of Federal Council has been appointed in place of the first member. The appointment shall be with the leave of the Council. A person so appointed shall exercise their own vote and that of the person who has appointed them as a proxy. The appointment as a proxy may be revoked at any time.

41 - POWERS AND DUTIES OF THE FEDERAL COUNCIL

The Federal Council shall have the general conduct and control of the business of the Association, and in that regard shall have complete authority to take any action it considers necessary or desirable on policy, management or any matter concerning the Association and/or its members, and without limiting the foregoing, such powers shall include:-

- (a) The overall management of the affairs of the Association whilst recognising that day to day management shall be in the hands of the Board and administered by the Board through the Chief Executive:
- (b) The determination, enforcement and protection of the policy of the Association in relation to the industrial and/or professional welfare of members, or any other matter of concern to the Association;
- (c) The amendment, rescission or alteration of the rules of the Association;
- (d) The enforcement of the rules of the Association;
- (e) Any action it considers necessary or advisable concerning any industrial claim or actual, threatened, impending or probable industrial dispute or in settlement of any industrial claim or dispute, and to authorise the Chief Executive to serve logs of claims on such general classes or groups of employers as it may determine from time to time. Such logs of claims may take such form as the Chief Executive shall determine unless specified otherwise by Federal Council.
- (f) The determination of the rate of entrance fees, payments and contributions to be paid by members of the Association.
- (g) The determination of the proportions of Association funds to be allocated to Branch funds.
- (h) The imposition and enforcement of the payment of levies on all or a portion of members provided that where a levy is imposed on a section of the membership, it shall be used for the benefit of that section.
- (i) The creation, re-formation or abolition of any branch or section, including the power to direct a branch to establish and organise a particular section or sections, and, subject to these rules, the determination of its authority, territory and membership provided that no branch shall be abolished or have its territory reduced without consultation.
- (j) In accordance with these Rules, the delegation of its authority, except the power to delegate, to the Board, and subject to the control of the Board, the Chief Executive. Such delegations shall continue in force unless and until subsequently rescinded or varied by Federal Council.
- (k) The determination of the wages and conditions of employment of officers and employees, and of any honoraria or similar payment and the discipline and dismissal of officers of the Association;
- (l) The accumulation, investment, custody and disposition of the property and funds of the Association, including the power to enter into any arrangements to secure mortgages or similar arrangements;

Page 29 of 63 Pages

42 - ORDINARY MEETINGS OF FEDERAL COUNCIL

- (m) To require financial reports from branches and sections, and to demand or cause to be made an audit of the books and accounts of any branch or division, and for that purpose take possession of all property, books bank books, documents and correspondence from any branch or office thereof.
- (n) The calling of any meeting of the Board, any Branch Council, Sectional Committee or Section or, sub-branch or of any members or category or group of members of the Association.
- (o) Hearing and determining appeals from any member or group of members aggrieved by a decision of a Branch Council including any decision dealing with the removal of an officer of the Branch Executive.
- (p) To submit any matter to a plebiscite of members or the members of a section.

The Federal Council shall endeavour to ensure that throughout Australia, as far as practicable, a uniform level of service to the members is provided, having regard to the nature and size of the membership of particular branches and sections and any special needs of the membership.

The Federal Council shall decide all matters in accordance with these Rules and have power to decide any questions or matter not provided for by these Rules. A decision of Federal Council shall be final and binding throughout the Association and shall remain in force until superseded, amended or rescinded either at a subsequent meeting of Federal Council or by decision reached by plebiscite.

42 - ORDINARY MEETINGS OF FEDERAL COUNCIL

- (a) A face to face meeting of the Federal Council shall be held at least every two years.
- (b) Business may be placed on the agenda paper for Federal Council by:
 - (i) any Branch Council;
 - (ii) any sectional committee;
 - (iii) any officer or Federal Councillor.

Such items shall be circulated in accordance with (d) hereof.

- (c) Federal Council shall be held in the month of November unless the Board decides on or before June 30 in each year to fix an alternative date and time for the opening of the meeting.
- (cc) The Chief Executive shall notify all Federal Councillors and Branches of the date and time of Federal Council and invite agenda items for the business paper.
- (d) Each Federal Councillor shall notify the Chief Executive of all business he or she desires to place on the agenda paper for the Federal Council meeting at least six weeks prior to the date of such meeting. The Chief Executive shall forward to each Branch Secretary or Regional Director and all Federal Councillors, a copy of the agenda paper at least 28 days prior to such annual meeting of the Federal Council.
- (e) A member of Federal Council may place before a meeting of Federal Council any item not on the agenda paper of the Federal Council if two-thirds of members of Council agree.
- (f) A quorum at any Federal Council meeting shall consist of at least one representative from each of at least three branches and 50% of the Council members.

Page 30 of 63 Pages

43 - ORDER OF BUSINESS AT FEDERAL COUNCIL MEETINGS

- (a) On assembling of the Federal Council, the Federal President shall take the chair. In the absence of the Federal President the Senior Deputy Federal President shall take the chair. In the absence of these officers the members assembled shall vote one of their own members to act as Chair for the time being.
- (b) The Federal President shall cause to be read or table the credentials of the various delegates.
- (c) Unless Federal Council decides otherwise the order of business thereafter shall be as follows:-
 - (i) Appointment of Minutes Secretary,
 - (ii) Confirmation of Minutes of previous Federal Council Meeting and all ensuing meetings of the Board,
 - (iii) Acceptance of urgent business,
 - (iv) Sessions of Federal Council,
 - (v) Federal Presidents address.
 - (vi) Annual Report, Balance Sheet and Statement of Accounts,
 - (vii) Sectional agenda items,
 - (viii) General Business,

44 - EXTRAORDINARY MEETINGS OF FEDERAL COUNCIL

- (a) An Extraordinary Meeting of the Federal Council shall be convened by the Federal President upon the request of:
 - (i) the Board;
 - (ii) Two or more branch councils of branches representing not less than a majority of the members of the Association;
 - (iii) A majority of Branch Councils; or,
 - (iv) By a request of the delegates from a section supported by a petition of 33% of the members of the section.
- (b) Extraordinary meetings shall be convened within twenty-eight days of the receipt by the Federal President of any such request, unless the Board determines otherwise.
- (c) A branch or section making a request for an Extraordinary Federal Council Meeting pursuant to this Rule shall notify the Federal President in writing incorporating in such notification the business which it wishes discussed, giving reasons in support of its request. Provided that a request made by two or more branches collectively within a period of fourteen days of each other pursuant to clause (b) hereof, it shall be considered a valid request for the purpose of this Rule, if business submitted by a branch bears a reasonable resemblance to business submitted by any other branch making such request and such requests must quote the Rule under which the request is made.

(d) The Federal President shall cause to be provided to all Federal Councillors, agenda items submitted by branches for any such Extraordinary Meeting as soon as is practicable prior to such meeting.

45 - MEETINGS AND/OR DECISIONS OF FEDERAL COUNCIL MAY BE CONDUCTED/TAKEN BY FACSIMILE, TELEPHONIC VOTES ETC

The Board shall determine the form of an extraordinary meeting of Federal Council. This may include by face to face, post, facsimile or electronic conference facilities or similar methods.

46 - CONTROL OF FEDERAL COUNCIL BY MEMBERS

(a)	All decisions of the Federal Council shall be subject to review by the members voting in a
	plebiscite.

(b)	A plebiscite may be	eauested to review	a decision of the	Federal Council	where requested by	V
(-)						,

- (i) the Board, or
- (ii) Two or more Branch Councils of branches representing not less than a majority of the members of the Association, or
- (iii) A majority of Branch Councils or,
- (iv) The delegates from a section supported by a petition of 33% of the members of the section, or
- (v) A petition of financial members signed by not less than 5% of financial members.
- (c) A request for a plebiscite must be made within eight weeks of the decision of Federal Council sought to be reviewed.
- (d) Where a valid request for a plebiscite is made, the Board shall appoint a returning officer who shall:-
 - (i) Take all such steps and have all necessary authority to conduct such plebiscite;
 - (ii) Set out the question to appear on the ballot paper,
 - (iii) Fix a date and time for the issue of ballot papers by the returning officer and also a date and time for the closing of the plebiscite,
 - (iv) Ensure that a full and fair explanation as to the reason for the plebiscite, and the competing views as to whether members should vote for or against it, accompanies the ballot paper.
- (e) A ballot paper issued in relation to this rule, shall be in the following form:-

"Are you in favour of the following......".

Then follows the resolution of Federal Council on which the Plebiscite is being taken.

YES () NO ()

(f) The returning officer shall conduct such ballot in accordance with rule 79 of these rules and any member may attend to scrutinise the returning officer's activities. The returning officer shall conduct the plebiscite promptly.

Page 32 of 63 Pages

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (g) The Federal President shall submit the report of the Returning Officer to the next meeting of the Board and shall send a copy of it to each Federal Councillor.
- (h) Any decision of the members voting in plebiscite shall be final and binding on the union and its members unless overturned by a subsequent plebiscite or, once a period of 25 years has elapsed, by a decision of the Federal Council.

47 - FEDERAL OFFICERS

The Federal Officers of the Association shall be the Federal President, Four Federal Section Presidents, Federal Vice-Presidents, and as determined by Federal Council.

48 - FEDERAL PRESIDENT

- (a) The Federal President shall preside at all meetings of the Federal Council, the Board and preserve order so that business may be conducted in due form and with propriety.
- (b) The Federal President shall at all times be under the control of the Federal Council and the Board.
- (c) The Federal President shall have the right to move motions, to vote and speak on Federal Council and on the Board and when speaking on a motion before the meeting shall vacate the chair and allow the senior Federal Section President to temporarily assume the chair.
- (d) The Federal President shall have the right to attend and speak at any meeting of the Association.
- (e) The Federal President shall observe and cause to be observed all the rules, policies and decisions of the Association.

49 - FEDERAL SECTION PRESIDENTS AND FEDERAL VICE-PRESIDENTS

- (a) The duties of the Federal Section Presidents and Federal Vice-Presidents shall be to assist the Federal President at all meetings of the Federal Council and, in the absence of the Federal President, a Federal Section President or Vice-President shall take the chair, conduct the business and perform all the duties of the Federal President.
- (b) Where a Federal Section President is to carry out a function or exercise a power under these rules and more than one Federal Section President is available to do so, the most senior shall do so seniority shall be determined by the number of votes which the Federal Section President received at the preceding election or where this method of establishing seniority cannot be achieved seniority shall be determined by lot.
- (c) Where no Federal Section President is available, and a Vice-President is to carry out a function or exercise a power under these rules and more than one Vice President is available to do so, the most senior shall do so seniority shall be determined by the number of votes which the Vice President received at the preceding election or where this method of establishing seniority cannot be achieved seniority shall be determined by lot.

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (a) The Board will appoint a Chief Executive. The Chief Executive will be employed pursuant to a contract of employment, the conditions and remuneration of which shall be determined by the Board.
- (b) The Chief Executive shall at all times be under the control of the Federal Council and the Board.

Page 33 of 63 Pages

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (c) The Chief Executive shall be appointed to administer the Association's affairs.
- (d) The Chief Executive shall observe and cause to be observed all the rules, policies and decisions of the Association.
- (e) The Chief Executive shall not have the right to vote at any meeting of the Federal Council or the Board.
- (f) The Chief Executive shall exercise the powers set out in this rule in accordance with the directions and/or delegations given by the Federal Council or the Board or shall so exercise them subject to subsequent ratification by the Board at its next meeting. Provided that in the absence of any determination by the Board to the contrary, the exercise of these powers shall be taken to be at the direction of the Board.
- (g) The Chief Executive shall have the power to serve logs of claim, to execute Industrial Agreements and Awards and rescissions or variations thereof by or on behalf of the Association, and at his or her discretion, lodge objections with the relevant Industrial Authority (including the General Manager of the Fair Work Commission) which he or she believes necessary to protect the interests of the Association.
- (h) The Chief Executive shall have the power to make all necessary decisions on the management and activities of the Association between meetings of the Board either in consultation with the Federal President or subject to ratification by the Board at its next meeting. Any such decisions shall be consistent with the decisions of Federal Council and the Board and the objects of the Association.
- (i) The Chief Executive shall have power to convene General Meetings of members in any branch or division or of members of the Branch Council in the event of a Branch Secretary's or Regional Director's refusal or neglect to do so. The Chief Executive shall have the power to convene meetings of the Federal Council or may perform any such duties that may be considered by the Board necessary or desirable in the interests of the Association.
- (j) If the Chief Executive has reason to believe the action of any Branch Secretary, Regional Director or Branch Council is contrary to the Rules, Awards and stated policies of the Association, he or she shall, in consultation with the Federal President have power to nullify same, providing the position of the Branch Secretary or Regional Director or Branch Council and also of the Chief Executive shall, within seven days, be submitted in writing to the Board who shall decide the matter. While the matter is under submission to the Board, the practice objected to shall discontinue.
- (k) The Chief Executive may be a member of any Committee formed by the Federal Council or the Board to advise the Association on any subject, and shall have the right to attend and speak, but not exercise a vote, at any Branch Council, Section Committee or general or special meeting of any branch or section.
- (l) The Chief Executive shall not pay, lend or otherwise appropriate any of the funds of the Association for any purpose except in accordance with these Rules, resolutions and minutes of the Federal Council and the Board.
- (m) The Chief Executive shall be responsible for the employment and supervision of all staff of the Association.
- (n) The duties of the Chief Executive shall be, inter alia:-
 - (i) To attend all meetings of the Federal Council and the Board and cause to be taken minutes of such meetings and to circulate copies of the minutes to all members of the Federal Council or the Board as the case may be as soon as possible and in any event no later than fourteen days after the conclusion of the meeting.

Page 34 of 63 Pages

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (ii) To act generally according to the direction of the Federal Council and the Board and to this end to delegate duties to senior employees and supervise and manage the work of these employees and the industrial and office staff.
- (iii) To summon members of the Federal Council and the Board to meetings.
- (iv) To keep a correct account of all monies received and expended together with dates of receipts and expenditure.
- (v) To pay all monies received by him or her into the Association's bank account to the credit of the Association as soon as possible but no later than within fourteen days.
- (vi) To produce books of accounts at all reasonable times when required by the Federal President, Federal Council or the Board .
- (vii) To submit books, accounts and receipts annually or as often as may be required or directed by the Federal Council or the Board, to the Auditor.
- (viii) To sit, if required, with the Auditor when he or she is auditing the Association's accounts.
- (ix) To prepare the Annual Report and assist in the preparation of the Annual Financial Report for submission.
- (x) To attend promptly to, keep and produce copies of all correspondence and provide details thereof reasonably required.
- (xi) To be responsible for the drafting, serving, filing and lodging of all Federal Industrial Logs of Claims and Award variations.
- (xii) To cause to be kept and maintained a national register of members showing the name and postal address of each member and a list of names, postal addresses and occupations of all officers of the Association and each branch.
- (xiii) To visit each branch of the Association where practicable.
- (xiv) To forward to the General Manager of the Fair Work Commission, a copy of the financial reports and returns in accordance with the Fair Work (Registered Organisations) Act 2009 and Regulations, as amended from time to time.
- (xv) To notify each member of the Federal Council of the time and place of the Biennial Meeting of the Federal Council at least six weeks before the date thereof and send to each member of the Federal Council, as early as practicable and not later than twenty eight days prior to the Biennial Meeting of the Federal Council, an agenda of the business to come before such meeting.
- (xvi) To exercise overall editorial control and policy of the publications of the Association.
- (xvii) To forward each year to the General Manager of the Fair Work Commission, such returns as required by him or her.
- (xviii) To forward within thirty days of notification of any change taking place in the Officers of the Association, a statement to the General Manager of the Fair Work Commission of such change.
- (xix) To forward to the General Manager of the Fair Work Commission within thirty-five days after any alteration has been made in the Rules of the Association, a notice and copy of any rule alterations made and certified by the Federal President.

Page 35 of 63 Pages

52 - BOARD - POWERS AND DUTIES

- (xx) To supervise and co-ordinate the industrial organisation of members in the callings for which the Association is constituted throughout Australia.
- (xxi) Subject to the Act and in accordance with any directions of the Federal Council or Board, to do all things necessary to be done by an organisation registered under the Fair Work (Registered Organisations) Act 2009.
- (xxii) To organise and establish branches when instructed to do so by the Board or Federal Council.
- (xxiii) To make careful inquiries in any branch deemed by him to be mismanaged and report the result of such inquiries to the Board who shall be empowered to instruct him/her, if necessary, to take over the affairs of such branch until control of such branch is determined under Section 9 of these Rules.
- (xxiv) To dispatch a copy of the Statement of Accounts and Balance Sheet of each branch to each other branch.
- (xxv) To use his or her best endeavours to keep branches informed of all matters relevant and of interest to the Branch.
- (xxvi) To prepare a report for submission to the Board and Federal Council on the finances and funds of the Association.
- (xxvii) To take all steps necessary to ensure that elections are held for both branch and Federal Offices in accordance with these Rules.
- (xxviii) To submit matters for determination to Federal Council and the Board when properly requested to do so under these Rules, or when necessary for the good management or pursuit of the objectives of the Association.
- (xxix) Any duties which may be delegated by the Federal Council or Board under these rules from time to time.

51 - DELETED

52 - BOARD - POWERS AND DUTIES

The Board shall be the authority to

- (a) administer and manage the affairs of the Association when the Federal Council is not in session.
- (b) appoint a Chief Executive and, in consultation with the relevant Branch Council, appoint Regional Directors.
- (c) make, amend and rescind administrative decisions concerning the exercise of the functions by the Association's Chief Executive and senior employees of the Association.
- (d) The Board shall wherever possible, consult branches and sections before initiating or determining any question involving policy. The Board may exercise all of the powers of the Federal Council except the power to:
 - (i) Add to, amend or rescind the Rules of the Association; or

Page 36 of 63 Pages

- (ii) Act contrary to or alter or revoke any decision of Federal Council unless authorised to do so by a decision of a membership plebiscite.
- (e) All decisions of the Board shall be binding throughout the Association and shall remain in force unless superseded, amended or rescinded by Federal Council or by a plebiscite of members or by a subsequent meeting of the Board.
- (f) The Board shall consist of:
 - (i) All federal officers under Rule 47:
 - (ii) One financial member elected by and from each Branch with more than 900 financial members as at June 30 immediately prior to the biennial elections; and
 - (iii) One financial member elected by and from all other Branches.
- (g) Each member of the Board shall have the right to move and second motions, and speak and cast a single vote on any motion. Decisions shall be by the majority of votes cast.
- (h) The Federal President or, in his or her absence, a Federal Section President shall chair meetings of the Board.
- (i) Where a member of the Board is unable to attend all or part of any meeting of the Board, the Board may appoint a financial member as an alternative to attend the Board in his or her place. A person so appointed shall be a person eligible under these rules to stand for the position held by the person they are replacing. He or she shall exercise all the powers and duties of the person whom they are replacing. The appointment may be revoked at any time.
- (j) Any member of the Board may appoint another member of the Board as a proxy for the first member where that member is unable to attend all or part of the Board meeting and where no alternate member of the Board has been appointed in place of the first member. The appointment shall be with the leave of the Board. A person so appointed shall exercise their own vote and that of the person who has appointed them as a proxy. The appointment as a proxy may be revoked at any time.

53 - MEETINGS OF THE BOARD

- (a) The Board shall meet at least six times in each year unless otherwise decided by Federal Council. Meetings of the Board shall be convened by the Federal President.
- (b) A Meeting of the Board shall be convened by the Federal President upon the request of three or more Branch Councils or two or more Section Councils. Such Meetings shall be convened within twenty-eight days of the receipt of such requests by the Federal President.
- (c) The Federal President shall cause to be provided to all Board members agenda items for any meeting as soon as is practicable prior to the meeting.
- (d) A quorum for Board meetings shall be half the members.
- (e) All meetings of the Board shall be called upon such notice of the date and place of the meeting as is reasonable in the circumstances.
- (f) All meetings of the Board shall be notified in advance to all members of the Board by the Federal President by notice including proposed agenda items for such meetings in order to allow members of the Board, branches and sections to submit further agenda items for the consideration of the Board.

Page 37 of 63 Pages

- (g) The Board may decide to consider such additional agenda items as it thinks fit.
- (h) Meetings of the Board may be held and decisions may be taken by means of post or facsimile or email or by the use of telephone or electronic conferencing or other facilities.

54 - DELETED

55 - NATIONAL GENERAL MEETINGS

- (a) A national general meeting which all members of the Alliance are entitled to attend may be convened by:
 - (i) Resolution of Federal Council
 - (ii) A request in writing signed by not less than five percent of the financial members of the Alliance.
- (b) A national general meeting shall be called by the Federal President by notice giving at least 14 days' notice either by:
 - (i) providing a notice to each financial member to his or her last known address;
 - (ii) forwarding a notice to all places of work where more than three members are employed and to theatrical and employment agents; or
 - (iii) placing a notice on the Alliance web page and sending an email notification to the last known email address of each financial member
- (c) The notice calling the meeting shall set out the place(s), date(s) and time(s) of the meeting and the nature of the business to be brought before the meeting.
- (d) The Board may determine that the meeting should be held as a series of gatherings in different cities at different times to consider a common resolution.
- (e) The quorum necessary to transact business at a national general meeting shall be at least 5 per cent of the financial membership of the Alliance.
- (f) A national general meeting shall be called not later than 28 days after the receipt by the Federal President of a request in writing signed by not less than 5% of the financial members of the Alliance.
- (g) A national general meeting shall not be convened in accordance with sub-rule (f) hereof for the purpose of reviewing any action or resolution of the Alliance unless such request is made within eight weeks of the action or resolution which it is proposed to review.
- (h) A national general meeting shall have the power to require the Board or Federal Council to deal with a matter. The relevant body shall deal with the matter promptly.

56 - DELETED

SECTION 6 - INDUSTRIAL MATTERS

57 - INDUSTRIAL DISPUTES

- (a) Federal Council, the Board or the Federal President or the Chief Executive is empowered to take any action considered necessary or desirable in connection with any industrial dispute or probable industrial dispute.
- (b) The Board or the Federal President or the Chief Executive shall have authority to enter into an industrial agreement or award, on behalf of the Association.
- (c) An industrial dispute may only be submitted
 - (i) To any federal court or tribunal on the authority of the Federal President or the Chief Executive;
 - (ii) To a State industrial court or commission on the authority of the Federal President, the Chief Executive, Branch Secretary or Regional Director.

58 - PROSECUTIONS ON BEHALF OF THE ASSOCIATION

- (a) The Federal President shall be:
 - (i) the registered Officer of the Association for the purposes of the industrial legislation.
 - (ii) empowered to act on behalf of the Association.
 - (iii) the Officer to sue and be sued on behalf of the Association.
 - (iv) empowered on behalf of the Association to lay any information under any Act of Parliament under which proceedings can or may be instituted on behalf of the Association for any offence or any recovery proceedings for an unpaid wages, superannuation contribution and/or other similar benefit.
- (b) In each state, the Branch President or the Branch Secretary or Regional Director of the relevant branch shall also have power in respect of any matter arising within the state to lay any information or take proceedings to recover any penalty under any State Act of Parliament by the provisions of which the Association or any authorised person may take proceedings.
- (c) In any proceedings or matter to which it is necessary that some other person shall exercise the power to sue on behalf of the Association, such person shall be deemed to be so authorised on production of a letter to that effect bearing the Seal of the Association signed by the Federal President or duly authorised Board Member.

59 - AGREEMENTS WITH STATE UNIONS

The Federal Council and the Board are authorised to enter into (and terminate) an agreement with a State registered union regarding coverage and representation of members.

Page 39 of 63 Pages

SECTION 7 - ADMINISTRATION

60 - SEAL AND EXECUTION OF DOCUMENTS

The Seal of the Association shall be kept by the Association. The affixture of the seal to any documents shall be attested to under the hand of the Federal President or duly authorised Board member.

61 - AUDITOR

- (a) A properly qualified Auditor (or auditors) not an Association member, shall audit the accounts of the Association yearly.
- (b) The Auditor(s) shall be appointed by the Board.
- (c) The Auditor shall have the power to call for all books, papers, vouchers and documents belonging to the Association. He or she shall furnish the report upon the books, Balance Sheets and accounts verifying correctness or otherwise.

62 - FINANCIAL YEAR

The Financial Year of federal and branch offices shall terminate on the thirtieth day of June in each year and all books and accounts shall close on that date. A duly audited Balance Sheet of the Association shall be caused to be presented to Federal Council by the Federal President. The Balance Sheet shall show all items of receipts and expenditure and the assets and liabilities, of the Association.

63 - FINANCIAL MANAGEMENT

- (a) Unless otherwise determined by Federal Council all assets and liabilities shall be vested in the Federal Council and administered between meetings by the Board.
- (b) The Board shall adopt a budget at the beginning of each financial year setting out the budgeted income and expenditure for the year.
- (c) The Federal President shall ensure the Board is advised on progress in meeting the Association's budget and any significant deviations from the budget. The Board may approve variations to the budget.
- (d) Monies of the Alliance shall be banked in the name of the Media, Entertainment & Arts Alliance.
- (e) Any payments of monies shall be authorised by the Federal President or such other people who may be authorized by the Board from time to time.
- (f) Expenditure shall only be approved as is in accordance with the objects of the Alliance.
- (g) The Alliance may invest the monies of the Alliance in
 - (i) real estate or other property
 - (ii) shares or other securities
 - (iii) bank accounts or other cash instruments
 - (iv) such other investment as the Alliance may deem appropriate
- (h) Where assets are held in the name of officers or other members, these officers or members shall be required to execute a deed of trust that they are merely trustees for the Alliance.

Loans, Grants and Donations

- (i) A loan, grant or donation of an amount exceeding \$1,000 shall not be made by the Association or any branch thereof as the case may be unless the Board or Council of the branch concerned, as the case may be, has satisfied itself -
 - (i) that the making of the loan, grant or donation would be in accordance with the other rules and policy of the Association; and
 - (ii) in relation to a loan that, in the circumstances, the security proposed to be given for the repayment of the loan is adequate and the proposed arrangements for the repayment of the loan are satisfactory; and,

it has approved the making of the loan, grant or donation.

Moneys held on trust

- (j) The Association may receive and hold moneys on trust, including moneys held on trust for members or people eligible to be members.
- (k) Moneys held on trust shall be banked in an account or accounts specifically designated for that purpose.
- (1) The Association shall:
 - (i) take all reasonable efforts to distribute moneys held on trust to financial members entitled to the money:
 - (ii) deduct any amount owing by a member to the Association from any amount received by the Association on behalf of that member and take all reasonable efforts to distribute the balance, if any, to the member;
 - (iii) deduct an administrative charge, determined from time to time as appropriate by Federal Council, or by the Board from any amount received by the Association on behalf
 - of any person who is neither a financial member or a non-financial member of the Association and take all reasonable efforts to distribute the balance to that person;
 - (iv) the Association shall not be required to distribute amounts of less than \$50 or such other amount as determined by Federal Council;
 - (v) the Association shall accept no liability for tax or superannuation levy or any other liability arising out of the payment;
 - (vi) any amounts not able to be distributed within six years of being received by the Association may be applied by the Association for the interests of the general class of people for whom the money was received, provided that if, after six years, any member can assert a right to any money received, the Association shall make good that money; and
 - (vii) unless provided otherwise by the terms of the trust, the Association may apply any net interest or related earnings for the interests of the general class of people for whom the money was received.

Public Funds

- (m) The Association may establish and maintain an Alliance Gift Fund as a public fund.
 - (i) Donations will be deposited into the public fund listed on the Register of Cultural Organisations. These monies will be kept separate from other funds of the Association and will only be used to further the objects of the Association. Investment of monies in this fund will be made in accordance with guidelines for public funds as specified by the Australian Taxation Office.
 - (ii) The fund will be administered by a management committee or a subcommittee of the management committee, the majority of whom, because of their tenure of some public office or their professional standing, have an underlying community responsibility, as distinct from obligations solely in regard to the cultural objectives of the Association.
 - (iii) No monies/assets in this fund will be distributed to members or office bearers of the Association, except as reimbursement of out-of-pocket expenses incurred on behalf of the fund or proper remuneration for administrative services.
 - (iv) The Department responsible for the administration of the Register of Cultural Organisations will be notified of any proposed amendments or alterations to provisions for the public fund, to assess the effect of any amendments on the public fund's continuing Deductible Gift Recipient status.
 - (v) Receipts for gifts to the public fund must state:
 - the name of the public fund and that the receipt is for a gift made to the public fund:
 - the Australian Business Number of the company;
 - the fact that the receipt is for a gift; and
 - any other matter required to be included on the receipt pursuant to the requirements of the Income Tax Assessment Act 1997.
 - (vi) Winding-up clause
 - If upon the winding-up or dissolution of the public fund listed on the Register of Cultural Organisations, there remains after satisfaction of all its debts and liabilities, any property or funds, the property or funds shall not be paid to or distributed among its members, but shall be given or transferred to some other fund, authority or institution having objects similar to the objects of this public fund, and whose rules shall prohibit the distribution of its or their income among its or their members, such fund, authority or institution to be eligible for tax deductibility of donations under Subdivision 30-B, section 30-100, of the Income Tax Assessment Act 1997 and listed on the Register of Cultural Organisations maintained under the Act.
- (n) The Association may establish and maintain an overseas aid fund, known as the Media Safety and Solidarity Fund, as a public fund.
 - (i) Donations will be deposited into the public fund as gazette by the Australian Taxation Office. These monies will be kept separate from other funds of the Association and will only be used to further the objects of the Association. Investment of monies in this fund will be made in accordance with guidelines for public funds as specified by the Australian Taxation Office.
 - (ii) The fund will be administered by a management committee or a subcommittee of the management committee, the majority of whom, because of their tenure of some public office or their professional standing, have an underlying community responsibility, as distinct from obligations solely in regard to the cultural objectives of the Association.

- (iii) No monies/assets in this fund will be distributed to members or office bearers of the Association, except as reimbursement of out-of-pocket expenses incurred on behalf of the fund or proper remuneration for administrative services.
- (iv) The Australian Taxation Office will be notified of any proposed amendments or alterations to provisions for the public fund, to assess the effect of any amendments on the public fund's continuing Deductible Gift Recipient status.
- (v) Receipts for gifts to the public fund must state:
 - the name of the public fund and that the receipt is for a gift made to the public fund;
 - the Australian Business Number of the company;
 - the fact that the receipt is for a gift; and
 - any other matter required to be included on the receipt pursuant to the requirements of the Income Tax Assessment Act 1997.

(vi) Winding-up clause

If upon the winding-up or dissolution of the public fund gazette by the Australian Taxation Office, there remains after satisfaction of all its debts and liabilities, any property or funds, the property or funds shall not be paid to or distributed among its members, but shall be given or transferred to some other fund, authority or institution having objects similar to the objects of this public fund, and whose rules shall prohibit the distribution of its or their income among its or their members, such fund, authority or institution to be eligible for tax deductibility of donations under Subdivision 30-B, section 30-100, of the Income Tax Assessment Act 1997 and gazette by the Australian Taxation Office.

- (o) The Association may establish and maintain an Alliance Necessitous Circumstances Fund as public fund.
 - (i) Donations will be deposited into the public fund as gazette by the Australian Taxation Office. These monies will be kept separate from other funds of the Association and will only be used to further the objects of the Association. Investment of monies in this fund will be made in accordance with guidelines for public funds as specified by the Australian Taxation Office.
 - (ii) The fund will be administered by a management committee or a subcommittee of the management committee, the majority of whom, because of their tenure of some public office or their professional standing, have an underlying community responsibility, as distinct from obligations solely in regard to the cultural objectives of the Association.
 - (iii) No monies/assets in this fund will be distributed to members or office bearers of the Association, except as reimbursement of out-of-pocket expenses incurred on behalf of the fund or proper remuneration for administrative services.
 - (iv) The Australian Taxation Office will be notified of any proposed amendments or alterations to provisions for the public fund, to assess the effect of any amendments on the public fund's continuing Deductible Gift Recipient status.
 - (v) Receipts for gifts to the public fund must state:
 - the name of the public fund and that the receipt is for a gift made to the public fund;
 - the Australian Business Number of the company;
 - the fact that the receipt is for a gift; and
 - any other matter required to be included on the receipt pursuant to the requirements of the Income Tax Assessment Act 1997.
 - (vi) Winding-up clause

If upon the winding-up or dissolution of the public fund gazette by the Australian Taxation Office, there remains after satisfaction of all its debts and liabilities, any property or funds,

the property or funds shall not be paid to or distributed among its members, but shall be given or transferred to some other fund, authority or institution having objects similar to the objects of this public fund, and whose rules shall prohibit the distribution of its or their income among its or their members, such fund, authority or institution to be eligible for tax deductibility of donations under Subdivision 30-B, section 30-100, of the Income Tax Assessment Act 1997 and gazette by the Australian Taxation Office.

63A - DISCLOSURE AND ACCOUNTABILITY

63A(i) - Board Membership and Related Party Payments

Federal

Each officer of the Association shall disclose to the Federal President or in the case of the Federal President, the Board, any remuneration paid to the officer:

- (a) because the officer is a member of a board, if: the officer is a member of the board only because the officer is an officer of the Association; or the officer was nominated for the position as a member of the board by the Association or a peak council; or
- (b) by any related party of the organisation in connection with the performance of the officer's duties as an officer.

Disclosures under this Rule shall be made in writing to the Association and tabled at the relevant Board meetings as soon as practicable after the remuneration is paid to the officer.

Branches

Each officer of a Branch of the Association shall disclose to the Branch Secretary or Regional Director or in the case of the Branch Secretary or Regional Director, the Branch President, any remuneration paid to the officer:

- (c) because the officer is a member of a board, if: the officer is a member of the board only because the officer is an officer of the Branch; or the officer was nominated for the position as a member of the board by the Association, a Branch of the Association or a peak council; or
- (d) by any related party of the organisation in connection with the performance of the officer's duties as an officer.

Disclosures under this Rule shall be made in writing to the Branch and tabled at the relevant committee of management meetings as soon as practicable after the remuneration is paid to the officer.

63A(ii) - Remuneration

Federal/Branches

The Association shall disclose to members and its Branches: the identity of the five highest paid federal officers in terms of relevant remuneration for the disclosure period.

Wherever constituted, Branches shall disclose to members of the relevant Branch: the identity of the five highest paid officers of the branch in terms of relevant remuneration for the disclosure period.

63A - DISCLOSURE AND ACCOUNTABILITY

For Federal Association and Branch officers, the disclosure shall include: (i) the actual amount of the officers' relevant remuneration for the disclosure period; and (ii) the form of the officers' relevant non-cash benefits, for the disclosure period.

Disclosures under this Rule shall be made in writing in relation to each financial year; and within six months after the end of the financial year.

63A(iii) - Disclosure of Material Personal Interests

Federal

Each officer of the Association shall disclose to the Association any material personal interest that relates to the affairs of the Association in a matter that:

- (a) the officer has or acquires; or
- (b) a relative of the officer has or acquires.

Disclosures under this rule shall be made in writing to the Association as soon as practicable after the interest is acquired.

Disclosures under the Rule shall be made in writing to members of the Association in relation to each financial year; and within six months after the end of the financial year.

Branches

Each officer of a Branch of the Association shall disclose to the relevant Branch any material personal interest that relates to the affairs of the Branch in a matter that:

- (a) the officer has or acquires; or
- (b) a relative of the officer has or acquires.

Disclosures to the Branch under this Rule shall be made in writing to the Branch as soon as practicable after the interest in acquired.

Disclosures under this Rule shall be made in writing to members of the Branch in relation to each financial year; and within six months after the end of the financial year.

63A(iv) - Disclosure of Payments to Related Parties and Declared Persons

Federal

The Association shall disclose to members of the Association the total of the payments made by the Association, during the disclosure period:

- i. to each related party of the Association; or
- ii. to each declared person or body of the Association.

Disclosures to members and the Branches under this Rule shall be made in writing in relation to each financial year and within six months after the end of the financial year.

Disclosure is not required for a payment made by the Association to a related party if:

(a) the payment consists of amounts deducted by the Association from remuneration payable to officers or employees of the Association; or

64 - RESTRICTED APPLICATION OF SECTION 8

- (b) the related party is an officer of the Association, and the payment:
 - i. consists of remuneration paid to the officer by the Association; or
 - ii. is reimbursement for expenses reasonably incurred by the officer in performing the officer's duties as an officer.

Branches

A Branch of the Association shall disclose to members of the relevant Branch the total payments made by the Branch, during the disclosure period:

- i. to each related party of the Branch; or
- ii. to each declared person or body of the Branch

Disclosures to members of the Branch under this Rule shall be made in writing in relation to each financial year and within six months after the end of the financial year.

Disclosure is not required for a payment made by a Branch of the Association to a related party if:

- (a) the payment consists of amounts deducted by the Branch from remuneration payable to officers or employees of the Branch; or
- (b) the related party is an officer of the Branch, and the payment:
 - i. consists of remuneration paid to the officer by the Branch; or
 - ii. is reimbursement for expenses reasonably incurred by the officer in performing the officer's duties as an officer.

63A(v) - Expenditure Policies and Procedures

Federal/Branches

The Board shall develop and implement a single set of policies and procedures relating to expenditure. These policies shall apply to the Federal Association and Branches of the Association.

63A(vi) - Financial Management Training

Federal/Branches

Each officer of the Association or a Branch of the Association whose duties include duties that relate to the financial management of the Association or a Branch (as the case may be) must undertake training that is: approved by the General Manager of the Fair Work Commission; and that covers each of the officer's financial duties. Approved training shall be undertaken by all relevant officers within six months of assuming office.

SECTION 8 - JOURNALISTS' CODE OF ETHICS

64 - RESTRICTED APPLICATION OF SECTION 8

(a) This section of the rules shall apply only to members covered by Rule 4 Part C of these rules. For the purposes of this part such members shall be called 'journalists'.

Page 46 of 63 Pages

65 - AUSTRALIAN JOURNALISTS ASSOCIATION CODE OF ETHICS

(b) Any amendment or alteration to this part of the rules shall only be made by Federal Council if it has first been approved by the Media section of the Association in accordance with the procedure specified in Rule 75.

65 - AUSTRALIAN JOURNALISTS ASSOCIATION CODE OF ETHICS

Respect for truth and the public's right to information are fundamental principles of journalism. Journalists describe society to itself. They convey information, ideas and opinions. They search, disclose, record, question, entertain, comment and remember. They inform citizens and animate democracy. They give a practical form to freedom of expression. They scrutinise power, but also exercise it, and should be responsible and accountable.

Journalists commit themselves to:

Honesty, Fairness, Independence and Respect for the rights of others.

Journalists will educate themselves about ethics and apply the following standards:

- 1. Report and interpret honestly, striving for accuracy, fairness and disclosure of all essential facts. Do not suppress relevant available facts, or give distorting emphasis. Do your utmost to give a fair opportunity for reply.
- 2. Do not place unnecessary emphasis on personal characteristics including race, ethnicity, nationality, gender, age, sexual orientation, family relationships, religious belief or physical or intellectual disability.
- 3. Aim to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source. Where confidences are accepted, respect them in all circumstances.
- 4. Do not allow personal interest, or any belief, commitment, payment, gift or benefit to undermine your accuracy, fairness or independence.
- 5. Disclose conflicts of interest that affect, or could be seen to affect, the accuracy, fairness or independence of your journalism. Do not improperly use a journalistic position for personal gain.
- 6. Do not allow advertising or other commercial considerations to undermine accuracy, fairness or independence.
- 7. Do your utmost to ensure disclosure of any direct or indirect payment made for interviews, pictures, information or stories.
- 8. Use fair, responsible and honest means to obtain material. Identify your self and your employer before obtaining any interview for publication or broadcast. Never exploit a person's vulnerability or ignorance of media practice.
- 9. Present pictures and sound which are true and accurate. Any manipulation likely to mislead should be disclosed.
- 10. Do not plagiarise.
- 11. Respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude.
- 12. Do your utmost to achieve fair correction of errors.

Guidance Clause

Basic values often need interpretation, and sometimes come into conflict. Ethical journalism requires conscientious decision-making in context. Only substantial advancement of the public interest or risk of substantial harm to people allows any standard to be overridden.

66 - OFFENCES AND COMPLAINTS AGAINST THE CODE OF ETHICS

- (a) A journalist shall be deemed to have committed an offence against the Code of Ethics if, after procedures as laid down by these rules, he or she has been found guilty of any of the following:
 - (i) Violation of and/or refusal to observe the Code of Ethics of the Association;
 - (ii) Failure to obey a summons to attend a meeting of an Ethics Committee and failing to supply the Ethics Committee with a reasonable explanation for non-attendance.
- (b) A journalist found guilty of an offence against the Code of Ethics shall be liable to any of the following penalties: warning, reprimand, fine (to a maximum of \$1000), suspension from membership (for up to one year) and expulsion from membership.

67 - ETHICS PANEL

- (a) At its first meeting following the declaration of the biennial elections of the Alliance, the National Media Section Committee shall:
- (i) Appoint nine financial members who are members pursuant to Rule 4 Part C as members of the Ethics Panel.
 - (ii) appoint from the general community an additional four persons to the Ethics Panel; and
 - (iii) appoint from among the persons appointed under subsections (i) and (ii) of this rule a chair and at least one deputy chair.
- (b) The appointments shall be made in a manner determined by the National Media Section Committee.
- (c) Persons appointed shall hold office until the conclusion of the next Section Committee meeting held under Rule 67(a).
- (d) If any person appointed to the Ethics Panel dies, resigns or is removed from office, the Section Committee shall take such steps it considers necessary to fill the vacancy.
- (e) The Ethics Panel shall be empowered to investigate any complaint of violation of and/or refusal to observe the Code of Ethics and to make decisions thereon.
- (f) The Ethics Panel shall keep a written record of all complaints received, a summary of the evidence and also a record of all decisions and recommendations.
- (g) The decisions and recommendations of the Ethics Panel shall be published in accordance with any guidelines which may be issued by the National Media Section Committee.

Page 48 of 63 Pages

68 - COMPLAINTS

- (a) Any person may write to the Ethics Panel alleging that a member of the Alliance employed or engaged in journalism has acted contrary to Rule 65. The complaint shall be submitted in writing to the President of the Association's Media Section setting out the allegations fully and clearly.
- (b) The Ethics Panel shall not receive any anonymous or oral complaint. It shall have the right to refuse to receive, investigate or make a decision upon any complaint which in the opinion of the majority of the Panel members considering a complaint does not come within the provisions of the Code of Ethics or is vexatious, frivolous or trivial. The Panel shall publish reasons for such a refusal.
- (c) The Ethics Panel shall inter alia investigate any report on any matter concerning the Code of Ethics which may be referred to it by the Federal Council, the Board, National or Branch Section Committee or a Branch Council.
- (d) The President of the Association's Media Section shall refer any written complaint to the Chair of the Ethics Panel as soon as possible.
- (e) The Panel Chair shall within eight days:
 - (i) convene a Complaints Panel consisting of three members of the Ethics Panel. At least one of these three shall not be a member of the Alliance;
 - (ii) advise the complainant that the complaint has been received; and
 - (iii) advise the member complained against of the nature of the complaint
- (f) The Complaints Panel shall consider the complaint and may:
 - (i) dismiss the complaint without further action
 - (ii) attempt to mediate between the complainant and the member complained against.
 - (iii) seek further information from either the complainant and/or the person complained against or from any other person. The Panel may seek this in writing or by statutory declaration.
 - (iv) have the parties appear personally before the Panel
 - (v) allow the parties to call witnesses. If witnesses are called, either party may examine or cross-examine the witnesses. They shall also have the right to furnish written statements and the right to a reasonable adjournment of proceedings for these purposes.
- (g) If one of the parties appears personally before the Panel, the other party shall also have the right to appear.
- (h) The formalities associated with legal proceedings shall be followed where necessary to protect the member against whom the complaint has been made, but the Complaints Panel shall not be bound by the formal rules of evidence. The object of any hearing shall be to ascertain the truth and substance of the matter and to this end the rules of natural justice shall be observed that is to say that the complainant and the respondent have a right to put their case to the Panel. The extent of that right is to be determined by the Panel after considering the seriousness of the allegation

- (i) Neither party shall have the right to legal representation at any stage of the process outlined in these Rules.
- (j) Upon completing its investigations, the Complaints Panel shall be majority vote decide whether the complaint should be upheld or dismissed. If it decides that the complaint is upheld, it shall also, by majority vote, decide the penalty to be imposed in accordance with Rule 66.
- (k) The chair of the Ethics Panel shall advise the complainant and the member complained against of the decision of the Complaints Panel within 28 days of the decision. Each party shall be advised of the right to appeal.
- (l) If no appeal is lodged within a further 28 days, the decision shall be confirmed and action required shall be taken.

69 - APPEALS PANEL

- (a) Any party to a matter considered by a Complaints Panel shall have the right to appeal against any decision of the Panel with the exception of a decision to dismiss the complaint
- (b) The Appeal Panel is restricted to correcting error in the decision of the complaints panel.
- (c) The parties to the appeal are entitled to provide further evidence to the appeal panel.
- (d) An appeal must be lodged with the President of the Association's Media Section in writing within 28 days of being notified of the decision being appealed against.
- (e) The President of the Association's Media Section shall refer any written appeal to the Chair of the Ethics Panel as soon as possible.
- (f) The Panel Chair shall within eight days:
 - (i) convene an Appeal Panel consisting of five members of the Ethics Panel. At least two of these five shall not be a member of the Alliance. No member of the original Complaints Panel shall sit on the Appeals Panel;
 - (ii) advise the appellant that the appeal has been received;
 - (iii) advise the other party of the nature of the appeal; and
 - (iv) provide the Appeals Panel with all material connected with the decision appealed against
- (g) The Appeals Panel shall consider the complaint and may:
 - (i) dismiss the appeal
 - (ii) uphold the appeal
 - (iii) vary the original decision of the Complaints Panel
 - (iv) direct that a new Complaints Panel be convened to reconsider the complaint
 - (v) seek further information from either party. The Panel may seek this in writing or by statutory declaration
 - (vi) have the parties appear personally before the Panel

71 - OFFENCES AND COMPLAINTS

- (vii) allow the parties to call witnesses. If witnesses are called, either party may examine or cross-examine the witnesses. They shall also have the right to furnish written statements and the right to a reasonable adjournment of proceedings for these purposes.
- (h) The processes set out for the Complaints Panel shall apply mutatis mutandis to the Appeals Panel.
- (i) The Chair of the Ethics Panel shall advise the parties of the decision of the Appeals Panel within 28 days of the decision.

70A - NATIONAL STUNT COMMITTEE

- (a) Members who are graded stunt performers, safety supervisors and stunt co-ordinators shall elect a National Stunt Committee of twelve financial members constituted as follows:
 - (i) four members who are graded as safety supervisors from a minimum of three states;
 - (ii) four members who are graded as stunt co-ordinators from a minimum of three states; and
 - (iii) four members who are graded as stunt performers from a minimum of three states.
- (b) Members of the National Stunt Committee shall be elected biennially in accordance with Rule 79, provided that a member may only nominate for election in a single category, notwithstanding that they may be qualified for more than one category.
- (c) Within three months of the Meeting at which the members of a National Stunt Committee are declared elected, the Federal President of the Association's Equity Section shall convene the first meeting of the Committee at which a Chair, a Vice Chair and a Secretary of the Committee shall be appointed by and from the members of the Committee.
- (d) Any member of a National Stunt Committee shall not be absent without reasonable grounds for two consecutive meetings.
- (e) If seven of its members are in attendance to form a quorum a meeting of the National Stunt Committee shall be sufficiently constituted to transact business.
- (f) The National Stunt Committee shall devise and administer the National Stunt Grading Procedure and consider matters affecting safety and related issues in the Film and Television industries.
- (g) Should a member of the National Stunt Committee be an applicant for grading he or she shall disqualify him or herself from all deliberations by the Committee on that complaint, and if the member previously had been chosen as Chair, Vice-Chair or Secretary of the Stunt Committee the remaining members of the Committee shall choose another member from among their number to fill that office for the duration of the hearing.

SECTION 9 - OFFENCES AND BREACHES OF THE RULES

71 - OFFENCES AND COMPLAINTS

- (a) A member shall be held to have committed an offence if, after procedures as laid down in these Rules, he or she shall have been found guilty of any of the following:-
 - (i) Violation of and/or refusal to observe a lawful decision of the Association or abide by these Rules.

73 - CHARGES AGAINST MEMBERS

- (ii) Violation of and/or refusal to observe a lawful decision of Federal Council, the Board, National Section Committee, or a Branch Council or Branch Section Committee, attention to which has been drawn in any journal of the Association or in a letter, memorandum or bulletin issued by Federal Council, the Board, National Section Committee, or a Branch Council or Branch Sectional Committee.
- (iii) Violation of and/or refusal to carry out a provision of an Industrial Award determination or agreement applicable to him or her,
- (iv) Disclosing to a person not entitled to know it, any confidential matter of the Association,
- (v) Misappropriating money and/or property belonging to the Association,
- (vi) Knowingly works with a non-unionist without first notifying the workplace representative or in the absence of such a representative, the Secretary or Regional Director of the branch to which he or she belongs,
- (vii) Obstructs or having been requested to assist, fails to assist any officer or duly appointed representative of the Association in the performance of his or her duty,
- (viii) Fails to attend any meetings of the Executive or of a branch to which he or she belongs when requested to do so,
- (ix) Fails to observe By-Laws which may be enforced by the Association from time to time.
- (b) A member, found guilty of an offence, shall be liable to any of the following penalties namely, warning, rebuke, censure, fine (to a maximum of one thousand dollars), suspension for a period of up to one year or expulsion from membership of the Association.

72 - REMOVAL FROM OFFICE

A person elected to an office in the Association (whether the office be a Federal, Branch, sub-Branch or Sectional office) may be removed from office where the person has been dealt with in the manner set out in this section and found guilty of misappropriation of any of the funds of the Association, a substantial breach of the rules of the Association or gross misbehaviour or gross neglect of duty or has ceased under the rules to be eligible to hold the office.

73 - CHARGES AGAINST MEMBERS

- (a) Any persons or members complaining of violation and/or refusal to observe these Rules by any member or any member alleging that a member has committed an offence under these Rules, shall submit the complaint in writing to the Chief Executive within seven days of the matter complained of coming to the notice of the member making the complaint, setting out the allegations fully and clearly.
- (b) The Chief Executive shall bring the complaint before the next meeting of the Board which shall fix a date and time for investigation by the Board if it resolves that such complaint is of substance.
- (c) The Chief Executive shall, within three days of such Board meeting, forward by registered or certified mail or personal service to the member concerned, a copy of all allegations made against her/him and any evidence received in support of them, the charges under the rules and particulars of those charges. It shall also inform her/him of the date, time and place fixed for investigation by the Board of the complaint and of her/his right to appear personally or submit a reply in writing.
- (d) The respondent member shall have the right to appear personally at the investigation or to submit to the Board in writing, his or her reply to the complaint. If the respondent appears personally at the

Page 52 of 63 Pages

75 - NEW RULES AND ALTERATIONS OF RULES

- investigation, the complainant shall also have the right to appear. Each party shall be permitted to call witnesses. No party shall be entitled to be legally represented.
- (e) A copy of any evidence by Statutory Declaration by one party shall be sent to the other party who shall have the right to submit evidence in reply.
- (f) If either party is not present at the investigation or fails to submit evidence, the Board may nevertheless proceed to consider and decide upon the complaint or if it decides that there is insufficient evidence it may, before reaching a decision, call for further evidence from either party or other persons, to be submitted orally or in writing.
- (g) The formalities associated with legal procedure shall be followed where it is necessary to protect the member against whom the allegations are made. The formal rules of evidence shall not be applied. The object of the investigation shall be to ascertain the truth and substance of the matter and to that end, the rules of natural justice shall be observed.
- (h) The Chief Executive shall ensure the Association maintains a written record of all complaints received and investigated, a precis of the evidence produced or heard and also a record of all decisions of the Board.
- (i) All communications to members shall be authorised by the Chief Executive upon the directions of the Board and shall be by registered or certified mail or personal service.
- (j) Any member so charged, shall receive a copy of the determination of the Board in the matter within seven days of each determination.
- (k) Notwithstanding the foregoing, the Board shall have the authority to instruct the Chief Executive to initiate proceedings against any member.
- (l) Any member, found guilty of an offence under this Rule, shall have the right of appeal to the Federal Council.
- (m) Notice of such appeal must be lodged with the Chief Executive stating the grounds upon which the appeal is based within thirty days of the decision appealed against. Otherwise, the right of appeal shall lapse and the decision shall continue in force.

74 - DELETED

SECTION 10 - RULES

75 - NEW RULES AND ALTERATIONS OF RULES

- (a) Subject to sub-rule (d) hereof, no new rules shall be made nor shall any of the rules of the Association for the time being be altered, added to, amended or rescinded except by the Federal Council.
- (b) Any proposal to alter, amend, add to or rescind the Rules shall be submitted to the Federal President to enable it to be circulated to all Federal Councillors and Branches by the Chief Executive at least 28 days before the date on which the meeting or the postal ballot of Federal Council to consider the proposal is scheduled to begin.
 - Provided that a proposal to alter, amend, add to or rescind the Rules may be considered and determined by Federal Council without such notice where two-thirds of Federal Councillors agree.
- (c) Any proposal to alter, amend, add to or rescind the rules may be proposed by any Branch Council or Section Committee to Federal Council at any time between meetings of the Federal Council. Such proposed rules and/or amendments shall be submitted to the Federal President and shall be circulated in accordance with (b) hereof.

Page 53 of 63 Pages

(d) No new rule (or amendment, addition or rescission) shall be made which alters any section rights set out in sections 4 & 8 of these rules without the section first approving any such change in accordance with the rules governing those sections.

76 - INTERPRETATION OF RULES

Where a dispute arises about the meaning of any rule, subject to any authoritative interpretation of the rules by a competent court or industrial tribunal, the Federal Council shall be the body to determine the true meaning of that rule.

SECTION 11 - AFFILIATION & REPRESENTATION

77 - AFFILIATION AND REPRESENTATION

- (a) Federal Council, a National or Branch Section Committee, Branch or sub- Branch shall be authorised to affiliate with any industrial organisation or peak body of bona fide trade unions or such other body as is in accordance with the objects of the Association.
- (b) The Board, or any Branch, Division or Section shall not be affiliated with or represented by any organisation cause or movement or at any meeting which is party-political or sectarian in relation to the Media section.
- (c) Federal Council, a National or Branch Section Committee, or Branch shall not affiliate with any industrial organisation or peak body of bona fide trade unions in relation to Journalist members of the Association except where:
 - (i) At the date of amalgamation the Australian Journalists Association was affiliated with the relevant peak body;
 - (ii) the national or branch Media Section Committee (as the case may be) approves the affiliation.
- (d) A Branch, Division or Section shall not affiliate with or be represented by or on any other organisation, cause or movement unless Federal Council or the Board has granted approval.

SECTION 12 - ELECTIONS

78 - TERMS OF OFFICE

(a) The terms of office for each office shall be as follows:

(i)	Honorary Federal Officers	2 Years
(ii)	Other Federal Councillors	2 Years
(iii)	Honorary Branch Officers	2 Years
(iv)	Other Branch Councillors	2 Years
(v)	Section Representatives	2 Years
(vi)	Ethics Panel member	4 Years
(vii)	National Stunt Committee*	2 Years

^{*} Equity section members graded as stunt performers, stunt co-ordinators and safety supervisors;

- (b) Notwithstanding (a), an incumbent officer shall hold office for the term specified in (a) or until a declaration of the ballot for that office occurs, whichever is the later.
- (c) No employee of the Association may hold any honorary office in the Association.

Page 55 of 63 Pages

79 - ELECTIONS

- (a) Not later than June 30 in each even-numbered year, the Board shall:
 - (i) Fix dates for nomination and election of Federal and Branch officers as required by these Rules.
 - (ii) Appoint a Federal Returning Officer for the conduct of the elections. The Returning Officer shall not be a holder of any office in, nor be an employee of, the Association or a Branch, Section or Division.
 - (iii) Determine a date for close of voting
- (b) The Federal Returning Officer shall appoint a Branch Returning Officer to conduct elections for each Branch. The Branch Returning Officer will not be a holder of any office in, nor be an employee of the Association or a Branch, Section or Division.

Notice of Elections

- (c) The Returning Officer shall:
 - (1) In each even-numbered year for honorary positions (or when appropriate in the case of a casual vacancy), circulate a notice to all members or take such other measures as are necessary calling for nominations of financial members entitled to nominate in accordance with these rules as candidates for election as:
 - (i) Federal President
 - (ii) Federal President (Media) (to be elected by members of the Media Section)
 - (iii) Federal President (Actors Equity) (to be elected by members of the Equity Section)
 - (iv) Federal President ECS (to be elected by members of the ECS section)
 - (v) Federal President (Musicians) (to be elected by members of the Musicians Section)
 - (vi) Federal Vice-Presidents (5) (the number for each section or group of sections to be determined by Rule 80)
 - (vii) Branch Officers
 - (viii) One Board member elected by and from the financial membership of each Branch with more than 900 financial members as at June 30 immediately prior to the biennial elections and One Board member elected by and from the financial membership of all other Branches
 - (ix) Branch Secretaries (where determined by Federal Council)
 - (x) State delegates to Federal Council/ Board as determined by Rule 40 from those States where Federal Council has not determined to form a Branch.
 - (xi) Delegates from the Sections of the Association to Federal Council (the number to be determined by Rule 80)
 - (xii) Delegates from the Sections of the Association to Branch Council (the number to be determined by Rule 80)
 - (xiii) National Stunt Committee 12 (Equity Section Stunt performer 4, Stunt co-ordinator 4, Safety Supervisor members 4)
 - (2) The notice shall stipulate that a member cannot stand for more than one of each of the positions specified in sub-rule (c), excepting that a member nominating for a Branch Council position other than Branch President or Branch Secretary or in the NSW and Victoria Branch Vice-President, may also nominate for the position of Section Delegate to Federal Council.

	(3)	The notice shall further stipulate that where there are three or more positions to be filled in any election (other than those applying to the Professional Sports Section or Professional Sports Branch) one of each three of the positions shall be filled by a woman according to the following formula:
		 3 - 5 positions: at least one woman 6 - 8 positions: at least two women 9 - 11 positions: at least three women 12 - 14 positions: at least four women 15 - 17 positions: at least five women
	(4)	The notice shall further stipulate that where a section is entitled to two or more delegates to Federal Council, they shall be elected according to the following formula:
		2 delegates from at least 2 states 7 delegates from at least 3 states 12 delegates from at least 4 states
	(5)	The notice shall further stipulate that where at least two vice-presidents are to be elected under $(c)(1)(vi)$ from any section or sections, at least one of those two shall be a woman, unless the President from the relevant section is a woman.
	(6)	If insufficient eligible candidates nominate to meet the provisions of parts (3) and (4) of this sub-rule, then the provisions shall not apply.
	(7)	The notice shall specify the time and date for the opening and closing of nominations and the name and address of the Branch Returning Officer appointed to receive the nominations. The notice shall be circulated at least 14 days prior to the time and date for the closing of nominations.
		Nominations
(d)		nations must be in writing and contain the given names and/or other identifying names and of employment and address of each candidate. Nominations:
	(i)	must be signed by at least one other financial member of the Branch and contain the addresses of the signatories;
	(ii)	must be accompanied by the written consent of the member nominated;
	(iii)	may be accompanied by a statement to a maximum of 150 words; and
	(iv)	Nominations must be submitted in the following form:
		Date
		I hereby nominate (block letters) a financial member of the Branch as a candidate for election as (state the position to which election is desired)
		Signature
		Name (Block Letters)
		Address

I hereby consent to the above nomination.
Signature
Address
Place of Employment

(e) The Branch Council in a Branch with less than 500 financial members shall have discretion to decide whether sub-clause (2) of Clause (c) of this rule shall apply or whether a member may stand for not more than two of the following positions: Branch President, Branch Vice-President, Branch Treasurer, Branch Secretary or the Branch Council. The Branch Committee shall decide the sequence of election.

Close of Nominations & Defective Nominations

(f) The Returning Officer shall close receipt of nominations at the time fixed. If the Returning Officer conducting such an election finds a nomination to be defective he or she shall, before rejecting the nomination, notify the person concerned of the defect, and, where it is practicable to do so, give him or her the opportunity of remedying the defect where practicable, within seven days after his or her being so notified. The Returning Officer shall submit a report in writing on all nominations received by him or her to the next meeting of the Branch Council in the case of all nominations for positions in that Branch and the Board in the case of all nominations for Federal Officers.

Contested Election

- (g) Should the number of valid nominations received exceed in any case the number required to fill the office or position concerned such nominations shall be submitted to a secret postal ballot of all financial members of the Branch or of the Association in the case of Federal Officers for election.
- (h) The Returning Officer shall:
 - (i) close the roll of voters 7 days before the opening of nominations and give instructions for the preparation of a list of names and last known addresses of financial members entitled to vote.
 - (ii) arrange for the printing of declaration envelopes, prepaid reply envelopes and ballot papers to be distributed by post to each eligible voter; the declaration and prepaid envelopes must comply with the forms prescribed by the relevant legislative requirements.
 - (iii) upon receiving advice in writing from any eligible member that the member shall be absent from his or her usual address during the period of the ballot, forward a ballot paper, a declaration envelope, prepaid reply envelope and candidates' statements (if provided) to such address as advised by the eligible member.
- (i) The Returning Officer shall draw lots to determine the order in which the names of candidates shall appear on the ballot paper.
- (j) The given names and/or other identifying names and the place of employment of each candidate for election shall be included on the ballot paper for the guidance of members in voting. This information shall be supplied by a candidate with his or her nomination. Each candidate may also prepare and include with his or her nomination a statement containing his or her Association and employment/professional history and place of employment to a maximum of 150 words. The Returning Officer shall issue a copy of each statement (including where applicable, the candidates photograph) with each ballot paper.

Page 58 of 63 Pages

System of Voting

- (k) The system of voting to apply to elections in the Alliance shall be the optional preferential system. Each voter is required to vote for at least the number of vacancies to be filled in each position.
- (l) After completing the ballot paper, the voter shall place the paper in the declaration envelope, complete the declaration on the envelope and insert the declaration envelope in the prepaid reply envelope.
- (m) At the close of the ballot, the returning officer shall check the declarations against the roll of voters. The following procedure shall then be followed for the counting of the ballots:-

Election of One Candidate Only

- (1) Where one candidate only is to be elected, the Returning Officer shall observe the following procedure to determine the successful candidate:
 - (i) A candidate who receives more than half the number of first preference votes cast shall be the successful candidate.
 - (ii) Should no candidate be successful on the first round, the candidate who receives the least number of first preference votes shall be excluded from the count and his or her second preference votes shall thereupon be distributed among the remaining candidates. A candidate then receiving more than half the total number of votes cast shall be thereupon be the successful candidate.
 - (iii) The above procedure shall be continued until one candidate has received the requisite number of votes to become the successful candidate.
 - (iv) If on any count two or more candidates each receive the same number of votes the candidate who received the greater number of first preference votes shall remain in the count. If two or more candidates receive an equal number of first preference votes the Returning Officer shall decide by lot which candidate shall remain in the count.

Election of More Than One Candidate

Where two or more candidates are to be elected the Returning Officer shall observe the following procedure to determine the successful candidate:

The votes shall be classified into two categories as follows:

- (i) The preference votes for the number of vacancies to be filled shall be termed "primary" votes, and shall have equal value in the first count and be credited to the
 - candidate for whom they are cast, whether marked 1, 2, 3, etc. according to the number of vacancies. The preference votes beyond those referred to in (1) shall be termed "secondary" votes, and shall have rank according to their numerical number and shall be allocated in rank order unless the ranking secondary vote has been previously allocated.
- (ii) The "primary" votes shall first be counted and a list shall be prepared of the candidates in order according to the primary votes cast for them. The candidate who is lowest on the list thus compiled shall be excluded from the count.
- (iii) Each ballot paper on which such excluded candidate received a "primary" vote shall then be examined to determine its "secondary" vote and the preference so found shall be allotted to the appropriate remaining candidate on the first count.

- (iv) On the conclusion of the second count, the above procedure of exclusion of candidates from the count and the distribution of their secondary votes shall continue until the required number of successful candidates has been determined.
- (v) If, in any count, the next available preference vote of an excluded candidate is cast in favour of an excluded candidate, such preference vote shall be disregarded and the next available preference vote cast in favour of a remaining candidate shall be added to the votes credited to that candidate.
- (vi) If, in any count, two or more candidates each receive the same number of votes and one of them has to be excluded, the Returning Officer shall decide by lot which candidate shall remain in the count.
- (vii) If at the conclusion of all necessary counts, the provisions of Rule 79(c)(3) and (4) have not been applied, the Returning Officer shall apply the provisions of the Rule. Where there is a conflict between the provisions of these sub-rules, then the provisions of Rule 79(c)(3) shall prevail.
- (3) (i) Where one candidate only is to be elected (that is, for the offices listed in (c)(1)(i) to (v)), the Returning Officer shall observe the procedure set out in sub-paragraph (1) of this rule.
 - (ii) Where two or more candidates are to be elected (that is, for the offices listed in (c)(1)(vi)), the Returning Officer shall observe the procedure set out in sub-paragraph (2) of this rule, provided that, if, at the conclusion of all necessary counts for the offices listed in (c)(1)(i) to (v), the provisions of Rule 79(c)(5) have not been applied, the Returning Officer shall apply the provisions of the Rule to the extent necessary in the count for positions listed in (c)(1)(vi). Where there is a conflict between the provisions of sub-rule (c)(5), then the provisions relating to minimum numbers of women shall prevail.

Appointment & Conduct of Scrutineers

- (n) Any candidate shall be entitled to appoint a scrutineer to inspect any aspect of the conduct of the election by the Returning Officer.
- (o) A scrutineer shall not interfere with the conduct of the ballot or the counting of votes. If he or she considers that any vote is invalid or that there is any irregularity in the counting, he or she may bring the matter under the notice of the Returning Officer who shall record in his or her report to the Federal President or the Branch Secretary/Regional Director as the case may be any objection raised by a scrutineer.

Returning Officer's Report & Declaration of Ballot

- (p) The Federal Returning Officer shall report the result of the ballot for Federal Officers to the Board.
- (q) After the Board has received the report of the Federal Returning Officer on the election of Federal Officers, the Federal President shall declare the result of the elections. If a vacancy then exists the Board shall take whatever action it considers necessary or desirable to fill the vacancy.
- (r) A member who has been declared elected or re-elected as a Federal Officer shall assume the title and carry out the duties of his or her office immediately upon the cessation of the term of office of his or her predecessor or, in the case of a casual vacancy, after the close of the meeting of the Board at which the result of the election is declared.
- (s) Each Branch Returning Officer shall declare the ballot and shall report the results of the ballot for positions in that Branch to the Branch Council.
- (t) The Branch Council on receiving the report of the Returning Officer on the result of the ballot shall submit it to the Annual General Meeting.

80 - FORMULA FOR ELECTION OF FEDERAL, BRANCH AND SECTION DELEGATES AND VOTING AT FEDERAL COUNCIL

- (u) If there are not sufficient nominations to fill the offices and positions listed in sub-clause (c) of this Rule or it is demonstrated that a successful candidate has become unable or ineligible to assume the office or position to which he or she has been elected, the Branch Council shall take action to fill the vacancy for the balance of the term, in accordance with sub-rule (u).
- (v) Any candidate defeated on a ballot may demand a recount of votes by lodging with the Returning Officer an application in writing within three days of the declaration of the ballot by the Branch Returning Officer or the Board as the case may be.

Casual Vacancies

- (w) Should any person elected to any office in the Association die, resign or be removed from office during the term for which they have been elected, the vacancy so created will be filled:
 - (i) in a manner determined by the Branch Council or the Board as the case may be, provided that where the unexpired part of the term of office so vacant exceeds 12 months or three quarters of the term of office, whichever is the greater, an election shall be conducted in accordance with this rule.
 - (ii) any person so elected or appointed to a casual vacancy shall hold the office until the expiration of the balance of the term left vacant.

80 - FORMULA FOR ELECTION OF FEDERAL, BRANCH AND SECTION DELEGATES AND VOTING AT FEDERAL COUNCIL

- (a) The Board shall determine the number of Federal Council delegates to which each national section is entitled by applying the following formula:
 - (i) The annual income of each national section from entrance fees and membership subscriptions shall be ascertained for the previous financial year.
 - (ii) The 'notional' number of members of each national section shall be ascertained by dividing the amount of income for each section by \$200.00 (or another amount as determined by the Board).
 - (iii) The respective proportions of the notional members of each national section shall be ascertained.
 - (iv) The proportional formula so obtained in respect of national sections shall be applied to the number fifty.
 - (v) The result rounded to the nearest whole number which is one or greater shall be the number of delegates to Federal Council from the respective sections.
- (b) The Board shall determine the number of Branch Council delegates to which each section is entitled by applying the following formula:
 - (i) The annual income of each section within the Branch from entrance fees and membership subscriptions shall be ascertained for the previous financial year shall be ascertained
 - (ii) The 'notional' number of members of each section shall be ascertained by dividing the amount of income for each section by \$200.00 (or another amount as determined by the Board).

83 - MEMBERS RIGHT TO VOTE IN BALLOT

- (iii) The respective proportions of the notional members of each section shall be ascertained.
- (iv) The proportional formula so obtained shall be applied to the number twenty-five (or such lesser number as determined by Federal Council or the Board).
- (v) The result rounded to the nearest whole number which is one or greater shall be the number of delegates to Branch Council from the respective sections.
- (vi) In accordance with clause (iv) of this sub-rule, Federal Council may determine that the lesser number be zero in which case there will be no section delegates to the Branch Council.
- (c) The Board shall determine the number of Federal Vice-Presidents to which each section or grouping or sections is entitled by applying the following formula:
 - (i) The annual income of each of the Media, Equity, ECS and Musicians Sections from entrance fees and membership subscriptions shall be ascertained for the previous financial year.
 - (ii) The 'notional' number of members of each section or grouping of sections shall be ascertained by dividing the amount of income for each section by \$200.00 (or other amount as determined by the Board).
 - (iii) The respective proportions of the notional members of each section or grouping of sections shall be ascertained.
 - (iv) The proportional formula so obtained in respect of section or grouping of sections shall be applied to the number five.
 - (v) The result rounded to the nearest whole number which one or greater shall be the number of federal vice-presidents from the respective sections or groupings of sections.

81 - AVOIDANCE OF IRREGULARITIES

Notwithstanding the provisions of this Rule a Returning Officer may take such action and give such directions as he or she considers necessary in order to ensure the secrecy of the ballot and that no irregularities occur in or in connection with the election or to remedy any inconsistency or inadequacy that may arise in the application of this Rule.

82 - OFFICERS ILLEGALLY ELECTED

Should any office of any Branch Council or the Board or Federal Council or Sectional Committee be illegally elected, any business transacted by such Officer or body of which such illegally-elected person is a member, shall nevertheless be held to be properly transacted and the legality of his or her act shall not be capable of being challenged or called into question unless it was done in bad faith.

83 - MEMBERS RIGHT TO VOTE IN BALLOT

Financial members entitled to vote in elections for federal officials of the Association shall have the right to vote in all ballots conducted under law for the amalgamation of the Association with any other association or organisation.

Page 62 of 63 Pages

84 - TRANSITIONAL RULES

- (a) The Association has determined that no officers shall be employees of the Association pursuant to Rule 5(g) with effect from biennial elections of 2014-2015.
- (b) The appointed chief executive shall not be an officer of the Association under these rules or the Fair Work (Registered Organisations) Act 2009;
- (c) To the extent that any of the duties laid out in Rule 50 or in any other Rule may only be implemented by an Officer under these Rules or the Fair Work (Registered Organisations) Act 2009, the Federal President shall be the relevant Officer, subject to the delegation of these powers in accordance with these rules.

END OF RULES

[129VFED: Incorporates alterations of 05 March 2019 in matter R2018/271]		
I CERTIFY under section 161 of the Fair Work (Registered Organisations) Act 2009 that the pages herein numbered 1 to 65 both inclusive contain a true and correct copy of the registered rules of the Media, Entertainment		
and Arts Alliance.		
DELEGATE OF THE GENERAL MANAGER FAIR WORK COMMISSION		
MDODTANT. For existing the set the second consultant and set to the second consultant and second consultant an		
MPORTANT: Enquiries about these rules or other rules relating to this organisation which are current a force may be directed to any office of the Fair Work Commission.]		

Rules of the Media, Entertainment and Arts Alliance Contents

SECTION 1		1
1 - NAME		1
2. OBJECTS		1
3 - INDUSTRY		4
Part A:		
Part A:		6
Part B:		
Part C:		8
Part D·		C
	L MEMBERSHIP	
	MEMBERSHIP	
16 - RESIGNATION FROM MEMBER	SHIP	19
17 - REMOVAL FROM THE ROLL OI	F MEMBERS	20
SECTION 3 - BRANCHES		20
18 - BRANCHES		20
19 - BRANCH COUNCIL		20
20 - DELETED		21
22 - DELETED		22
23 - CONTROL OF BRANCH COUNC	TIL BY MEMBERS	22
24 - DELETED		23
25 - BRANCH OFFICERS		23
26 - BRANCH PRESIDENT		23
27 - BRANCH VICE-PRESIDENTS		23
28 - POWERS & DUTIES OF BRANCI	H SECRETARIES AND REGIONAL DIRECTORS	23
	FESSIONAL INTERESTS	
33 TROILEMON OF BLETTON TRO	LOSTOTIL ITTLICUTO	

34 - SECTIONS	
35 - SECTION COMMITTEES	
36 - DELETED	
37 - DELETED	
38 - DELETED	
39 - SECTION PLEBISCITES	
SECTION 5 - FEDERAL ORGANISATION	
40 - CONSTITUTION OF FEDERAL COUNCIL	
41 - POWERS AND DUTIES OF THE FEDERAL COUNCIL	
42 - ORDINARY MEETINGS OF FEDERAL COUNCIL	
43 - ORDER OF BUSINESS AT FEDERAL COUNCIL MEETINGS	
44 - EXTRAORDINARY MEETINGS OF FEDERAL COUNCIL	
45 - MEETINGS AND/OR DECISIONS OF FEDERAL COUNCIL MAY BE CONDUCT	
BY FACSIMILE, TELEPHONIC VOTES ETC	
46 - CONTROL OF FEDERAL COUNCIL BY MEMBERS	
47 - FEDERAL OFFICERS	
48 - FEDERAL PRESIDENT	
49 - FEDERAL SECTION PRESIDENTS AND FEDERAL VICE-PRESIDENTS	
50 - POWERS AND DUTIES OF CHIEF EXECUTIVE	
51 - DELETED	
52 - BOARD - POWERS AND DUTIES	
53 - MEETINGS OF THE BOARD	
54 - DELETED	
55 - NATIONAL GENERAL MEETINGS	
56 – NATIONAL GENERAL MEETING	
SECTION 6 - INDUSTRIAL MATTERS	
57 - INDUSTRIAL DISPUTES	
58 - PROSECUTIONS ON BEHALF OF THE ASSOCIATION	
59 - AGREEMENTS WITH STATE UNIONS	
SECTION 7 - ADMINISTRATION	
60 - SEAL AND EXECUTION OF DOCUMENTS	
61 - AUDITOR	
62 - FINANCIAL YEAR	
63 - FINANCIAL MANAGEMENT	
63A - DISCLOSURE AND ACCOUNTABILITY	
SECTION 8 - JOURNALISTS' CODE OF ETHICS	
64 - RESTRICTED APPLICATION OF SECTION 8	
65 - AUSTRALIAN JOURNALISTS ASSOCIATION CODE OF ETHICS	
66 - OFFENCES AND COMPLAINTS AGAINST THE CODE OF ETHICS	
67 - ETHICS COMMITTEE	
68 - COMPLAINTS	
69 - APPEALS PANEL	
70A - NATIONAL STUNT COMMITTEE	
SECTION 9 - OFFENCES AND BREACHES OF THE RULES	
71 - OFFENCES AND COMPLAINTS	
72 - REMOVAL FROM OFFICE	
73 - CHARGES AGAINST MEMBERS	
74 - DELETED	
SECTION 10 - RULES	
75 - NEW RULES AND ALTERATIONS OF RULES	
76 - INTERPRETATION OF RULES	
SECTION 11 - AFFILIATION & REPRESENTATION	57
77 - AFFILIATION AND REPRESENTATION	
SECTION 12 - ELECTIONS	57
78 - TERMS OF OFFICE	57
79 - ELECTIONS	58

Contents

Nominations	59
Contested Election	60
80 - FORMULA FOR ELECTION OF FEDERAL, BRANCH AND SECTION DELEGAT	ES AND
VOTING AT FEDERAL COUNCIL	63
81 - AVOIDANCE OF IRREGULARITIES	64
82 - OFFICERS ILLEGALLY ELECTED.	64
83 - MEMBERS RIGHT TO VOTE IN BALLOT	64
84 - TRANSITIONAL RULES	

SECTION 1

1 - NAME

The name of the Association shall be the Media, Entertainment and Arts Alliance.

2. OBJECTS

The objects of the Association shall be:-

Members

- (a) To regulate, improve and protect the wages and conditions of work welfare and rights of all members including by advancing and protecting the professional interests status and rights of members and the usages and customs of callings covered by the Association, and where considered necessary by the Federal Council of the Association, of persons entitled to become members, and to improve and foster the interests of members of the Association.
- (b) To secure the membership in the Association of all persons who are entitled to become members in accordance with these rules.
- (c) To secure preference in employment and in all aspects of that employment for members of this Association.
- (d) To provide effective representation (including legal representation) to member(s) or any section or group of members in connection with any matter where such representation is considered desirable by the Federal Council or a Branch Council.
- (e) To provide services generally to members (including legal assistance) to member(s) or any section or group of members or access to such services at special or discounted rates in connection with any matter where such services are considered desirable by the Federal Council or a Branch Council.
- (f) To attain sex and racial equality in all spheres of the Association's activity and to oppose all discrimination on the grounds of race, sex, colour, religion, political beliefs, sexual preference or disability.
- (g) To regulate and decide all questions of professional conduct, including, to prescribe and enforce a Code of Ethics to ensure and maintain ethical standards in all areas of journalism.

Education and Training

- (h) To take all steps considered necessary or desirable by the Federal Council or a Branch Council to further and promote the opportunities for training and education of members especially where such training and education has a direct vocational benefit including by the establishment and fostering of schemes of industry training, apprenticeship and the like.
- (h) To ensure that the Association's financial policies and practices accord with all relevant standards and laws and that key financial and operating decisions are disclosed to members in a timely and transparent manner.
- (i) To foster and promote trade union training among the membership.

[129VFED: Incorporates alterations of 05 March 2019 in matter R2018/271] Page 1 of 65 Page

Benevolent activities

- (j) To provide financial and other assistance at the discretion of the Federal Council of the Association to members in case of accident, death, sickness unemployment or other distress.
- (k) To establish a Benevolent Fund and/or Funds for the benefit of members or former members of the Association.
- (l) To establish funeral, sick, accident, unemployment or other insurance or assurance funds or benefits for the assistance of members of the Association.

Industry Matters

- (m) To ensure that not less than a minimum proportion of resident members as decided by the Federal Council are employed in any film, television or theatrical production.
- (n) To maximise the use of Australian creative resources in all aspects of the media, entertainment and amusement industries and ensure that not less than a minimum proportion of all radio and television programs broadcast in Australia are produced in Australia.
- (o) To promote and attain the use of standard contracts of engagement of the members throughout the industries with which the Association is associated.
- (p) To seek the regulation and control by appropriate legislation if necessary, of the operation of theatrical and other employment and engagement booking agencies and the business methods of theatrical and/or other employment agencies who arrange employment for the members of the Association.
- (q) To issue to members from time to time a list which contains the name of any employer, theatrical agent or employment agent or other person who in the opinion of the Federal Council of the Association has acted in an unfair manner in connection with the employment of any member or members.
- (r) To protect the welfare and rights, including the intellectual property rights, of members including by:
 - (i) seeking appropriate legislation and/or industrial regulation to protect the welfare and rights, including the intellectual property rights, and moral rights, of members and similar rights such as residual, secondary usage, or re-use fees and/or royalties
 - (ii) acting as agent and/or licensor for members in all respects in relation to the authorisation of uses of copyright material and the collection and distribution of copyright fees and similar fees; and
 - (iii) seeking appropriate legislation and/or industrial regulation to protect the welfare and rights of outdoor amusement and recreation workers.

Public Education and Publicity

(s) To promote the objects policies and activities of the Association by means of publications and the media generally.

Co-operation with other Bodies

(t) To co-operate with any other person, for the defence and improvement of theatrical, radio, film and television performances and productions generally, and for the promotion of the arts of the theatre, film, radio and television in all their spheres and to further the establishment and advancement of Australian art and culture within the theatre, live entertainment and in film, radio and television generally.

Page 2 of 65 Pages

- (u) To amalgamate with, absorb, affiliate to, or co-operate (including by providing financial assistance thereto) or otherwise combine with, any trade or industrial union or association or associations of trade unions including any international federation of trade unions whether in Australia or overseas or similar international bodies, or any other organisations having objects similar in whole or in part to the objects of the Association and to be represented on other bodies and organisations.
- (v) To provide financial or other assistance to and/or participate in the activities of any other union or unions whether in Australia or overseas, including any international federation of trade unions or similar international bodies, or any other organisations having objects similar in whole or in part to the objects of the Association.

Trade Union Rights

- (w) To assist members to obtain a fair remuneration for their labour and to assist other trade unions, whether in Australia or overseas to maintain, preserve and advance the interests of labour.
- (x) To uphold the right of all workers to combine for the preservation and advancement of their interests.
- (y) To promote industrial peace by amicable means and to foster and promote means of conciliation to settle industrial disputes.

Management & other Activities of the Association

- (z) To adopt & promote such other objects which are from time to time considered desirable by the Federal Council.
 - (aa) To provide the necessary and reasonable expenses of management of the Association.
 - (bb) To raise funds for the carrying out of the objects, policies and activities of the Association, including by the striking of levies upon members or sections or groups of members for the benefit of those members or sections or groups of members.
 - (cc) To take all steps necessary or desirable to organise and represent the members including by the establishment of sections, sub branches, delegates committees, and delegates, however described.
 - (dd) To hold, purchase, sell, lease, mortgage, borrow or otherwise deal in real property and to enter into agreements in connection with same and to do all such other things as may be deemed necessary in connection therewith.
 - (ee) To initiate and carry into effect in any way considered necessary or advisable by the Federal Council and/or the Board, authorised as herein provided, all or any of the provisions of any statute, state or federal, relating to industrial disputes and arbitration and for all or any such purposes to employ legal or other assistance.
 - (ff) To enforce the rules of the Association.

Cultural Activities

- (za) To promote culture through undertaking activities that advance the professional and industry development of cultural pursuits including literature, music, media, performing arts, visual arts, design, film, video, television, radio, community arts, Indigenous arts and movable cultural heritage.
- (zb) To promote cultural development through activities and industry seminars, forums, workshops, discussion papers and other activities.

Overseas Aid

- (zc) To undertake charitable overseas development and/or relief activities including:
 - (i) to provide support to journalists, media, entertainment and arts workers facing intimidation, discrimination or physical violence;
 - (ii) to provide financial relief to journalists, media, entertainment and arts workers and/or their families:
 - (iii) to provide legal assistance to journalists, media, entertainment and arts workers;
 - (iv) to support human rights advocacy and other collective action by journalists, media, entertainment and arts workers and their unions in support of press freedom and media and journalists rights;
 - (v) to provide support with particular priority to the Asia and Pacific region;
 - (vi) to take any steps thought appropriate to advance the interests of professional and ethical journalism;
 - (vii) to raise funds from members and the public through donations and fund raising activities.

3 - INDUSTRY

Part A:

The industry in connection with which the Association is registered shall be the industry of the employment of every person employed or likely to be employed in or in connection with any of the following industries or callings, namely:

Employees employed in or in connection with, including selling tickets by any means in connection therewith, or in or about, any kind of amusement, whether indoor or outdoor, including:-

- (a) cultural complexes, theatres, halls, racecourses, sports, exhibitions, agricultural shows, planetaria, animal parks, puppet shows and film exchanges, but excluding any person employed in or about the foregoing in any capacity in or in connection with the provision, sale, service or preparation of food or drink;
- (b) Clubs, licensed clubs and discotheques, but only insofar as such employees are employed as set and property carpenters and painters, stage crews, mechanists, projectionists, audio and lighting technicians, flymen, props persons, scenic artists, wardrobe including dressers, costume and property workers, stage managers, make-up artists, hairdressers, wigmakers and wig dressers, directors, choreographers and designers;
- (c) Casinos, but only insofar as such employees are employed as supervisors, pit bosses, inspectors, croupiers, dealers, bankers, cashiers and change clerks, but excluding such persons employed at the Wrest Point Casino, Tasmania;
- (d) In all aspects of Motion Picture Film, Video and Television Production and Processing, the Australian Film Commission and the Australian Film and Television School, including but without limiting the generality of the foregoing Producers, Directors, Production or Studio Unit Managers, Assistant Directors, Production Accountants, Dialogue and/or Commentary Writers, Script and/or Continuity Recordists, Location and/or Talent Scouts, Contact Men, Make-up Artists, Casting Directors, Art Directors, Chief Cameramen, Operative Cameramen, Special and/or Process Cameramen, Title and/or Cartoon Cameramen, Camera Dolly and/or Rotambulation Operators,

Slate Operators, Studio Gripmen, Studio Mechanists, Chief Sound Engineers, Sound Engineers, Sound Recordists, Microphone Boom Operators, Sound Mixers, Film Editors, Film Cutters, Specialist Film Cutters, Film Librarians, Film Vault Keepers, Film Splicers, Laboratory and/or Studio Maintenance Men, Film Stock Keepers, Film Laboratory Managers, Film Laboratory Chemists, Film Printing Operators, Film By- Product Recovery Chemists, Film Timers, Film Cleaners and/or Waxers, Film Checkers, Laboratory and/or Studio Projectionists, Film Processors, Film Graders, Film Despatchers, Film Packers and Film Examiners, Supervising and other classes of Technician involved in Maintenance, Installation, Videotape, Lighting, Telecine or Audio Departments, Cinecameramen, Videocameramen, Set Designers, Graphic Artists, Co-ordinators, Stills Photographers, Floor Managers, Film Sound Recordists, Wardrobe Supervisors and Assistants, Set and Property Carpenters and Painters, Property men/ women, Scenic Artists, Producers/ Directors Assistants, Vision Switchers, Set Dressers, Hairdressers, Film Department Assistants, Studio Hands, Film/Videotape and Record Librarians, Property and Scenery Storemen, and all trainees and inexperienced adults employed in or in connection with television or videotape production houses;

- (e) In film and television distribution, persons employed in film release and control, statistics and contracts, film despatch, (other than officers in charge), projectionists, assistant projectionists, film packers, film checkers, film examiners, film cleaners and film splicers; and
- (f) Cinemas;
- (h) All persons employed or to be employed at World Congress Centre Melbourne and/or the Melbourne Exhibition Centre, other than the employees of contractors providing cleaning, carparking, or food and drink services.

together with such other persons, whether so employed or not as have been elected Officers and Industrial Staff of the Association and have been admitted as members thereof.

and:-

Part B:-

In or in connection with journalism, public relations or authorship in or in connection with the printed media, radio, television, satellite, cable transmission or broadcast or electronic data bases and Hansard, law or other reporting.

and:-

Part C:-

In or in connection with the industry of commercial and industrial art which without limiting the generality of the foregoing includes any business, trade, manufacture, undertaking, calling, service, employment, handicraft or industrial occupation or avocation in the industry or in any branch of the industry including concept visualisation, art direction, art buying, layout, illustration, photography, decorative set and prop design, three dimension and surface packaging design, lettering, typographic design, photo-retouching, video, film graphics, cartooning, finished art and assembly of all design elements including type, provided that it has been set in a recognised trade house and production supervision, book brochure design, map drawing, display and exhibition design, and development of corporate image provided that persons shall not be eligible to join the Association who are employees in or in connection with the printing industry.

Part D:-

The industry of entertaining the public in any place which could reasonably be construed to be a place of entertainment; and of acting, rehearsing or otherwise appearing in cinematographic films and of entertaining and providing and or preparing commercial advertising and/or entertainment, and/or making announcements, and/or devising entertainment for transmission by short or long wave or frequency modulated broadcasting (wireless) transmitters, or televisors or for gramophone recordings.

Part E:-

The Association shall also consist of such independent contractors who, if they were employees performing work of the kind which they usually perform as independent contractors, would be employees eligible for membership of the Association.

Part F:-

Part to reflect orders made under the Industrial Relations Act 1988 (now the Workplace Relations Act 1996) and recorded in Print N5128

Notwithstanding anything elsewhere contained in this rule and without limiting Parts A, B, C, D and E of this rule and without in any way being limited by parts A, B, C, D or E, for the purpose of giving effect to the orders made on 18 September 1996 and recorded in Print N5128 and subject to further order of the Commission to vary or set aside the orders, with effect from 4 July 1997 the industry in connection with which the Association is registered shall include the industry of every person employed or likely to be employed in or in connection with the Live Theatre and Concert Industry which, for the purposes of this rule, shall mean all activities undertaken in or in connection with producing, presenting, or otherwise undertaking live theatrical, performance art, operatic, orchestral, dance, variety, revue, comedy, multimedia, choral, or musical performances, productions, presentations, workshops, rehearsals or concerts, including the provision, sale, service or preparation of food or drink and also including selling tickets by any means, for or in or in connection with any such performances, productions, presentations, workshops, rehearsals or concerts, and including the operation of venues or other facilities, whether permanent or temporary, utilised for such performances, productions, presentations, workshops, rehearsals or concerts, whether or not such performances, productions, presentations, workshops, rehearsals or concerts are performed or presented in the presence of an audience, or are recorded by any means.

4 - ELIGIBILITY FOR MEMBERSHIP

Part A:

the following persons shall be eligible for membership:

Without limiting parts B, C, D or G of this rule and without in any way being limited by parts B, C, D or G:

The Association shall consist of an unlimited number of persons employed on any contractual, (i) weekly, daily or other basis of employment as actors, actresses, singers, choristers, dancers, variety, revue and/or vaudeville artists, circus artists, supernumeraries, extras, understudies, showgirls, models, nudes, mannequins, stand-ins, skaters, aquatic performers, comperes, announcers, narrators and stunt men or women or persons employed for the purpose of commercial display in the theatrical, concert, cabaret, ballroom, hotel, restaurant, club, circus or skating branches of the entertainment industry or in any other place which could be construed to be a place of entertainment, or who are employed as entertainers in any other place, or who are employed in the cinematographic film, television, television film, wireless broadcast recording, commercial wireless broadcasting, or other wireless broadcasting stations, or any other sections of the wireless broadcasting industry, or in the production of gramophone recordings, and all persons employed by or at commercial or other wireless broadcasting stations, or in the production of transcribed radio programs or transcribed commercial announcements for use in wireless broadcasting as monitors, comperes, narrators, members of general information or quiz programs, announcers, monitors of international broadcasts for the purpose of gathering material, translators, checkers, and other persons engaged in the presentation and/or preparation of foreign language broadcasts, and all writers who write specialised radio or television scripts and material as defined in Schedule A hereof, and writers of film scripts and/or scenarios and all persons who are employed at commercial wireless broadcasting stations or elsewhere in the production of transcribed wireless broadcast programs and/or commercial announcements or direct (live) wireless broadcast programs as members of the presentation, program, record library, and/or continuity staff, or in manual sound effects work, or employed as advertising copywriters by a commercial wireless broadcasting station together with such other persons whether employed in the industry or not as have been

appointed officers of the Association (including appointed as Organisers) and admitted as members thereof at present or in the future.

Provided however that an employee whose work in the main consists of writing news or similar commentaries or an employee whose work in the main consists of writing news and similar commentaries and who also verbally broadcasts these commentaries, instrumental musicians other than variety artists, copyists of music, persons engaged on technical and mechanical duties and included within the constitution of the Professional Radio Employees Institute of Australia, or the constitution of the Postal Telecommunication Technicians Association, or employees included within the constitution of the Federated Clerks Union or officers or employees of the Australian Broadcasting Commission who are qualified by the Constitution of the Australian Broadcasting Commission Staff Association to become other than Associate members of the Australian Broadcasting Commission Staff Association, employees engaged solely as clerks, telephonists, watchmen, caretakers, cleaners, or lift attendants or salesmen, copywriters employed by advertising agencies, shall not be eligible for membership.

Schedule A: A writer of specialised radio or television material is one who writes specialised radio or television material, irrespective of length, which is suitable only for radio or television presentation and is pre-designed for that purpose, such as comic or straight dramatic spots, straight plays, including drama, comedy, farce, burlesque & c., musical or variety performances, documentaries in dramatic, musical or other entertainment form and adaptations designed specifically for radio or television performances from an original play or book.

- (ii) Without limiting or in any way being limited by sub-rule (i) of this rule, the Association shall also consist of persons employed as:
 - (a) disc jockeys and discotheque comperes;
 - (b) bingo, housie callers;
 - (c) puppeteers excluding persons whose sole duties are the building, painting and finishing of puppets;
 - (d) stunt co-ordinators and stunt performers;
 - (e) performance artists.

Part B:

the following persons shall be also eligible for membership:

Without limiting parts A, C, D or G of this rule and without in any way being limited by parts A, C, D or G:

The Association shall also be composed of an unlimited number of employees employed in or in connection with, including selling tickets by any means in connection therewith, or in or about, any kind of amusement, whether indoor or outdoor, including:-

- (a) cultural complexes, theatres, halls, racecourses, sports, exhibitions, agricultural shows, planetaria, animal parks, puppet shows and film exchanges, but excluding any person employed in or about the foregoing in any capacity in or in connection with the provision, sale, service or preparation of food or drink;
- (b) Clubs, licensed clubs and discotheques, but only insofar as such employees are employed as set and property carpenters and painters, stage crews, mechanists, projectionists, audio and lighting technicians, flymen, props persons, scenic artists, wardrobe including dressers, costume and property workers, stage managers, make-up artists, hairdressers, wigmakers and wig dressers, directors, choreographers and designers;

- (c) Casinos, but only insofar as such employees are employed as supervisors, pit bosses, inspectors, croupiers, dealers, bankers, cashiers and change clerks, but excluding such persons employed at the Wrest Point Casino, Tasmania;
- In all aspects of Motion Picture Film, Video and Television Production and Processing, the (d) Australian Film Commission and the Australian Film and Television School, including but without limiting the generality of the foregoing Producers, Directors, Production or Studio Unit Managers, Assistant Directors, Production Accountants, Dialogue and/or Commentary Writers, Script and/or Continuity Recordists, Location and/or Talent Scouts, Contact Men, Make-up Artists, Casting Directors, Art Directors, Chief Cameramen, Operative Cameramen, Special and/or Process Cameramen, Title and/or Cartoon Cameramen, Camera Dolly and/or Rotambulation Operations, Slate Operations, Studio Gripmen, Studio Mechanists, Chief Sound Engineers, Sound Engineers, Sound Recordists, Microphone Boom Operators, Sound Mixers, Film Editors, Film Cutters, Specialist Film Cutters, Film Librarians, Film Vault Keepers, Film Splicers, Laboratory and/or Studio Maintenance Men, Film Stock Keepers, Film Laboratory Managers, Film Laboratory Chemists, Film Printing Operators, Film By- Product Recovery Chemists, Film Timers, Film Cleaners and/or Waxers, Film Checkers, Laboratory and/or Studio Projectionists, Film Processors, Film Graders, Film Despatchers, Film Packers and Film Examiners, Supervising and other classes of Technician involved in Maintenance, Installation, Videotape, Lighting, Telecine or Audio Departments, Cinecameramen, Videocameramen, Set Designers, Graphic Artists, Co-ordinators, Stills Photographers, Floor Managers, Film Sound Recordists, Wardrobe Supervisors and Assistants, Set and Property Carpenters and Painters, Property men/women, Scenic Artists, Producers/Directors Assistants, Vision Switchers, Set Dressers, Hairdressers, Film Department Assistants, Studio Hands, Film/Videotape and Record Librarians, Property and Scenery Storemen, and all trainees and inexperienced adults employed in or in connection with television or videotape production houses;
- (e) In film and television distribution, persons employed in film release and control, statistics and contracts, film despatch, (other than officers in charge), projectionists, assistant projectionists, film packers, film checkers, film examiners, film cleaners and film splicers; and
- (f) Cinemas;
- (h) All persons employed or to be employed at World Congress Centre Melbourne and/or the Melbourne Exhibition Centre, other than the employees of contractors providing cleaning, carparking, or food and drink services.

together with such other persons, whether so employed or not as have been elected Officers and Industrial Staff of the Association and have been admitted as members thereof.

The following persons, otherwise eligible for membership of the Association under Part B shall not be eligible for membership by reason of that Part:

All persons employed or to be employed by Kirby Banner Pty Ltd (collectively trading as Movie World Enterprises) at the Movie World Theme Park, Movie Studios (except where such employees are engaged directly in the production of film or television programmes) and Wet'N'Wild Water Slide Complex at Oxenford in the State of Queensland.

Part C:

the following persons shall be also eligible for membership:

Without limiting parts A, B, D or G of this rule and without in any way being limited by parts A, B, D or G:

(a) The Association shall also consist of persons employed or engaged -

Page 8 of 65 Pages

- 1. as journalists, authors, licensed or official shorthand writers, Hansard reporters and publicity and public relations officers;
- 2. in any branch of writing or drawing or photographic work for the press;
- 3. in the collection and/or preparation of news, and/or information on current events for broadcasting or radio transmission;
- 4. in any form of writing, collection and/or preparation of news and/or information on current events, or drawing or news photography for use in television services;
- 5. in any branch of writing or drawing or photographic work for publicity, published instructions or public relations purposes;
- 6. wholly or in major part as script writers, except those engaged solely, or in major part, in the preparation of advertising material for broadcasting or radio or television transmission;
- 7. in the Public Service of the Commonwealth or a State -
 - (a) as journalists in writing and/or preparing matter for publication in newspapers, magazines, books or pamphlets and/or broadcasting and persons performing work of a similar nature as publicity officers or public relations officers;
 - (b) as photographers, the greater part of whose duty is to take and prepare photographs for reproduction in newspapers and/or magazines.
- (b) Only those persons who constantly or regularly perform substantially the work specified in Clause (a) of this Rule, shall be eligible for membership.
- (c) Persons not eligible to be members of the Association are:
 - 1. the Editor-in-Chief and the Editor of a metropolitan daily newspaper;
 - 2. the chief of the general reporting staff permanently employed as such on a daily newspaper in a capital city;
 - 3. a proprietor or part-proprietor of a newspaper who does not derive the major part of his or her income from salary or other remuneration for journalistic work.
 - 4. Any person eligible for membership of the Theatre Managers' Association as at the 27th day of March, 1958.
 - 5. Any person who is a member, staff member or special member of the Australian Federal Police.

Part D:

the following persons shall be also eligible for membership:

Without limiting parts A, B, C or G of this rule and without in any way being limited by parts A, B or C:

The Association shall also consist of an unlimited number of persons

- (a) who are employees or whose occupation is that of an employee in or in connection with the industry as set out in Rule 3, part C;
- (b) who are employees engaged in an industrial pursuit in or connected with the industry as set out in Rule 3, part C;

Page 9 of 65 Pages

- (c) who are employees qualified to be employed in or in connection with the industry or to be engaged as employees in an industrial pursuit connected with the industry as set out in Rule 3, part C;
- (d) who are officers of the Association and who have been admitted as members of the Association.

A person otherwise eligible under sub paragraph (c) of this part shall not be admitted as a member of the Association if such admission shall have the effect of causing the Association to cease being effectively representative of the members employed in or in connection with the industry and the members engaged in industrial pursuits in or connected with the industry.

Provided that persons who are eligible to be members of the Association of Architects Engineers Surveyors and Draughtsmen of Australia in accordance with the registered rules of Association of Architects Engineers Surveyors and Draughtsmen of Australia as at 24 October 1978 shall not be eligible for membership of the Association under this part.

Part E:

The Association shall also consist of such independent contractors who, if they were employees performing work of the kind which they usually perform as independent contractors, would be employees eligible for membership of the Association.

Part F:

No restriction or qualification under parts A B C D or G of this rule shall restrict or qualify eligibility for membership under any other parts of this rule.

Part G:

Part to reflect orders made under the Industrial Relations Act 1988 (now the Workplace Relations Act 1996) and recorded in Print N5128

For the purposes of this rule, the Live Theatre and Concert Industry shall mean all activities undertaken in or in connection with producing, presenting, or otherwise undertaking live theatrical, performance art, operatic, orchestral, dance, variety, revue, comedy, multi-media, choral, or musical performances, productions, presentations, workshops, rehearsals or concerts, including the provision, sale, service or preparation of food or drink and also including selling tickets by any means, for or in or in connection with any such performances, productions, presentations, workshops, rehearsals or concerts, and including the operation of venues or other facilities, whether permanent or temporary, utilised for such performances, productions, presentations, workshops, rehearsals or concerts, whether or not such performances, productions, presentations, workshops, rehearsals or concerts are performed or presented in the presence of an audience, or are recorded by any means.

Notwithstanding anything elsewhere contained in this rule and without limiting Parts A, B, C, D and F of this rule and without in any way being limited by parts A, B, C, D or F, for the purpose of giving effect to the orders made on 18 September 1996 and recorded in Print N5128 and subject to further order of the Commission to vary or set aside the orders, with effect from 4 July 1997 the Association shall also be composed of:

- 1. persons employed or to be employed in all States and Territories of Australia other than Queensland in the Live Theatre and Concert Industry,
- 2. persons employed or to be employed in Queensland in the Live Theatre and Concert Industry,
 - (i) who are eligible to be members of the Association by virtue of Part A, Part C or Part D of this Rule as at 1 January 1996; or

- (ii) who are employed at major performing arts venues in Queensland including but not limited to the Queensland Performing Arts Centre, and the Suncorp Theatre, or at companies or employers in receipt of subsidies from either Commonwealth or Queensland state arts funding bodies, including but not limited to the Queensland Theatre Company, the Queensland Opera, Queensland Ballet, and Dance North, or by companies engaged in the contracting of theatre technical and crewing services, or by the Tjapuki Dance Theatre; or
- (iii) who are employed at venues or by companies associated with institutions of higher learning and including persons employed by student unions or guilds; or
- (iv) who are employed in theatre restaurants; or
- (v) who are employed at the Gold Coast Arts Centre and at Jupiters Casino; or
- (vi) who are employed at venues or by employers in Queensland which are members of the National Association of Regional Performing Arts Centres other than at the NARPAC centre at Redcliffe Queensland.

Part H:

Notwithstanding the provisions of Part A, Part B, Part C, Part D, Part E and Part G of Rule 4, the following persons shall not be eligible for membership of the Union:

All persons employed or to be employed by Village Sea World Operations Pty Ltd and Warner Sea World Operations Pty Ltd (collectively trading as Sea World Enterprises) at the Sea World Theme Park, Gold Coast and its associated facilities; and

All persons employed or to be employed by Janola Dale Pty Ltd, its successors, assignees or transmittees at Dreamworld Theme Park, Coomera, Queensland.

5 - DEFINITIONS

Unless the context otherwise requires, the following construction shall be applied throughout these Rules:

- means an individual or organisation whether incorporated or (a) Associate Member unincorporated which is not eligible for full membership of the Association (b) board means a group of persons who supervise, govern or otherwise have oversight of a corporation, organisation, association or other like body including a Board of Directors Chief Executive means the senior employee appointed to administer on behalf of the (c) Federal Council and the Board the overall operations of the Association. disclosure period (d) For the purpose of these rules means the financial year unless a shorter period is specified.
- (e) declared person or body A person is a declared person or body if:
 - (i) an officer of the Association or a Branch of the Association has disclosed a material personal interest; and
 - (ii) the interest relates to, or is in, the person or body; and

Page 11 of 65 Pages

- (iii) the officer has not notified the Association or a Branch of the Association that the officer no longer has the interest. financial duties includes duties that relate to the financial management of the Association (f) or a Branch of the Association. non-cash benefit means property or services in any form other than money, but does not (g) include a computer, mobile phone or other electronic device that is used only or mainly for work purposes. (h) office has the same meaning as defined by section 9 of the Fair Work (Registered Organisations) Act 2009. (i) Regional Director means the employee appointed to administer the Association's operations in states and/or territories has the same meaning as defined by section 9B of the Fair Work related party (i) Registered Organisations) Act 2009. (k) relative in relation to a person, means: (i) parent, step parent, child, stepchild, grandparent, grandchild, brother or sister of the person; or (ii) the spouse of the first mentioned person. (1) in relation to an officer of the Association or Branch of the Association relevant remuneration for a disclosure period is the sum of the following: any remuneration disclosed to the Association or Branch of the (i) Association by the officer during the disclosure period; (ii) any remuneration paid during the disclosure period, to the officer of the Association or Branch of the Association. (m) relevant non-cash in relation to an officer of the Association or Branch of the Association benefits for a disclosure period means the non-cash benefits provided to the officer, at any time during the disclosure period, in connection with the performance of the officer's duties as an officer, by the Association or Branch of the Association or by a related party of the Association or Branch of the Association. remuneration (i) includes pay, wages, salary, fees, allowances, leave, benefits or (n) or other entitlements; but does not include a non-cash benefit; and (ii) does not include the reimbursement or payment of reasonable (iii) expenses for the costs incurred in the course of the officer carrying out his or her duties.
- (o) "Member" means a duly admitted member of the Association other than an Associate Member.
- (p) "international member" means a member who is not ordinarily resident in Australia and who is employed in Australia on a temporary basis or pursuant to a contract for a specified duration and/or specified work [e.g. a theatrical or concert tour, film, radio or television programme].
- (q) "Quarter" means those three month periods ending March 31, June 30, September 30 or December 31 in any year.

7 - ADMISSION TO MEMBERSHIP

- (r) "Half-year" means those six month periods ending June 30 or December 31 in any year.
- (s) The "Association" means the Media, Entertainment and Arts Alliance.
- (t) "Officer" means any person who has been elected or appointed to the Federal Council or the Board or a Branch Council of the Association.
- (u) "Honorary Officer" shall be an office in the Association other than a full-time office provided that the Federal Council and/or the Board from time to time may decide to second such an officer to an employed position within the Association for a limited period or to work on a particular project or assignment.
- (v) "Federal Section Presidents" means Federal President [Media], Federal President [Actors Equity], Federal President [ECS] and Federal President [Musicians].
- (w) "Meeting" includes any meeting held by any means, including by telephone, post, email, on-line or any other electronic manner.
- (x) Senior employee means a person appointed to the position of Director.

Words of the singular number shall include the plural and vice versa. Words of the masculine gender shall include the feminine gender.

6 - REGISTERED OFFICE

The Registered Office of the Association shall be: 245 Chalmers Street Redfern NSW 2016.

The situation of the Registered Office may be altered at the discretion of the Federal Council and such alteration shall be notified immediately to the Federal Industrial Registrar by the Chief Executive.

In each state there shall be Association offices the location of which office may be altered by the Branch Council, with the approval of the Board.

SECTION 2 - MEMBERSHIP

7 - ADMISSION TO MEMBERSHIP

- (a) A person wishing to apply for membership of the Association shall complete an application form approved by the Association. Unless otherwise exempted by the Chief Executive, Branch Secretary or Regional Director, the applicant shall pay an entrance fee according to their category of membership as determined from time to time by the Board.
- (b) The Chief Executive, Branch Secretary or Regional Director shall examine the application and once satisfied that:
 - (i) the person is eligible for membership
 - (ii) the person has paid the required fees or has made arrangement to pay or has been exempted from paying all or part of the required fees

Page 13 of 65 Pages

8 - TEMPORARY & INTERNATIONAL MEMBERSHIP

the Chief Executive, Branch Secretary or Regional Director shall approve the application or refer the application to the next meeting of the Branch Council.

- (c) No error, omission or want of form in connection with any application for or admission to membership shall invalidate membership.
- (d) Each member shall be deemed to be attached to the branch of the Association in which he or she resides and the section to which he or she is allocated by the Branch Council in accordance with the relevant policy regarding allocation to sectional membership then in force provided that where a member's employment is in a branch other than the branch where the member resides [e.g. in a border town or city] the Chief Executive, Branch Secretary or Regional Director may allocate that member to the branch where the member is employed. For the purposes of these Rules members residing in the Northern Territory shall be regarded as residing in South Australia.

And further provided that members of the Professional Sports Branch shall be attached to that Branch no matter where they may reside and shall not be members of any other Branch.

- (e) Each member when allocated to a section shall have the rights and responsibilities of a member of that section as determined by these rules and by the Federal Council. Members who wish to be allocated to more than one section will nominate, and be allocated to, a primary section and will be entitled to vote in sectional elections for that primary section only. Where a member wishes to be allocated to another section or sections or transfer to another section, he or she shall submit an application to that effect to the Chief Executive, Branch Secretary or Regional Director.
- (f) Where a member is admitted to another section or transfers her or his membership, the member shall be required to pay the difference between any entrance fee or subscriptions applicable to that section, unless the amount is waived by the Chief Executive, Branch Secretary or Regional Director.
- (g) Applicants for membership shall be advised by the Association in writing of:
 - (i) the financial obligations arising from membership of the Association; and
 - (ii) the circumstances, and the manner, in which a member may resign from the Association.

7A - ASSOCIATE MEMBERSHIP

An Associate Member is an individual or organisation whether incorporated or not that supports the Association's aims and objectives. Associate Members are persons or entities that are not eligible to become full members under Rule 4. Associate Members can be invited to attend general meetings and speak where invited to do so or where a majority of members present support a request to address the meeting. Neither an Associate Member nor its representative shall be entitled to vote or hold office in the Association or to take part in any election under these Rules.

8 - TEMPORARY & INTERNATIONAL MEMBERSHIP

- (a) The Federal Council of the Association may create categories of temporary membership which will allow the enrolment of members for fixed periods of time.
- (b) International members shall be admitted for the period during which they are contracted to perform services in Australia pursuant to a valid visa. At the end of the such period the member shall cease to be a member of the Association.

Page 14 of 65 Pages

9 - ENTRANCE FEES

- (a) Entrance fees shall be determined by the Board.
- (b) Additional entrance fees shall be payable where a member moves from one category to another or from one section to another. Where this occurs, and the member is admitted to the new category or section, the member shall pay the difference between the entrance fee previously paid by him or her and the entrance fee payable by new applicants coming within the category or section to which he or she has moved. Failure to pay such difference to the Association not later than eight weeks after an account or other written demand for its payment has been forwarded to the member shall render the member unfinancial.
- (c) Payment of all or part of the entrance fee may be waived, reduced or deferred by the Chief Executive, Branch Secretary or Regional Director.

10 - SUBSCRIPTIONS

- (a) Unless relieved of the liability to do so by the Chief Executive, Branch Secretary or Regional Director under these rules, each member or person authorised to make subscription payments on their behalf, shall pay an annual subscription to the Association. Subscriptions shall be fixed each year by the Board no later than April 30 before the financial year in which the subscriptions are to be charged.
- (b) Subscriptions for members in any year shall fall due on the first day of July in that year and shall be payable in advance. They may be paid:
 - (i) yearly;
 - (ii) half-yearly;
 - (iii) by regular deductions from the member's pay;
 - (iv) by regular deductions from a member's bank or similar account or credit card; or
 - (v) by such other means as the Chief Executive, Branch Secretary or Regional Director may approve.
- (c) A member will become unfinancial:
 - (i) in the case of members paying yearly, if payments are not made within two calendar months of July 1 in each year;
 - (ii) in the case of half-yearly payments, if payments are not made within two calendar months of July 1 and/or January 1 in each year; or
 - (iii) in the case of a member paying by regular deductions from the member's pay or from a member's bank or similar account or credit card, if no payments are received for 93 days.
- (d) An unfinancial member shall become financial when:
 - (i) All outstanding monies are paid, or
 - (ii) The member enters into a scheme for periodic payments approved by the Branch Secretary.

11 - RIGHTS OF MEMBERS

- (e) The Chief Executive, Branch Secretary or Regional Director may make arrangements with employers or government departments for the deduction, on the signed authority of the member, of entrance fees and/or subscriptions from the members wages or other monies payable to the member, and for the forwarding of such amounts to the Association. Any such arrangements shall conform to any guidelines determined by the Board to apply to such deduction schemes. As long as such authority remains in force, the member shall be regarded as a financial member provided that if no subscriptions are received from a member in respect of employment for three months, the member shall be regarded as an unfinancial member as from the first day of the succeeding half year until such time as a further payment is received or action is taken under either Rule 15 or 17.
- (f) Additional subscriptions may be payable where a member moves from one category to another or from one area of employment or section to another. Where this occurs, and the member is admitted to the new category or section, the member shall pay the difference between the subscriptions previously paid by him or her and the subscriptions payable by new applicants coming within the category or section to which he or she has moved. Failure to pay such difference to the Association not later than eight weeks after an account or other written demand for its payment has been forwarded to the member shall render the member unfinancial.
- (g) Fines and Levies shall be the first charge on all payments by members.
- (h) Any member who fails to pay her/his subscriptions (and/or fines and levies) prior to or upon the due date may also be required thereafter to pay any additional costs incurred by the union in the recovery of the outstanding subscriptions (and/or fines and levies).
- (i) Payment of all subscriptions, entrance fees, levies and fines may be made to any person authorised by the Chief Executive to receive them.
- (j) Payment of any sum due by any member under these Rules may be postponed, reduced or waived by the Chief Executive, Branch Secretary or Regional Director if, in her or his view, it would be appropriate to do so.
- (k) Where payment of subscriptions is postponed by a decision under sub-rule (h), the member shall be regarded as a financial member as from the date of such decision until the date specified in the decision for payment of such postponed amount, provided that any other sums due by the member to the Association are paid in accordance with these Rules.
- (l) Where an amount is reduced or waived by a decision under this sub-rule, the financial status of the member shall be determined as though the amount reduced or waived had been paid by the member on the date of the decision or such other date as may be specified in the decision.
- (m) It shall be the duty of each member or person authorised to make subscription payments on their behalf, without the necessity for any request to do so, to pay his or her subscriptions when required to do so by these rules to any person authorised by the Association to receive such subscriptions.

11 - RIGHTS OF MEMBERS

- (a) Each financial member shall be entitled to all the rights and privileges of membership prescribed in these rules and to participate to the maximum degree possible in the activities of the Association under the Rules. Without limiting these rights, each member shall also be entitled to vote in any relevant election, plebiscite or ballot in accordance with these rules.
- (b) Each financial member shall be entitled to attend any Association, branch, sectional committee or branch council meeting to which he or she is attached as an observer. Provided that such member may be required to leave any such meeting where confidential information is being discussed.
- (c) Any financial member may at a reasonable time during office hours inspect the books and records of the Association or of a Branch upon giving the Chief Executive, Branch Secretary or Regional

Page 16 of 65 Pages

13 - MEMBERSHIP HONOURS

Director as the case may be, 72 hours' notice in writing of their wish to do so <u>provided that</u> the member shall not have the right to inspect any graded, staff or employment list other than that relating to his or her employment or to see any confidential record except that relating to the member personally.

12 - DUTIES OF MEMBERS

- (a) Each member shall be bound by the rules of the Association and each shall take all steps as are reasonable in the circumstances to ensure that the rules of the Association are observed.
- (b) Each member shall pay his or her dues and any other monies owing or due to be paid to the Association without a request to do so having to be made to the member.
- (c) Any member in attendance at a meeting of the Association which is to deal with a matter which affects that member's activity as an employer or agent of an employer shall, immediately prior to discussion of that matter, rise to declare his or her interest. Upon the objection of any other member, the Chair of the meeting shall exclude the member with a declared interest while the particular matter is dealt with.
- (d) Any member who believes that another member should declare his or her interest in a matter shall ask the Chair to give a ruling on whether a declaration of interest should be made. The member under challenge shall have the right to be heard. Upon an interest being found by the Chair, the member under challenge shall be excluded from the meeting during the debate and voting on a matter subject of a declared interest upon one member objecting in accordance with this sub-rule.
- (e) A member who is indebted for any sum of money to the Association in any way whatsoever notwithstanding that the member may not be unfinancial within the meaning of this Rule, shall pay within seven days of his or her receipt from the Chief Executive or Branch Secretary or Regional Director, a demand for payment of such sum of money.
- (f) Each member shall co-operate with the officers of the Association, representatives and workplace delegates.
- (g) A member changing her or his residence shall report this in writing to the Chief Executive, Branch Secretary or Regional Director within twenty-eight days of such change.

13 - MEMBERSHIP HONOURS

(1) Honorary Membership

- (a) The Branch Council may create an Honorary Membership and by resolution may transfer to such membership any financial member or former member who has been a member of the union for no less than 10 years and who has rendered valuable assistance in promoting the Objects of the Association and who is not employed on work defined in rule 4.
- (b) Honorary Members shall not pay any dues to the Association and shall not exercise any voting power. They shall be entitled only to receive notice of any General Meeting, to attend and speak at such meetings, to receive copies of the Association's journal and any report or document issued by the Association to the general membership.
- (c) Honorary Members shall not be included in the membership of the Branch, but a list of Honorary Members may be published in the annual report of the Branch.
- (d) Honorary Members on obtaining employment in work defined in Rule 4 may be readmitted to membership without entrance fee on making application.

(2) Gold Honour Badge

- (a) The Gold Honour Badge of the Association may be awarded by Federal Council to a member for meritorious services, which, in the opinion of the Council, were of conspicuous benefit to the Association.
- (b) The design of the Gold Honour Badge shall be determined by Federal Council.
- (c) Federal Council shall not make an award of the Gold Honour Badge unless at least 75 per cent of delegates vote in favour of such Award.
- (d) A record of the names of members awarded the Gold Honour Badge shall be kept by the Federal President on behalf of the Association.

(3) Honorary Life Membership

- (a) Honorary Life Membership of the Association may be conferred by Federal Council on any holder of the Gold Honour Badge who in the opinion of the Council has given long and outstanding meritorious services additional to those for which the Gold Honour Badge was awarded.
- (b) The Honorary Life Membership list shall be limited to a total of 20 recipients. When that number is reached, no further Honorary Life Memberships shall be bestowed until the number of living Honorary Life Members falls below 20.
- (c) The distinction of Honorary Life Membership shall be conferred only by the unanimous vote of Federal Council.
- (d) Honorary Life Members shall have all the rights and privileges of financial members of the Association.
- (e) A record of the names of members on whom the distinction of Honorary Life Membership has been conferred shall be kept by the Federal President on behalf of the Association.

(4) Honours Previously Granted

Members who immediately before the date of amalgamation enjoyed the status of life membership or long service life membership of the Australian Theatrical and Amusement Employees Association shall be deemed to have an award equivalent to the Gold Honour badge conferred under this rule. Persons conferred with such an honour shall not be required to pay subscriptions whether they are engaged in an occupation covered by Rule 4, part B, or not.

(5) The Federal Council in its discretion may confer upon members the distinction of Honorary Long Service Life Membership for those members who have at least 40 years of continuous membership in the Association. A member granted Honorary Long Service Life Membership shall retain all rights which accrue to financial members of the Association but shall not be required to pay any subscriptions or levy.

14 - UNFINANCIAL MEMBERS

(a) A member who has not paid subscriptions in accordance with rule 10 (or who is not an honorary life member), shall be deemed to be an unfinancial member and shall remain an unfinancial member until such time as all contributions including any fines, levies or other monies payable by the member have been paid.

Page 18 of 65 Pages

16 - RESIGNATION FROM MEMBERSHIP

- (b) An unfinancial member, except as provided by Rule 56, shall not be entitled to:
 - (i) Any of the rights privileges and benefits of the Association,
 - (ii) Hold any office in the Association,
 - (iii) Nominate for, or vote in, an election to any office,
 - (iv) Nominate any candidate for election to any office,
 - (v) Have access to union records,
 - (vi) Receive notice of any meetings,
 - (vii) Take part in any meeting or proceedings connected with the Association,
 - (viii) Receive copies of any journals, reports or documents issued by the Association.
- (c) The Association may deduct any subscriptions not paid in accordance with rule 10 from any moneys the Association receives on behalf of the member.

15 - TEMPORARY SUSPENSION OF MEMBERSHIP

- (a) Any financial member who expects to be absent from Australia or who expects not to be employed for six months or more on work defined in rule 4 and who desires to retain some form of contact with the Association, may apply to the Chief Executive.to be taken off the membership list and placed on a temporary suspension list. Unless the Chief Executive decides otherwise, only persons who agree to notify the Association when they resume employment in the industry shall be eligible to be placed on the temporary suspension list.
- (b) Persons who are placed on the temporary suspension list shall not pay any fees to the Association and shall not be members of the Association for the period of being on the temporary suspension list.
- (c) A person on the temporary suspension list on obtaining employment covered by Rule 4 shall again become a member entitled to all rights, privileges and benefits of membership provided they make themselves financial in accordance with Rule 10.
- (d) If a person whose membership is temporarily suspended takes up work and does not notify the Association the members' dues shall become payable as and from the date when the member so resumes work.
- (e) A person on the temporary suspension list shall, if he or she desires, receive copies of any relevant Association publication. The Board may require a subscription fee for any publication.
- (f) The Association may deduct an administrative charge from any moneys the Association receives on behalf of a member who has placed his/her membership on temporary suspension.

16 - RESIGNATION FROM MEMBERSHIP

(a) A member or associate member may resign her or his membership of the Association by notice in writing and such resignation shall take effect:

Page 19 of 65 Pages

19 - BRANCH COUNCIL

- (i) Where the member or associate member has ceased to be eligible to become a member of the Association on the day on which the notice of resignation is received or a later date if that later date is specified in the notice; or
- (ii) In any other case, at the end of two weeks after the day on which the notice of resignation is received or a later date if that later date is specified in the notice.
- (b) Notice of resignation shall be in writing, addressed and delivered to the Chief Executive, Branch Secretary or Regional Director as appropriate.
- (c) For the purposes of this Rule, subscriptions payable shall be calculated on a quarterly basis. Nothing in this rule shall mean that any or all subscriptions, fines and levies owed by the member or associate member to the Association and payable on the date on which the resignation is to take effect and unpaid, shall not continue as a debt owed by the member to the Association.
- (d) The Association may deduct an administrative charge from any moneys the Association receives on behalf of a member or associate member who has resigned his/her membership of the Association.

17 - REMOVAL FROM THE ROLL OF MEMBERS

The Chief Executive may at any time purge the roll of membership by striking off the names of members:

- (i) who are in arrears of more than six months;
- (ii) who have ceased to be eligible to become a member of the Association;
- (iii) whose address is unknown; or
- (iv) who are deceased,

but such action shall not free any such discharged member from liability for the arrears at the time the member is removed from the roll.

The Association may deduct an administrative charge from any moneys the Association receives on behalf of a member whose membership has been purged from the roll.

SECTION 3 - BRANCHES

18 - BRANCHES

- (a) Federal Council may by resolution establish branches within the membership to reflect geographical locations and/or occupational groupings within the Association.
- (b) Provided that no branch shall be dissolved, amalgamated or have its boundaries altered without first being consulted by the Board, or where authorised by the Board, the Chief Executive and approved by the Branch Council of the affected Branch or by a vote of Federal Council carried by no fewer than 75% of the votes exercised by Federal Councillors.

19 - BRANCH COUNCIL

(a) Subject to these rules, the supreme governing body of each Branch of the Association shall be the Branch Council.

Page 20 of 65 Pages

- (b) The Branch Council shall be responsible for the general conduct and control of the Branch of the Association within the powers and decisions of the Federal Council and the Board.
- (c) Federal Council, in consultation with the Branch, shall determine that the Branch Council shall consist of either:
 - (1) (i) the Branch President
 - (ii) three Branch Vice-Presidents
 - (iii) the Branch Secretary (in those branches where Federal Council has approved the creation of a Branch Secretary)
 - (iv) Delegates from the sections of the Association as determined by Rule 80 [other than in those branches where Federal Council has determined that the number of delegates shall be zero].

Or

- (2) (i) the Branch President of each section that has more than 100 financial members within the Branch
 - (ii) the Branch Vice-President of each section that has more than 500 financial members within the Branch
 - (iii) the Branch Secretary (in those branches where Federal Council has approved the creation of a Branch Secretary)
 - (iv) Delegates from the sections of the Association as determined by Rule 80 [other than in those branches where Federal Council has determined that the number of delegates shall be zero].
- (d) The Branch Council shall meet whenever convened by the Branch President, or whenever determined by the Branch Council or the Board. Notice of any such meeting shall be given to all members of Branch Council by the officer convening the meeting. Where practicable, such notice shall be given in writing.
- (e) Notwithstanding any other rule precluding an officer being an employee of the Association, the Branch Council may, with the approval of the Board, in the case of absence of the Branch Secretary or Regional Director, appoint another member of the Association, eligible under the rules, to act as Branch Secretary or Regional Director for the period of such absence provided that no such appointment shall exceed 12 months. A member appointed under this rule may hold another office in the Association during such appointment.
- (f) The Branch Council shall decide all matters in accordance with these Rules. A decision of Branch Council shall be final and binding throughout the Branch and shall remain in force until superseded, amended or rescinded either at a subsequent meeting of the Branch Council, by the Board or Federal Council or by decision of the members reached by plebiscite of the Branch or Association.
- (g) The Branch President or in his or her absence, a Branch Vice-President shall preside at all Branch Council meetings or in the absence of these officers, a Chair shall be elected by the Council members present.
- (h) A quorum of members at a Branch Council meeting shall be a majority of the members, provided that the Board may approve a lesser quorum of no less than a third of the members.
- (i) If any member of Branch Council fails to attend three succeeding meetings without the leave of the Council, the Branch Council may declare the office vacant and seek to fill the office in accordance with rule 79(u).

20 - DELETED

21 – DELETED

22 - DELETED

23 - CONTROL OF BRANCH COUNCIL BY MEMBERS

- (a) All decisions of the Branch Council shall be subject to review by the members either by decision of a special general meeting or by the members voting in a plebiscite.
- (b) A special general meeting of members of the Branch may be called to consider a decision of the Branch Council where a petition of financial members signed by not fewer than 5% of the financial members of the Branch requests it.
- (c) The special general meeting so called may consider a resolution referring the decision of the Branch Council to the Federal Council. Where a resolution to that effect is carried, the Chief Executive shall take all necessary steps to refer the matter to the Federal Council for review of the decision of the Branch Council within eight weeks of the request of the special general meeting being made.
- (d) Alternatively, a Branch plebiscite shall be held to review a decision of the Branch Council where a petition of financial members signed by not fewer than 10% of the financial members of the Branch request it.
- (e) A request for a plebiscite must be made within eight weeks of the decision of Branch Council sought to be reviewed.
- (f) Where a valid request for a plebiscite is made, the Branch Council shall appoint a returning officer who shall:-
 - (i) Take all such steps and have all necessary authority to conduct such plebiscite;
 - (ii) Set out the question to appear on the ballot paper,
 - (iii) Fix a date and time for the issue of ballot papers by the returning officer and also a date and time for the closing of the plebiscite,
 - (iv) Ensure that a full and fair explanation as to the reason for the plebiscite, and the competing views as to whether members should vote for or against it, accompanies the ballot paper.
- (g) A ballot paper issued in relation to this rule, shall be in the following form:-

"Are you in favour of the following......".

Then follows the resolution of Branch Council on which the plebiscite is being taken.

YES() NO()

- (h) The Branch returning officer shall conduct such ballot in accordance with rule 79 of these rules and any member may arrange to attend to scrutinise the returning officer's activities. The returning officer shall conduct the plebiscite promptly.
- (i) The Branch Secretary or Regional Director shall submit the report of the Returning Officer to the next meeting of the Branch Council.

28 - POWERS & DUTIES OF BRANCH SECRETARIES AND REGIONAL DIRECTORS

(j) Any decision of the members voting in plebiscite shall be final and binding on the Branch of the union and its members until superseded by another plebiscite decision, or a decision of the Federal Council or, once a period of 25 years has elapsed, a decision of the Branch Council.

24 - DELETED

25 - BRANCH OFFICERS

The Branch Officers of the Association shall be in each branch the officers listed in either 19(c)(1)(i) and (ii) or 19(c)(2)(i) and (ii), and where determined by Federal Council, with the consent of the relevant Branch, Branch Secretary.

26 - BRANCH PRESIDENT

The Branch President shall:-

- (a) Be the senior officer of the branch and preside at all meetings of the branch and superintend the discussion of all business tabled for consideration.
- (b) Have a deliberative vote.
- (c) Be an ex-officio member of all sections, sub-branches, committees and sub-committees formed within the branch to advise the Association on matters concerning members or other Association matters and have the right to move and second motions, speak and vote at all meetings whether Council, Section, Committee or Sub-Committee or Special or General Meetings of members. The President may delegate this power, except the right to vote, to any member of the Branch Council to represent the President at any such meeting except at a meeting of the Branch Council.
- (d) Sign the Minutes of the proceedings of all meetings of the branch.
- (e) Where practicable, the Branch President shall be consulted by the Branch Secretary or Regional Director where urgent matters of substance arise between Branch Council meetings which require an urgent decision by the Branch Secretary or Regional Director. Any decisions so taken shall be reported to the Branch Council at the earliest opportunity by the Branch President, Branch Secretary or Regional Director.
- (f) The Branch President shall observe and cause to be observed all the rules, policies and decisions of the Association.

27 - BRANCH VICE-PRESIDENTS

- (a) There shall be three Branch Vice-Presidents. One of the Branch Vice- Presidents shall take the chair in the absence of the Branch President and thereupon shall have and may exercise all the powers of the Branch President.
- (b) In ordinary cases, one of the Branch Vice-Presidents shall assist the President in maintaining order at the meetings of the branch.

28 - POWERS & DUTIES OF BRANCH SECRETARIES AND REGIONAL DIRECTORS

The Branch Secretary or Regional Director (whichever is applicable) (and a person appointed to act as Branch Secretary or Regional Director in a temporary capacity in accordance with these Rules) shall conscientiously, efficiently and expeditiously do all things required to safeguard the interests of members and of the branch as a whole and:-

Page 23 of 65 Pages

30 - GENERAL MEETINGS

- (a) Attend all general meetings of the branch and Branch Council, keep the Minutes of such meetings (and send a copy of each set of minutes when completed, to the Chief Executive), and take note of all the necessary proceedings.
- (b) Be an ex-officio member of all sections, sub-branches, committees and sub-committees formed within the branch to advise the Association in matters concerning members or other Association matters and, in the case of Branch Secretaries, have the right to move and second motions, speak and vote at all meetings whether Council, Sub-branches, Section, Committee or Sub-Committee or Special or General Meetings of members.
- (c) On request of the Board or Federal Council or on a request signed by a majority of Branch Council members or on resolution of a General Meeting, hand over all books, documents and papers of the branch to a person named in such request within twenty-four hours of the receipt of such request, always provided that the provisions of these Rules relating to the removal of and/or suspension of officers shall prevail.
- (d) Obey the directions of the Branch Council regarding branch affairs.
- (e) Attend to all correspondence related to Branch affairs.
- (f) Take all such steps as are necessary and are required by the Branch Council, for the participation of the branch in a state industrial relation system.
- (g) Observe and cause to be observed all the rules, policies and decisions of the Association.

29 - DELETED

30 - GENERAL MEETINGS

- (a) Meetings which all the members of Branch are entitled to attend shall be known as Branch General Meetings. Meetings which all members of a section within a Branch are entitled to attend shall be known as Section General Meetings.
- (b) A general meeting may be convened at any time by:
 - (i) resolution of the Branch Council or Branch Sectional Committee as the case may be;
 - (ii) a request in writing signed by not less than five per cent of the financial members of the Branch or of the section as the case may be.
- (c) A general meeting shall be called by the Branch Secretary or Regional Director or in his or her absence, the Branch President, by notice giving at least 14 days notice either by:
 - (i) providing notice to each financial member at his or her last known address; or
 - (ii) forwarding a notice to all places of work where more than three members are employed and to theatrical and employment agents (where applicable).
- (d) The notice calling the meeting shall set out the place, date and time of the meeting and the nature of the business to be brought before the meeting.
- (e) The quorum necessary to transact business at general meetings shall be:
 - (i) At least 15 financial members in a branch with a financial membership not exceeding 200.

Page 24 of 65 Pages

33- PROTECTION OF SECTION PROFESSIONAL INTERESTS

- (ii) Two more financial members for each 100 financial members thereafter, provided that no quorum shall exceed 85.
- (iii) general meeting quorums shall be calculated by Branches according to the following table:

Financial Members	Quorum	Financial Members	Quorum		
0-200	15	1501-1600	43		
201-300	17	1601-1700	45		
301-400	19	1701-1800	47		
401-500	21	1801-1900	49		
501-600	23	1901-2000	51		
601-700	25	2001-2100	53		
701-800	27	2101-2200	55		
801-900	29	2201-2300	57		
901-1000	31	2301-2400	59		
1001-1100	33	2401-2500	61		
1101-1200	35	2501-2600	63		
1201-1300	37	2601-2700	65		
1301-1400	39	2701-2800	67		
1401-1500	41	2801-2900	69		

and thereafter an extra 2 members for each additional 100 members of the Branch to a maximum of 85 members.

- (f) A general meeting shall be called not later than 14 days after the receipt by the Branch Secretary or Regional Director, or in his or her absence the Branch President, of a request in writing signed by not less than 5 per cent of the financial members of the Branch or section as the case may be.
- (g) A general meeting shall not be convened in accordance with sub-rule (f) hereof for the purpose of reviewing any action or resolution of a Branch Council or section committee unless such request is made within eight weeks of the action or resolution which it is proposed to review.
- (h) A general meeting shall have the power to require the Branch Council or Section Committee or in the case of a matter of federal importance, the Board or Federal Council, to deal with a matter. The relevant body shall deal with the matter promptly.

31 - ROLL OF MEMBERSHIP

A register of the names of the officers and members resident in each branch, their postal addresses, sections and place of work (as far as known), shall be kept at the office of the branch and shall be open for inspection at all convenient times to the Industrial Registrar or any persons appointed by him or her. The register may be kept in a computerised form.

32 - DELETED

SECTION 4 - SECTIONS

33- PROTECTION OF SECTION PROFESSIONAL INTERESTS

(a) Notwithstanding anything else contained in these rules, the policies adopted by the Association regarding the professional standards and interests of members of any section (and in relation to

Page 25 of 65 Pages

35 - SECTION COMMITTEES

Journalists the establishment of a code of professional ethics) shall be determined exclusively by the section of the Association concerned. Such issues shall include the admission to membership of prospective members and approval of the entry to the country and the issue of permission to take up employment of those prospective members.

- (b) This rule shall only be altered with the consent of each of the sections of the Association and only after a plebiscite of each of the sections approves of any such alteration in accordance with the rule alterations rule 75.
- (c) For the purposes of this rule, professional standards and interests shall not include matters pertaining to wages and conditions of employment.

34 - SECTIONS

- (a) The Federal Council shall by resolution, establish sections within the membership to reflect occupational or industry groupings within the Association.
- (b) Upon the establishment of each section, the Federal Council shall issue a charter to the section, defining the scope of the section, and allocate members to each section.
- (c) Any dispute about the scope and membership of a section shall be determined by the Board , subject to appeal to the Federal Council.
- (d) New members shall be required to nominate a section which corresponds with their primary employment in the industry in accordance with Rule 7 of these rules. Once allocated to a section, a member shall not be reallocated without the approval of the Branch Council. A member shall be allocated to a primary section and may stand for any elective office and vote only as a member of that section.
- (e) The Federal Council shall have the power, subject to this sub-rule, to decide that a section shall be dissolved or amalgamated with another section. The size of a section shall be a factor to be taken into account by the Federal Council when making such a decision. No section shall be dissolved or amalgamated without first being consulted by the Federal President, and approved by the national sectional committee of the section concerned or by a vote of Federal Council carried by no fewer than 75% of votes exercised by Federal Councillors.

35 - SECTION COMMITTEES

- (a) Federal Council may approve the formation of a National Section Committee in any section.
- (b) The National Section Committee shall consist of all members of Federal Council who are members of that section and the vice-presidents of each branch entitled to three or more votes at Federal Council in accordance with Rule 80 where the holder of that office is member of the relevant section but not also a member of Federal Council.
- (c) Each member of the section committee shall exercise a single deliberative vote. Decisions shall be by a majority of votes cast.
- (d) A National Section Committee may adopt by-laws to govern its conduct and activities, subject to the approval of those by-laws by the Federal Council.
- (e) The National Section Committee may approve the formation of a State Section Committee in any State. A State Section Committee shall consist of all members of Federal Council who are members of the relevant section in that State together with all members of the Branch Council in that State who are members of the relevant section and such other members as are co-opted by the State Section Committee.

Page 26 of 65 Pages

39 - SECTION PLEBISCITES.

- (f) The National Section Committee shall have the power to make recommendations to the Board and Federal Council on all matters pertaining to that section especially those matters affecting the policies and industrial objectives to be adopted by the Association.
- (g) The State Section Committee shall have the power to make recommendations to the Branch Council and National Section Committee on all matters pertaining to that division especially those matters affecting the policies and industrial objectives to be adopted by the Association.
- (h) Each recommendation of a National Section Committee or a State Section Committee shall be considered by the relevant deliberative body at its next ordinary meeting except in cases of urgency.

36 - DELETED

37 - DELETED

38 - DELETED

39 - SECTION PLEBISCITES.

- (a) All decisions of a Section Committee shall be subject to review by the members of that section either by decision of a special general meeting or by the members of that section voting in a plebiscite.
- (b) A sectional plebiscite shall be held to review a decision of the National Sectional Committee or Branch Sectional Committee where a petition of financial members signed by not fewer than 5% of the financial members of the section or in the case of a Branch matter 10% of the financial members of the section attached to the branch in question requests it.
- (c) The Federal Council or a Branch Council with the approval of the Federal Council, may conduct a plebiscite on any question affecting a section or sections.
- (d) Where the plebiscite seeks to review a decision of the Association, a request for a plebiscite must be made to the Federal President or Branch President as the case may be within eight weeks of the decision sought to be reviewed.
- (e) Where a valid request or decision to hold a plebiscite is made, the Board or Branch Council (as the case may be) shall appoint a returning officer who shall:-
 - (i) Take all such steps and have all necessary authority to conduct such plebiscite;
 - (ii) Set out the question to appear on the ballot paper,
 - (iii) Fix a date and time for the issue of ballot papers by the returning officer and also a date and time for the closing of the plebiscite,
 - (iv) Ensure that a full and fair explanation as to the reason for the plebiscite, and the competing views as to whether members should vote for or against it, accompanies the ballot paper.
- (f) A ballot paper issued in relation to this rule, shall be in the following form:-

"Are you in favour of the following......?"

Then follows the question or matter on which the plebiscite is being taken.

 $YES() \qquad NO()$

40 - CONSTITUTION OF FEDERAL COUNCIL

- (g) The returning officer shall conduct such ballot in accordance with rule 79 of these rules and any member may arrange to attend or to be represented by a scrutineer to scrutinise the returning officer's activities. The returning officer shall conduct the plebiscite promptly.
- (h) The Federal President or Branch President as appropriate, shall submit the report of the Returning Officer to the Board or the Branch Council.
- (i) Any decision of the members voting in plebiscite shall be final and binding on the section unless overturned by a subsequent plebiscite or by a decision of Federal Council or, once a period of 25 years has elapsed, a decision by the section committee.

SECTION 5 - FEDERAL ORGANISATION

40 - CONSTITUTION OF FEDERAL COUNCIL

- (a) Subject to these rules, the supreme governing body of the Association shall be the Federal Council.
- (b) The Federal Council shall consist of:
 - (i) All members of the Board in accordance with rule 52
 - (ii) Delegates from the sections as determined by rule 80
 - (iii) Delegates from Branches as determined by sub-rule (c) of this rule
- (c) Provided that, where Federal Council has approved a Branch to operate in any state, the delegates shall be:

In the case of NSW and Victoria, the Branch Officers.

In the case of any other Branch with officers determined by Rule 19(c)(1), the Branch President and, if applicable, the Branch Secretary.

In the case of any Branch with officers determined by Rule 19(c)(2), the Branch Officers.

- (cc) In any state where the Federal Council has not approved a Branch to operate, there shall be one delegate.
- (d) No member shall hold two positions on Federal Council.
- (e) Each member of Federal Council shall exercise a single vote.
- (f) No proceeding of the Federal Council shall be affected by or rendered void by reason only that one or more casual vacancies in the respective offices of those bodies has or have occurred and has or have not been filled.
- (g) Where a member of Federal Council is unable to attend a meeting of Federal Council, a financial member may be appointed as an alternative member of Federal Council to attend Federal Council in his or her place. A person so appointed shall exercise all the powers and duties of the person whom they are replacing. The appointment may be revoked at any time. The appointment shall be made by:
 - (i) the relevant Branch Council in the case of a branch representative
 - (ii) the relevant National Section Committee in the case of a sectional delegate
 - (iii) the Board in the case of a federal officer.
- (h) Any member of Federal Council may appoint another member of Federal Council as a proxy for the first member where that member is unable to attend all or part of the Council meeting and

Page 28 of 65 Pages

41 - POWERS AND DUTIES OF THE FEDERAL COUNCIL

where no alternate member of Federal Council has been appointed in place of the first member. The appointment shall be with the leave of the Council. A person so appointed shall exercise their own vote and that of the person who has appointed them as a proxy. The appointment as a proxy may be revoked at any time.

41 - POWERS AND DUTIES OF THE FEDERAL COUNCIL

The Federal Council shall have the general conduct and control of the business of the Association, and in that regard shall have complete authority to take any action it considers necessary or desirable on policy, management or any matter concerning the Association and/or its members, and without limiting the foregoing, such powers shall include:-

- (a) The overall management of the affairs of the Association whilst recognising that day to day management shall be in the hands of the Board and administered by the Board through the Chief Executive:
- (b) The determination, enforcement and protection of the policy of the Association in relation to the industrial and/or professional welfare of members, or any other matter of concern to the Association;
- (c) The amendment, rescission or alteration of the rules of the Association;
- (d) The enforcement of the rules of the Association;
- (e) Any action it considers necessary or advisable concerning any industrial claim or actual, threatened, impending or probable industrial dispute or in settlement of any industrial claim or dispute, and to authorise the Chief Executive to serve logs of claims on such general classes or groups of employers as it may determine from time to time. Such logs of claims may take such form as the Chief Executive shall determine unless specified otherwise by Federal Council.
- (f) The determination of the rate of entrance fees, payments and contributions to be paid by members of the Association.
- (g) The determination of the proportions of Association funds to be allocated to Branch funds.
- (h) The imposition and enforcement of the payment of levies on all or a portion of members provided that where a levy is imposed on a section of the membership, it shall be used for the benefit of that section.
- (i) The creation, re-formation or abolition of any branch or section, including the power to direct a branch to establish and organise a particular section or sections, and, subject to these rules, the determination of its authority, territory and membership provided that no branch shall be abolished or have its territory reduced without consultation.
- (j) In accordance with these Rules, the delegation of its authority, except the power to delegate, to the Board, and subject to the control of the Board, the Chief Executive. Such delegations shall continue in force unless and until subsequently rescinded or varied by Federal Council.
- (k) The determination of the wages and conditions of employment of officers and employees, and of any honoraria or similar payment and the discipline and dismissal of officers of the Association;
- (l) The accumulation, investment, custody and disposition of the property and funds of the Association, including the power to enter into any arrangements to secure mortgages or similar arrangements;

Page 29 of 65 Pages

42 - ORDINARY MEETINGS OF FEDERAL COUNCIL

- (m) To require financial reports from branches and sections, and to demand or cause to be made an audit of the books and accounts of any branch or division, and for that purpose take possession of all property, books bank books, documents and correspondence from any branch or office thereof.
- (n) The calling of any meeting of the Board, any Branch Council, Sectional Committee or Section or, sub-branch or of any members or category or group of members of the Association.
- (o) Hearing and determining appeals from any member or group of members aggrieved by a decision of a Branch Council including any decision dealing with the removal of an officer of the Branch Executive.
- (p) To submit any matter to a plebiscite of members or the members of a section.

The Federal Council shall endeavour to ensure that throughout Australia, as far as practicable, a uniform level of service to the members is provided, having regard to the nature and size of the membership of particular branches and sections and any special needs of the membership.

The Federal Council shall decide all matters in accordance with these Rules and have power to decide any questions or matter not provided for by these Rules. A decision of Federal Council shall be final and binding throughout the Association and shall remain in force until superseded, amended or rescinded either at a subsequent meeting of Federal Council or by decision reached by plebiscite.

42 - ORDINARY MEETINGS OF FEDERAL COUNCIL

- (a) A face to face meeting of the Federal Council shall be held at least every two years.
- (b) Business may be placed on the agenda paper for Federal Council by:
 - (i) any Branch Council;
 - (ii) any sectional committee;
 - (iii) any officer or Federal Councillor.

Such items shall be circulated in accordance with (d) hereof.

- (c) Federal Council shall be held in the month of November unless the Board decides on or before June 30 in each year to fix an alternative date and time for the opening of the meeting.
- (cc) The Chief Executive shall notify all Federal Councillors and Branches of the date and time of Federal Council and invite agenda items for the business paper.
- (d) Each Federal Councillor shall notify the Chief Executive of all business he or she desires to place on the agenda paper for the Federal Council meeting at least six weeks prior to the date of such meeting. The Chief Executive shall forward to each Branch Secretary or Regional Director and all Federal Councillors, a copy of the agenda paper at least 28 days prior to such annual meeting of the Federal Council.
- (e) A member of Federal Council may place before a meeting of Federal Council any item not on the agenda paper of the Federal Council if two-thirds of members of Council agree.
- (f) A quorum at any Federal Council meeting shall consist of at least one representative from each of at least three branches and 50% of the Council members.

Page 30 of 65 Pages

43 - ORDER OF BUSINESS AT FEDERAL COUNCIL MEETINGS

- (a) On assembling of the Federal Council, the Federal President shall take the chair. In the absence of the Federal President the Senior Deputy Federal President shall take the chair. In the absence of these officers the members assembled shall vote one of their own members to act as Chair for the time being.
- (b) The Federal President shall cause to be read or table the credentials of the various delegates.
- (c) Unless Federal Council decides otherwise the order of business thereafter shall be as follows:-
 - (i) Appointment of Minutes Secretary,
 - (ii) Confirmation of Minutes of previous Federal Council Meeting and all ensuing meetings of the Board,
 - (iii) Acceptance of urgent business,
 - (iv) Sessions of Federal Council,
 - (v) Federal Presidents address,
 - (vi) Annual Report, Balance Sheet and Statement of Accounts,
 - (vii) Sectional agenda items,
 - (viii) General Business,

44 - EXTRAORDINARY MEETINGS OF FEDERAL COUNCIL

- (a) An Extraordinary Meeting of the Federal Council shall be convened by the Federal President upon the request of:
 - (i) the Board;
 - (ii) Two or more branch councils of branches representing not less than a majority of the members of the Association;
 - (iii) A majority of Branch Councils; or,
 - (iv) By a request of the delegates from a section supported by a petition of 33% of the members of the section.
- (b) Extraordinary meetings shall be convened within twenty-eight days of the receipt by the Federal President of any such request, unless the Board determines otherwise.
- (c) A branch or section making a request for an Extraordinary Federal Council Meeting pursuant to this Rule shall notify the Federal President in writing incorporating in such notification the business which it wishes discussed, giving reasons in support of its request. Provided that a request made by two or more branches collectively within a period of fourteen days of each other pursuant to clause (b) hereof, it shall be considered a valid request for the purpose of this Rule, if business submitted by a branch bears a reasonable resemblance to business submitted by any other branch making such request and such requests must quote the Rule under which the request is made.

Page 31 of 65 Pages

(d) The Federal President shall cause to be provided to all Federal Councillors, agenda items submitted by branches for any such Extraordinary Meeting as soon as is practicable prior to such meeting.

45 - MEETINGS AND/OR DECISIONS OF FEDERAL COUNCIL MAY BE CONDUCTED/TAKEN BY FACSIMILE, TELEPHONIC VOTES ETC

The Board shall determine the form of an extraordinary meeting of Federal Council. This may include by face to face, post, facsimile or electronic conference facilities or similar methods.

46 - CONTROL OF FEDERAL COUNCIL BY MEMBERS

(a)	All decisions of the Federal Council shall be subject to review by the members voting in a
	plebiscite.

(ł	o)	A plebiscite may	be requested	to review a	a decision of	of the Federal	Council v	where rea	uested by	

- (i) the Board, or
- (ii) Two or more Branch Councils of branches representing not less than a majority of the members of the Association, or
- (iii) A majority of Branch Councils or,
- (iv) The delegates from a section supported by a petition of 33% of the members of the section, or
- (v) A petition of financial members signed by not less than 5% of financial members.
- (c) A request for a plebiscite must be made within eight weeks of the decision of Federal Council sought to be reviewed.
- (d) Where a valid request for a plebiscite is made, the Board shall appoint a returning officer who shall:-
 - (i) Take all such steps and have all necessary authority to conduct such plebiscite;
 - (ii) Set out the question to appear on the ballot paper,
 - (iii) Fix a date and time for the issue of ballot papers by the returning officer and also a date and time for the closing of the plebiscite,
 - (iv) Ensure that a full and fair explanation as to the reason for the plebiscite, and the competing views as to whether members should vote for or against it, accompanies the ballot paper.
- (e) A ballot paper issued in relation to this rule, shall be in the following form:-

"Are you in favour of the following......".

Then follows the resolution of Federal Council on which the Plebiscite is being taken.

YES() NO()

(f) The returning officer shall conduct such ballot in accordance with rule 79 of these rules and any member may attend to scrutinise the returning officer's activities. The returning officer shall conduct the plebiscite promptly.

Page 32 of 65 Pages

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (g) The Federal President shall submit the report of the Returning Officer to the next meeting of the Board and shall send a copy of it to each Federal Councillor.
- (h) Any decision of the members voting in plebiscite shall be final and binding on the union and its members unless overturned by a subsequent plebiscite or, once a period of 5 years has elapsed, by a decision of the Federal Council.

47 - FEDERAL OFFICERS

The Federal Officers of the Association shall be the Federal President, Four Federal Section Presidents, Federal Vice-Presidents, and as determined by Federal Council.

48 - FEDERAL PRESIDENT

- (a) The Federal President shall preside at all meetings of the Federal Council, the Board and preserve order so that business may be conducted in due form and with propriety.
- (b) The Federal President shall at all times be under the control of the Federal Council and the Board.
- (c) The Federal President shall have the right to move motions, to vote and speak on Federal Council and on the Board and when speaking on a motion before the meeting shall vacate the chair and allow the senior Federal Section President to temporarily assume the chair.
- (d) The Federal President shall have the right to attend and speak at any meeting of the Association.
- (e) The Federal President shall observe and cause to be observed all the rules, policies and decisions of the Association.

49 - FEDERAL SECTION PRESIDENTS AND FEDERAL VICE-PRESIDENTS

- (a) The duties of the Federal Section Presidents and Federal Vice-Presidents shall be to assist the Federal President at all meetings of the Federal Council and, in the absence of the Federal President, a Federal Section President or Vice-President shall take the chair, conduct the business and perform all the duties of the Federal President.
- (b) Where a Federal Section President is to carry out a function or exercise a power under these rules and more than one Federal Section President is available to do so, the most senior shall do so seniority shall be determined by the number of votes which the Federal Section President received at the preceding election or where this method of establishing seniority cannot be achieved seniority shall be determined by lot.
- (c) Where no Federal Section President is available, and a Vice-President is to carry out a function or exercise a power under these rules and more than one Vice President is available to do so, the most senior shall do so seniority shall be determined by the number of votes which the Vice President received at the preceding election or where this method of establishing seniority cannot be achieved seniority shall be determined by lot.

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (a) The Board will appoint a Chief Executive. The Chief Executive will be employed pursuant to a contract of employment, the conditions and remuneration of which shall be determined by the Board.
- (b) The Chief Executive shall at all times be under the control of the Federal Council and the Board.

Page 33 of 65 Pages

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (c) The Chief Executive shall be appointed to administer the Association's affairs.
- (d) The Chief Executive shall observe and cause to be observed all the rules, policies and decisions of the Association.
- (e) The Chief Executive shall not have the right to vote at any meeting of the Federal Council or the Board.
- (f) The Chief Executive shall exercise the powers set out in this rule in accordance with the directions and/or delegations given by the Federal Council or the Board or shall so exercise them subject to subsequent ratification by the Board at its next meeting. Provided that in the absence of any determination by the Board to the contrary, the exercise of these powers shall be taken to be at the direction of the Board.
- (g) The Chief Executive shall have the power to serve logs of claim, to execute Industrial Agreements and Awards and rescissions or variations thereof by or on behalf of the Association, and at his or her discretion, lodge objections with the relevant Industrial Authority (including the General Manager of the Fair Work Commission) which he or she believes necessary to protect the interests of the Association.
- (h) The Chief Executive shall have the power to make all necessary decisions on the management and activities of the Association between meetings of the Board either in consultation with the Federal President or subject to ratification by the Board at its next meeting. Any such decisions shall be consistent with the decisions of Federal Council and the Board and the objects of the Association.
- (i) The Chief Executive shall have power to convene General Meetings of members in any branch or division or of members of the Branch Council in the event of a Branch Secretary's or Regional Director's refusal or neglect to do so. The Chief Executive shall have the power to convene meetings of the Federal Council or may perform any such duties that may be considered by the Board necessary or desirable in the interests of the Association.
- (j) If the Chief Executive has reason to believe the action of any Branch Secretary, Regional Director or Branch Council is contrary to the Rules, Awards and stated policies of the Association, he or she shall, in consultation with the Federal President have power to nullify same, providing the position of the Branch Secretary or Regional Director or Branch Council and also of the Chief Executive shall, within seven days, be submitted in writing to the Board who shall decide the matter. While the matter is under submission to the Board, the practice objected to shall discontinue.
- (k) The Chief Executive may be a member of any Committee formed by the Federal Council or the Board to advise the Association on any subject, and shall have the right to attend and speak, but not exercise a vote, at any Branch Council, Section Committee or general or special meeting of any branch or section.
- (l) The Chief Executive shall not pay, lend or otherwise appropriate any of the funds of the Association for any purpose except in accordance with these Rules, resolutions and minutes of the Federal Council and the Board.
- (m) The Chief Executive shall be responsible for the employment and supervision of all staff of the Association.
- (n) The duties of the Chief Executive shall be, inter alia:-
 - (i) To attend all meetings of the Federal Council and the Board and cause to be taken minutes of such meetings and to circulate copies of the minutes to all members of the Federal Council or the Board as the case may be as soon as possible and in any event no later than fourteen days after the conclusion of the meeting.

Page 34 of 65 Pages

50 - POWERS AND DUTIES OF CHIEF EXECUTIVE

- (ii) To act generally according to the direction of the Federal Council and the Board and to this end to delegate duties to senior employees and supervise and manage the work of senior employees and the industrial and office staff.
- (iii) To delegate any of these powers and duties, other than this power of delegation, to any senior employee.
- (iv) To summon members of the Federal Council and the Board to meetings.
- (v) To keep a correct account of all monies received and expended together with dates of receipts and expenditure.
- (vi) To pay all monies received by him or her into the Association's bank account to the credit of the Association as soon as possible but no later than within fourteen days.
- (vii) To produce books of accounts at all reasonable times when required by the Federal President, Federal Council or the Board .
- (viii) To submit books, accounts and receipts annually or as often as may be required or directed by the Federal Council or the Board, to the Auditor.
- (ix) To sit, if required, with the Auditor when he or she is auditing the Association's accounts.
- (x) To prepare the Annual Report and assist in the preparation of the Annual Financial Report for submission.
- (xi) To attend promptly to, keep and produce copies of all correspondence and provide details thereof reasonably required.
- (xii) To be responsible for the drafting, serving, filing and lodging of all Federal Industrial Logs of Claims and Award variations.
- (xiii) To cause to be kept and maintained a national register of members showing the name and postal address of each member and a list of names, postal addresses and occupations of all officers of the Association and each branch.
- (xiv) To visit each branch of the Association where practicable.
- (xv) To forward to the General Manager of the Fair Work Commission, a copy of the financial reports and returns in accordance with the Fair Work (Registered Organisations) Act 2009 and Regulations, as amended from time to time.
- (xvi) To notify each member of the Federal Council of the time and place of the Biennial Meeting of the Federal Council at least six weeks before the date thereof and send to each member of the Federal Council, as early as practicable and not later than twenty eight days prior to the Biennial Meeting of the Federal Council, an agenda of the business to come before such meeting.
- (xvii) To exercise overall editorial control and policy of the publications of the Association.
- (xviii) To forward each year to the General Manager of the Fair Work Commission, such returns as required by him or her.
- (xix) To forward within thirty days of notification of any change taking place in the Officers of the Association, a statement to the General Manager of the Fair Work Commission of such change.

Page 35 of 65 Pages

52 - BOARD - POWERS AND DUTIES

- (xx) To forward to the General Manager of the Fair Work Commission within thirty-five days after any alteration has been made in the Rules of the Association, a notice and copy of any rule alterations made and certified by the Federal President.
- (xxi) To supervise and co-ordinate the industrial organisation of members in the callings for which the Association is constituted throughout Australia.
- (xxii) Subject to the Act and in accordance with any directions of the Federal Council or Board, to do all things necessary to be done by an organisation registered under the Fair Work (Registered Organisations) Act 2009.
- (xxiii) To organise and establish branches when instructed to do so by the Board or Federal Council.
- (xxiv) To make careful inquiries in any branch deemed by him to be mismanaged and report the result of such inquiries to the Board who shall be empowered to instruct him/her, if necessary, to take over the affairs of such branch until control of such branch is determined under Section 9 of these Rules.
- (xxv) To dispatch a copy of the Statement of Accounts and Balance Sheet of each branch to each other branch.
- (xxvi) To use his or her best endeavours to keep branches informed of all matters relevant and of interest to the Branch.
- (xxvii) To prepare a report for submission to the Board and Federal Council on the finances and funds of the Association.
- (xxviii) To take all steps necessary to ensure that elections are held for both branch and Federal Offices in accordance with these Rules.
- (xxix) To submit matters for determination to Federal Council and the Board when properly requested to do so under these Rules, or when necessary for the good management or pursuit of the objectives of the Association.
- (xxx) Any duties which may be delegated by the Federal Council or Board under these rules from time to time.

51 - DELETED

52 - BOARD - POWERS AND DUTIES

The Board shall be the authority to

- (a) administer and manage the affairs of the Association when the Federal Council is not in session.
- (b) appoint a Chief Executive and, in consultation with the relevant Branch Council, appoint Regional Directors.
- (c) make, amend and rescind administrative decisions concerning the exercise of the functions by the Association's Chief Executive and senior employees of the Association.
- (d) The Board shall wherever possible, consult branches and sections before initiating or determining any question involving policy. The Board may exercise all of the powers of the Federal Council except the power to:

Add to, amend or rescind the Rules of the Association; or (i)

- (ii) Act contrary to or alter or revoke any decision of Federal Council unless authorised to do so by a decision of a membership plebiscite.
- (e) All decisions of the Board shall be binding throughout the Association and shall remain in force unless superseded, amended or rescinded by Federal Council or by a plebiscite of members or by a subsequent meeting of the Board.
- (f) The Board shall consist of:
 - (i) All federal officers under Rule 47:
 - (ii) One financial member elected by and from each Branch with more than 900 financial members as at June 30 immediately prior to the biennial elections; and
 - (iii) One financial member elected by and from all other Branches.
- (g) Each member of the Board shall have the right to move and second motions, and speak and cast a single vote on any motion. Decisions shall be by the majority of votes cast.
- (h) The Federal President or, in his or her absence, a Federal Section President shall chair meetings of the Board.
- (i) Where a member of the Board is unable to attend all or part of any meeting of the Board, the Board may appoint a financial member as an alternative to attend the Board in his or her place. A person so appointed shall be a person eligible under these rules to stand for the position held by the person they are replacing. He or she shall exercise all the powers and duties of the person whom they are replacing. The appointment may be revoked at any time.
- (j) Any member of the Board may appoint another member of the Board as a proxy for the first member where that member is unable to attend all or part of the Board meeting and where no alternate member of the Board has been appointed in place of the first member. The appointment shall be with the leave of the Board. A person so appointed shall exercise their own vote and that of the person who has appointed them as a proxy. The appointment as a proxy may be revoked at any time.

53 - MEETINGS OF THE BOARD

- (a) The Board shall meet at least six times in each year unless otherwise decided by Federal Council. Meetings of the Board shall be convened by the Federal President.
- (b) A Meeting of the Board shall be convened by the Federal President upon the request of three or more Branch Councils or two or more Section Councils. Such Meetings shall be convened within twenty-eight days of the receipt of such requests by the Federal President.
- (c) The Federal President shall cause to be provided to all Board members agenda items for any meeting as soon as is practicable prior to the meeting.
- (d) A quorum for Board meetings shall be half the members.
- (e) All meetings of the Board shall be called upon such notice of the date and place of the meeting as is reasonable in the circumstances.
- (f) All meetings of the Board shall be notified in advance to all members of the Board by the Federal President by notice including proposed agenda items for such meetings in order to allow members of the Board, branches and sections to submit further agenda items for the consideration of the Board.

Page 38 of 65 Pages

- (g) The Board may decide to consider such additional agenda items as it thinks fit.
- (h) Meetings of the Board may be held and decisions may be taken by means of post or facsimile or email or by the use of telephone or electronic conferencing or other facilities.

54 - DELETED

55 - NATIONAL GENERAL MEETINGS

- (a) A national general meeting which all members of the Alliance are entitled to attend may be convened by:
 - (i) Resolution of Federal Council
 - (ii) A request in writing signed by not less than five percent of the financial members of the Alliance.
- (b) A national general meeting shall be called by the Federal President by notice giving at least 14 days' notice either by:
 - (i) providing a notice to each financial member to his or her last known address;
 - (ii) forwarding a notice to all places of work where more than three members are employed and to theatrical and employment agents; or
 - (iii) placing a notice on the Alliance web page and sending an email notification to the last known email address of each financial member
- (c) The notice calling the meeting shall set out the place(s), date(s) and time(s) of the meeting and the nature of the business to be brought before the meeting.
- (d) The Board may determine that the meeting should be held as a series of gatherings in different cities at different times to consider a common resolution.
- (e) The quorum necessary to transact business at a national general meeting shall be at least 5 per cent of the financial membership of the Alliance.
- (f) A national general meeting shall be called not later than 28 days after the receipt by the Federal President of a request in writing signed by not less than 5% of the financial members of the Alliance.
- (g) A national general meeting shall not be convened in accordance with sub-rule (f) hereof for the purpose of reviewing any action or resolution of the Alliance unless such request is made within eight weeks of the action or resolution which it is proposed to review.
- (h) A national general meeting shall have the power to require the Board or Federal Council to deal with a matter. The relevant body shall deal with the matter promptly.

Page 39 of 65 Pages

56 - NATIONAL GENERAL MEETING

- (a) A national general meeting which all members of the Alliance are entitled to attend may be convened by resolution of Federal Council or by a request in writing signed by not less than 5% of the members of the Alliance, for the purpose of considering the auditors report, the general purpose financial report and the operating report of the Alliance within 7 months after the end of the financial year.
- (b) A national general meeting shall be called by the Federal Secretary by notice giving at least 14 days' notice either by:
 - (i) posting a notice to each member to his or her last known address;
 - (ii) placing a notice in daily newspaper(s) circulating in the area(s) in which the meeting is to be held and by forwarding a notice to all places of work where more than three members are employed and to theatrical and employment agents; or
 - (iii) placing a notice on the Alliance web page and sending an email notification to the last known email address of each member
- (c) The notice calling the meeting shall set out the place(s), date(s) and time(s) of the meeting and the nature of the business to be brought before the meeting.
- (d) The Federal Management Committee may determine that the meeting should be held as a series of gatherings in different cities at different times to consider a common resolution.
- (e) The quorum necessary to transact business at a national general meeting shall be at least 5 per cent of the membership of the Alliance.
- (f) A national general meeting shall be called not later than 28 days after the receipt by the federal secretary of a request in writing signed by not less than 5% of the members of the Alliance.

SECTION 6 - INDUSTRIAL MATTERS

57 - INDUSTRIAL DISPUTES

- (a) Federal Council, the Board or the Federal President or the Chief Executive is empowered to take any action considered necessary or desirable in connection with any industrial dispute or probable industrial dispute.
- (b) The Board or the Federal President or the Chief Executive shall have authority to enter into an industrial agreement or award, on behalf of the Association.
- (c) An industrial dispute may only be submitted
 - (i) To any federal court or tribunal on the authority of the Federal President or the Chief Executive;
 - (ii) To a State industrial court or commission on the authority of the Federal President, the Chief Executive, Branch Secretary or Regional Director.

58 - PROSECUTIONS ON BEHALF OF THE ASSOCIATION

- (a) The Federal President shall be:
 - (i) the registered Officer of the Association for the purposes of the industrial legislation.

59 - AGREEMENTS WITH STATE UNIONS

- (ii) empowered to act on behalf of the Association.
- (iii) the Officer to sue and be sued on behalf of the Association.
- (iv) empowered on behalf of the Association to lay any information under any Act of Parliament under which proceedings can or may be instituted on behalf of the Association for any offence or any recovery proceedings for an unpaid wages, superannuation contribution and/or other similar benefit.
- (b) In each state, the Branch President or the Branch Secretary or Regional Director of the relevant branch shall also have power in respect of any matter arising within the state to lay any information or take proceedings to recover any penalty under any State Act of Parliament by the provisions of which the Association or any authorised person may take proceedings.
- (c) In any proceedings or matter to which it is necessary that some other person shall exercise the power to sue on behalf of the Association, such person shall be deemed to be so authorised on production of a letter to that effect bearing the Seal of the Association signed by the Federal President or duly authorised Board Member.

59 - AGREEMENTS WITH STATE UNIONS

The Federal Council and the Board are authorised to enter into (and terminate) an agreement with a State registered union regarding coverage and representation of members.

Page 41 of 65 Pages

SECTION 7 - ADMINISTRATION

60 - SEAL AND EXECUTION OF DOCUMENTS

The Seal of the Association shall be kept by the Association. The affixture of the seal to any documents shall be attested to under the hand of the Federal President or duly authorised Board member.

61 - AUDITOR

- (a) A properly qualified Auditor (or auditors) not an Association member, shall audit the accounts of the Association yearly.
- (b) The Auditor(s) shall be appointed by the Board.
- (c) The Auditor shall have the power to call for all books, papers, vouchers and documents belonging to the Association. He or she shall furnish the report upon the books, Balance Sheets and accounts verifying correctness or otherwise.

62 - FINANCIAL YEAR

The Financial Year of federal and branch offices shall terminate on the thirtieth day of June in each year and all books and accounts shall close on that date. A duly audited Balance Sheet of the Association shall be caused to be presented to Federal Council by the Federal President. The Balance Sheet shall show all items of receipts and expenditure and the assets and liabilities, of the Association.

63 - FINANCIAL MANAGEMENT

- (a) Unless otherwise determined by Federal Council all assets and liabilities shall be vested in the Federal Council and administered between meetings by the Board.
- (b) The Board shall adopt a budget at the beginning of each financial year setting out the budgeted income and expenditure for the year.
- (c) The Federal President shall ensure the Board is advised on progress in meeting the Association's budget and any significant deviations from the budget. The Board may approve variations to the budget.
- (d) Monies of the Alliance shall be banked in the name of the Media, Entertainment & Arts Alliance.
- (e) Any payments of monies shall be authorised by the Federal President or such other people who may be authorized by the Board from time to time.
- (f) Expenditure shall only be approved as is in accordance with the objects of the Alliance.
- (g) The Alliance may invest the monies of the Alliance in
 - (i) real estate or other property
 - (ii) shares or other securities
 - (iii) bank accounts or other cash instruments
 - (iv) such other investment as the Alliance may deem appropriate
- (h) Where assets are held in the name of officers or other members, these officers or members shall be required to execute a deed of trust that they are merely trustees for the Alliance.

Loans, Grants and Donations

- (i) A loan, grant or donation of an amount exceeding \$1,000 shall not be made by the Association or any branch thereof as the case may be unless the Board or Council of the branch concerned, as the case may be, has satisfied itself -
 - (i) that the making of the loan, grant or donation would be in accordance with the other rules and policy of the Association; and
 - (ii) in relation to a loan that, in the circumstances, the security proposed to be given for the repayment of the loan is adequate and the proposed arrangements for the repayment of the loan are satisfactory; and,

it has approved the making of the loan, grant or donation.

Moneys held on trust

- (j) The Association may receive and hold moneys on trust, including moneys held on trust for members or people eligible to be members.
- (k) Moneys held on trust shall be banked in an account or accounts specifically designated for that purpose.
- (1) The Association shall:
 - (i) take all reasonable efforts to distribute moneys held on trust to financial members entitled to the money:
 - (ii) deduct any amount owing by a member to the Association from any amount received by the Association on behalf of that member and take all reasonable efforts to distribute the balance, if any, to the member;
 - (iii) deduct an administrative charge, determined from time to time as appropriate by Federal Council, or by the Board from any amount received by the Association on behalf
 - of any person who is neither a financial member or a non-financial member of the Association and take all reasonable efforts to distribute the balance to that person;
 - (iv) the Association shall not be required to distribute amounts of less than \$50 or such other amount as determined by Federal Council;
 - (v) the Association shall accept no liability for tax or superannuation levy or any other liability arising out of the payment;
 - (vi) any amounts not able to be distributed within six years of being received by the Association may be applied by the Association for the interests of the general class of people for whom the money was received, provided that if, after six years, any member can assert a right to any money received, the Association shall make good that money; and
 - (vii) unless provided otherwise by the terms of the trust, the Association may apply any net interest or related earnings for the interests of the general class of people for whom the money was received.

Public Funds

- (m) The Association may establish and maintain an Alliance Gift Fund as a public fund.
 - (i) Donations will be deposited into the public fund listed on the Register of Cultural Organisations. These monies will be kept separate from other funds of the Association and will only be used to further the objects of the Association. Investment of monies in this fund will be made in accordance with guidelines for public funds as specified by the Australian Taxation Office.
 - (ii) The fund will be administered by a management committee or a subcommittee of the management committee, the majority of whom, because of their tenure of some public office or their professional standing, have an underlying community responsibility, as distinct from obligations solely in regard to the cultural objectives of the Association.
 - (iii) No monies/assets in this fund will be distributed to members or office bearers of the Association, except as reimbursement of out-of-pocket expenses incurred on behalf of the fund or proper remuneration for administrative services.
 - (iv) The Department responsible for the administration of the Register of Cultural Organisations will be notified of any proposed amendments or alterations to provisions for the public fund, to assess the effect of any amendments on the public fund's continuing Deductible Gift Recipient status.
 - (v) Receipts for gifts to the public fund must state:
 - the name of the public fund and that the receipt is for a gift made to the public fund:
 - the Australian Business Number of the company;
 - the fact that the receipt is for a gift; and
 - any other matter required to be included on the receipt pursuant to the requirements of the Income Tax Assessment Act 1997.
 - (vi) Winding-up clause
 - If upon the winding-up or dissolution of the public fund listed on the Register of Cultural Organisations, there remains after satisfaction of all its debts and liabilities, any property or funds, the property or funds shall not be paid to or distributed among its members, but shall be given or transferred to some other fund, authority or institution having objects similar to the objects of this public fund, and whose rules shall prohibit the distribution of its or their income among its or their members, such fund, authority or institution to be eligible for tax deductibility of donations under Subdivision 30-B, section 30-100, of the Income Tax Assessment Act 1997 and listed on the Register of Cultural Organisations maintained under the Act.
- (n) The Association may establish and maintain an overseas aid fund, known as the Media Safety and Solidarity Fund, as a public fund.
 - (i) Donations will be deposited into the public fund as gazette by the Australian Taxation Office. These monies will be kept separate from other funds of the Association and will only be used to further the objects of the Association. Investment of monies in this fund will be made in accordance with guidelines for public funds as specified by the Australian Taxation Office.
 - (ii) The fund will be administered by a management committee or a subcommittee of the management committee, the majority of whom, because of their tenure of some public office or their professional standing, have an underlying community responsibility, as distinct from obligations solely in regard to the cultural objectives of the Association.

- (iii) No monies/assets in this fund will be distributed to members or office bearers of the Association, except as reimbursement of out-of-pocket expenses incurred on behalf of the fund or proper remuneration for administrative services.
- (iv) The Australian Taxation Office will be notified of any proposed amendments or alterations to provisions for the public fund, to assess the effect of any amendments on the public fund's continuing Deductible Gift Recipient status.
- (v) Receipts for gifts to the public fund must state:
 - the name of the public fund and that the receipt is for a gift made to the public fund;
 - the Australian Business Number of the company;
 - the fact that the receipt is for a gift; and
 - any other matter required to be included on the receipt pursuant to the requirements of the Income Tax Assessment Act 1997.

(vi) Winding-up clause

If upon the winding-up or dissolution of the public fund gazette by the Australian Taxation Office, there remains after satisfaction of all its debts and liabilities, any property or funds, the property or funds shall not be paid to or distributed among its members, but shall be given or transferred to some other fund, authority or institution having objects similar to the objects of this public fund, and whose rules shall prohibit the distribution of its or their income among its or their members, such fund, authority or institution to be eligible for tax deductibility of donations under Subdivision 30-B, section 30-100, of the Income Tax Assessment Act 1997 and gazette by the Australian Taxation Office.

- (o) The Association may establish and maintain an Alliance Necessitous Circumstances Fund as public fund.
 - (i) Donations will be deposited into the public fund as gazette by the Australian Taxation Office. These monies will be kept separate from other funds of the Association and will only be used to further the objects of the Association. Investment of monies in this fund will be made in accordance with guidelines for public funds as specified by the Australian Taxation Office.
 - (ii) The fund will be administered by a management committee or a subcommittee of the management committee, the majority of whom, because of their tenure of some public office or their professional standing, have an underlying community responsibility, as distinct from obligations solely in regard to the cultural objectives of the Association.
 - (iii) No monies/assets in this fund will be distributed to members or office bearers of the Association, except as reimbursement of out-of-pocket expenses incurred on behalf of the fund or proper remuneration for administrative services.
 - (iv) The Australian Taxation Office will be notified of any proposed amendments or alterations to provisions for the public fund, to assess the effect of any amendments on the public fund's continuing Deductible Gift Recipient status.
 - (v) Receipts for gifts to the public fund must state:
 - the name of the public fund and that the receipt is for a gift made to the public fund;
 - the Australian Business Number of the company;
 - the fact that the receipt is for a gift; and
 - any other matter required to be included on the receipt pursuant to the requirements of the Income Tax Assessment Act 1997.
 - (vi) Winding-up clause

If upon the winding-up or dissolution of the public fund gazette by the Australian Taxation Office, there remains after satisfaction of all its debts and liabilities, any property or funds,

the property or funds shall not be paid to or distributed among its members, but shall be given or transferred to some other fund, authority or institution having objects similar to the objects of this public fund, and whose rules shall prohibit the distribution of its or their income among its or their members, such fund, authority or institution to be eligible for tax deductibility of donations under Subdivision 30-B, section 30-100, of the Income Tax Assessment Act 1997 and gazette by the Australian Taxation Office.

63A - DISCLOSURE AND ACCOUNTABILITY

63A(i) - Board Membership and Related Party Payments

Federal

Each officer of the Association shall disclose to the Federal President or in the case of the Federal President, the Board, any remuneration paid to the officer:

- (a) because the officer is a member of a board, if: the officer is a member of the board only because the officer is an officer of the Association; or the officer was nominated for the position as a member of the board by the Association or a peak council; or
- (b) by any related party of the organisation in connection with the performance of the officer's duties as an officer.

Disclosures under this Rule shall be made in writing to the Association and tabled at the relevant Board meetings as soon as practicable after the remuneration is paid to the officer.

Branches

Each officer of a Branch of the Association shall disclose to the Branch Secretary or Regional Director or in the case of the Branch Secretary or Regional Director, the Branch President, any remuneration paid to the officer:

- (c) because the officer is a member of a board, if: the officer is a member of the board only because the officer is an officer of the Branch; or the officer was nominated for the position as a member of the board by the Association, a Branch of the Association or a peak council; or
- (d) by any related party of the organisation in connection with the performance of the officer's duties as an officer.

Disclosures under this Rule shall be made in writing to the Branch and tabled at the relevant committee of management meetings as soon as practicable after the remuneration is paid to the officer.

63A(ii) - Remuneration

Federal/Branches

The Association shall disclose to members and its Branches: the identity of the five highest paid federal officers in terms of relevant remuneration for the disclosure period.

Wherever constituted, Branches shall disclose to members of the relevant Branch: the identity of the five highest paid officers of the branch in terms of relevant remuneration for the disclosure period.

63A - DISCLOSURE AND ACCOUNTABILITY

For Federal Association and Branch officers, the disclosure shall include: (i) the actual amount of the officers' relevant remuneration for the disclosure period; and (ii) the form of the officers' relevant non-cash benefits, for the disclosure period.

Disclosures under this Rule shall be made in writing in relation to each financial year; and within six months after the end of the financial year.

63A(iii) - Disclosure of Material Personal Interests

Federal

Each officer of the Association shall disclose to the Association any material personal interest that relates to the affairs of the Association in a matter that:

- (a) the officer has or acquires; or
- (b) a relative of the officer has or acquires.

Disclosures under this rule shall be made in writing to the Association as soon as practicable after the interest is acquired.

Disclosures under the Rule shall be made in writing to members of the Association in relation to each financial year; and within six months after the end of the financial year.

Branches

Each officer of a Branch of the Association shall disclose to the relevant Branch any material personal interest that relates to the affairs of the Branch in a matter that:

- (a) the officer has or acquires; or
- (b) a relative of the officer has or acquires.

Disclosures to the Branch under this Rule shall be made in writing to the Branch as soon as practicable after the interest in acquired.

Disclosures under this Rule shall be made in writing to members of the Branch in relation to each financial year; and within six months after the end of the financial year.

63A(iv) - Disclosure of Payments to Related Parties and Declared Persons

Federal

The Association shall disclose to members of the Association the total of the payments made by the Association, during the disclosure period:

- i. to each related party of the Association; or
- ii. to each declared person or body of the Association.

Disclosures to members and the Branches under this Rule shall be made in writing in relation to each financial year and within six months after the end of the financial year.

Disclosure is not required for a payment made by the Association to a related party if:

(a) the payment consists of amounts deducted by the Association from remuneration payable to officers or employees of the Association; or

64 - RESTRICTED APPLICATION OF SECTION 8

- (b) the related party is an officer of the Association, and the payment:
 - i. consists of remuneration paid to the officer by the Association; or
 - ii. is reimbursement for expenses reasonably incurred by the officer in performing the officer's duties as an officer.

Branches

A Branch of the Association shall disclose to members of the relevant Branch the total payments made by the Branch, during the disclosure period:

- i. to each related party of the Branch; or
- ii. to each declared person or body of the Branch

Disclosures to members of the Branch under this Rule shall be made in writing in relation to each financial year and within six months after the end of the financial year.

Disclosure is not required for a payment made by a Branch of the Association to a related party if:

- (a) the payment consists of amounts deducted by the Branch from remuneration payable to officers or employees of the Branch; or
- (b) the related party is an officer of the Branch, and the payment:
 - i. consists of remuneration paid to the officer by the Branch; or
 - ii. is reimbursement for expenses reasonably incurred by the officer in performing the officer's duties as an officer.

63A(v) - Expenditure Policies and Procedures

Federal/Branches

The Board shall develop and implement a single set of policies and procedures relating to expenditure. These policies shall apply to the Federal Association and Branches of the Association.

63A(vi) - Financial Management Training

Federal/Branches

Each officer of the Association or a Branch of the Association whose duties include duties that relate to the financial management of the Association or a Branch (as the case may be) must undertake training that is: approved by the General Manager of the Fair Work Commission; and that covers each of the officer's financial duties. Approved training shall be undertaken by all relevant officers within six months of assuming office.

SECTION 8 - JOURNALISTS' CODE OF ETHICS

64 - RESTRICTED APPLICATION OF SECTION 8

(a) This section of the rules shall apply only to members covered by Rule 4 Part C of these rules. For the purposes of this part such members shall be called 'journalists'.

Page 48 of 65 Pages

65 - AUSTRALIAN JOURNALISTS ASSOCIATION CODE OF ETHICS

(b) Any amendment or alteration to this part of the rules shall only be made by Federal Council if it has first been approved by the Media section of the Association in accordance with the procedure specified in Rule 75.

65 - AUSTRALIAN JOURNALISTS ASSOCIATION CODE OF ETHICS

Respect for truth and the public's right to information are fundamental principles of journalism. Journalists describe society to itself. They convey information, ideas and opinions. They search, disclose, record, question, entertain, comment and remember. They inform citizens and animate democracy. They give a practical form to freedom of expression. They scrutinise power, but also exercise it, and should be responsible and accountable.

Journalists commit themselves to:

Honesty, Fairness, Independence and Respect for the rights of others.

Journalists will educate themselves about ethics and apply the following standards:

- 1. Report and interpret honestly, striving for accuracy, fairness and disclosure of all essential facts. Do not suppress relevant available facts, or give distorting emphasis. Do your utmost to give a fair opportunity for reply.
- 2. Do not place unnecessary emphasis on personal characteristics including race, ethnicity, nationality, gender, age, sexual orientation, family relationships, religious belief or physical or intellectual disability.
- 3. Aim to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source. Where confidences are accepted, respect them in all circumstances.
- 4. Do not allow personal interest, or any belief, commitment, payment, gift or benefit to undermine your accuracy, fairness or independence.
- 5. Disclose conflicts of interest that affect, or could be seen to affect, the accuracy, fairness or independence of your journalism. Do not improperly use a journalistic position for personal gain.
- 6. Do not allow advertising or other commercial considerations to undermine accuracy, fairness or independence.
- 7. Do your utmost to ensure disclosure of any direct or indirect payment made for interviews, pictures, information or stories.
- 8. Use fair, responsible and honest means to obtain material. Identify your self and your employer before obtaining any interview for publication or broadcast. Never exploit a person's vulnerability or ignorance of media practice.
- 9. Present pictures and sound which are true and accurate. Any manipulation likely to mislead should be disclosed.
- 10. Do not plagiarise.
- 11. Respect private grief and personal privacy. Journalists have the right to resist compulsion to intrude.
- 12. Do your utmost to achieve fair correction of errors.

Guidance Clause

Basic values often need interpretation, and sometimes come into conflict. Ethical journalism requires conscientious decision-making in context. Only substantial advancement of the public interest or risk of substantial harm to people allows any standard to be overridden.

66 - OFFENCES AND COMPLAINTS AGAINST THE CODE OF ETHICS

- (a) A journalist shall be deemed to have committed an offence against the Code of Ethics if, after procedures as laid down by these rules, he or she has been found guilty of any of the following:
 - (i) Violation of and/or refusal to observe the Code of Ethics of the Association;
 - (ii) Failure to obey a summons to attend a meeting of a Complaints or Appeals Panel and failing to supply the Panel with a reasonable explanation for non-attendance.
- (b) A journalist found guilty of an offence against the Code of Ethics shall be liable to any of the following penalties: warning, reprimand, fine (to a maximum of \$1000), suspension from membership (for up to one year) and expulsion from membership.

67 - ETHICS COMMITTEE

- (a) At its first meeting following the declaration of the biennial elections of the Alliance, the National Media Section Committee shall:
 - (i) Appoint nine financial members of the National Media Section as members of the Ethics Committee.
 - (ii) appoint from the general community an additional four persons to the Ethics Committee; and
 - (iii) appoint from among the persons appointed under subsections (i) and (ii) of this rule a chair and at least one deputy chair.
- (b) The appointments shall be made in a manner determined by the National Media Section Committee.
- (c) Persons appointed shall hold office until the conclusion of the next National Media Section Committee meeting held under Rule 67(a).
- (d) If any person appointed to the Ethics Committee dies, resigns or is removed from office, the National Media Section Committee shall take such steps it considers necessary to fill the vacancy.
- (e) The Ethics Committee shall be empowered to investigate any complaint of violation of and/or refusal to observe the Code of Ethics and to make decisions thereon.
- (f) The Ethics Committee shall keep a written record of all complaints received, a summary of the evidence and also a record of all decisions and recommendations.
- (g) The decisions and recommendations of the Ethics Committee shall be published in accordance with any guidelines which may be issued by the National Media Section Committee.

68 - COMPLAINTS

- (a) Any person may write to the President of the National Media Section alleging that a member of the Alliance employed or engaged in journalism has acted contrary to Rule 65. The complaint must be in writing and set out the allegations fully and clearly. Anonymous or oral complaints shall not be received or progressed. Any complaint must be lodged within six months of the first publication of the material that is the subject of a formal complaint.
- (b) A Complaints Panel shall have the right to refuse to receive, investigate or make a decision upon any complaint which in the opinion of the majority of the Panel members considering a complaint does not come within the provisions of the Code of Ethics or is vexatious, frivolous or trivial. The Panel shall publish reasons for such a refusal.
- (c) The Ethics Committee shall inter alia investigate any report on any matter concerning the Code of Ethics which may be referred to it by the Federal Council, the Board, National or Branch Section Committee or a Branch Council.
- (d) The President of the National Media Section shall refer any written complaint to the Chair of the Ethics Committee as soon as possible.
- (e) The Committee Chair shall within eight days:
 - (i) convene a Complaints Panel consisting of three members of the Ethics Committee. At least one of these three shall not be a member of the Alliance:
 - (ii) advise the complainant that the complaint has been received; and
 - (iii) advise the member complained against of the nature of the complaint
- (f) The Complaints Panel shall consider the complaint and may:
 - (i) dismiss the complaint without further action
 - (ii) attempt to mediate between the complainant and the member complained against.
 - (iii) seek further information from either the complainant and/or the person complained against or from any other person. The Panel may seek this in writing or by statutory declaration.
 - (iv) where a request for further information is made of a complainant, they shall be required to provide a response to this request within 60 days of the date of the request. Where no response is provided, the Panel may exercise its discretion to continue or terminate its consideration of the complaint.
 - (v) have the parties appear personally before the Panel
 - (vi) allow the parties to call witnesses. If witnesses are called, either party may examine or cross-examine the witnesses. They shall also have the right to furnish written statements and the right to a reasonable adjournment of proceedings for these purposes.
- (g) If one of the parties appears personally before the Panel, the other party shall also have the right to appear.
- (h) The formalities associated with legal proceedings shall be followed where necessary to protect the member against whom the complaint has been made, but the Complaints Panel shall not be bound by the formal rules of evidence. The object of any hearing shall be to ascertain the truth and substance of the matter and to this end the rules of natural justice shall be observed, that is to say

- that the complainant and the respondent have a right to put their case to the Panel. The extent of that right is to be determined by the Panel after considering the seriousness of the allegation
- (i) Neither party shall have the right to legal representation at any stage of the process outlined in these Rules.
- (j) Upon completing its investigations, the Complaints Panel shall by majority vote decide whether the complaint should be upheld or dismissed. If it decides that the complaint is upheld, it shall also, by majority vote, decide the penalty to be imposed in accordance with Rule 66.
- (k) The chair of the Ethics Committee shall advise the complainant and the member complained against of the decision of the Complaints Panel within 28 days of the decision. Each party shall be advised of the right to appeal.
- (l) If no appeal is lodged within a further 28 days, the decision shall be confirmed and action required shall be taken.

69 - APPEALS PANEL

- (a) Any party to a matter considered by a Complaints Panel shall have the right to appeal against any decision of the Panel with the exception of a decision to dismiss the complaint.
- (b) The Appeals Panel is restricted to correcting error in the decision of the Complaints Panel.
- (c) The parties to the appeal are entitled to provide further evidence to the Appeals Panel.
- (d) An appeal must be lodged with the President of the National Media Section in writing within 28 days of being notified of the decision being appealed against.
- (e) The President of the National Media Section shall refer any written appeal to the Chair of the Ethics Committee as soon as possible.
- (f) The Committee Chair shall within eight days:
 - (i) convene an Appeals Panel consisting of five members of the Ethics Committee. At least two of these five shall not be a member of the Alliance. No member of the original Complaints Panel shall sit on the Appeals Panel;
 - (ii) advise the appellant that the appeal has been received;
 - (iii) advise the other party of the nature of the appeal; and
 - (iv) provide the Appeals Panel with all material connected with the decision which is subject to appeal.
- (g) The Appeals Panel shall consider the complaint and may:
 - (i) dismiss the appeal
 - (ii) uphold the appeal
 - (iii) vary the original decision of the Complaints Panel
 - (iv) direct that a new Complaints Panel be convened to reconsider the complaint
 - (v) seek further information from either party. The Panel may seek this in writing or by statutory declaration

(vi) have the parties appear personally before the Panel

71 - OFFENCES AND COMPLAINTS

- (vii) allow the parties to call witnesses. If witnesses are called, either party may examine or cross-examine the witnesses. They shall also have the right to furnish written statements and the right to a reasonable adjournment of proceedings for these purposes.
- (h) The processes set out for the Complaints Panel shall apply mutatis mutandis to the Appeals Panel.
- (i) The Chair of the Ethics Committee shall advise the parties of the decision of the Appeals Panel within 28 days of the decision.

70A - NATIONAL STUNT COMMITTEE

- (a) Members who are graded stunt performers, safety supervisors and stunt co-ordinators shall elect a National Stunt Committee of twelve financial members constituted as follows:
 - (i) four members who are graded as safety supervisors from a minimum of three states;
 - (ii) four members who are graded as stunt co-ordinators from a minimum of three states; and
 - (iii) four members who are graded as stunt performers from a minimum of three states.
- (b) Members of the National Stunt Committee shall be elected biennially in accordance with Rule 79, provided that a member may only nominate for election in a single category, notwithstanding that they may be qualified for more than one category.
- (c) Within three months of the Meeting at which the members of a National Stunt Committee are declared elected, the Federal President of the Association's Equity Section shall convene the first meeting of the Committee at which a Chair, a Vice Chair and a Secretary of the Committee shall be appointed by and from the members of the Committee.
- (d) Any member of a National Stunt Committee shall not be absent without reasonable grounds for two consecutive meetings.
- (e) If seven of its members are in attendance to form a quorum a meeting of the National Stunt Committee shall be sufficiently constituted to transact business.
- (f) The National Stunt Committee shall devise and administer the National Stunt Grading Procedure and consider matters affecting safety and related issues in the Film and Television industries.
- (g) Should a member of the National Stunt Committee be an applicant for grading he or she shall disqualify him or herself from all deliberations by the Committee on that complaint, and if the member previously had been chosen as Chair, Vice-Chair or Secretary of the Stunt Committee the remaining members of the Committee shall choose another member from among their number to fill that office for the duration of the hearing.

SECTION 9 - OFFENCES AND BREACHES OF THE RULES

71 - OFFENCES AND COMPLAINTS

- (a) A member or associate member, where relevant, shall be held to have committed an offence if, after procedures as laid down in these Rules, he or she shall have been found guilty of any of the following:-
 - (i) Violation of and/or refusal to observe a lawful decision of the Association or abide by these Rules,

Page 54 of 65 Pages

73 - CHARGES AGAINST MEMBERS

- (ii) Violation of and/or refusal to observe a lawful decision of Federal Council, the Board, National Section Committee, or a Branch Council or Branch Section Committee, attention to which has been drawn in any journal of the Association or in a letter, memorandum or bulletin issued by Federal Council, the Board, National Section Committee, or a Branch Council or Branch Sectional Committee.
- (iii) Violation of and/or refusal to carry out a provision of an Industrial Award determination or agreement applicable to him or her,
- (iv) Disclosing to a person not entitled to know it, any confidential matter of the Association,
- (v) Misappropriating money and/or property belonging to the Association,
- (vi) Knowingly works with a non-unionist without first notifying the workplace representative or in the absence of such a representative, the Secretary or Regional Director of the branch to which he or she belongs,
- (vii) Obstructs or having been requested to assist, fails to assist any officer or duly appointed representative of the Association in the performance of his or her duty,
- (viii) Fails to attend any meetings of the Executive or of a branch to which he or she belongs when requested to do so,
- (ix) Fails to observe By-Laws which may be enforced by the Association from time to time.
- (b) A member or associate member, found guilty of an offence, shall be liable to any of the following penalties namely, warning, rebuke, censure, fine (to a maximum of one thousand dollars), suspension for a period of up to one year or expulsion from the Association.

72 - REMOVAL FROM OFFICE

A person elected to an office in the Association (whether the office be a Federal, Branch, sub-Branch or Sectional office) may be removed from office where the person has been dealt with in the manner set out in this section and found guilty of misappropriation of any of the funds of the Association, a substantial breach of the rules of the Association or gross misbehaviour or gross neglect of duty or has ceased under the rules to be eligible to hold the office.

73 - CHARGES AGAINST MEMBERS

- (a) Any member complaining of a violation or offence under these Rules by any member or associate member, shall submit the complaint in writing to the Chief Executive within seven days of the matter complained of coming to the notice of the member making the complaint, setting out the allegations fully and clearly.
- (b) The Chief Executive shall bring the complaint before the next meeting of the Board which shall fix a date and time for investigation by the Board if it resolves that such complaint is of substance.
- (c) The Chief Executive shall, within three days of such Board meeting, forward by registered or certified mail or personal service to the member or associate member concerned, a copy of all allegations made against her/him and any evidence received in support of them, the charges under the rules and particulars of those charges. It shall also inform her/him of the date, time and place fixed for investigation by the Board of the complaint and of her/his right to appear personally or submit a reply in writing.
- (d) The respondent member or associate member shall have the right to appear personally at the investigation or to submit to the Board in writing, his or her reply to the complaint. If the respondent appears personally at the

Page 55 of 65 Pages

75 - NEW RULES AND ALTERATIONS OF RULES

- investigation, the complainant shall also have the right to appear. Each party shall be permitted to call witnesses. No party shall be entitled to be legally represented.
- (e) A copy of any evidence by Statutory Declaration by one party shall be sent to the other party who shall have the right to submit evidence in reply.
- (f) If either party is not present at the investigation or fails to submit evidence, the Board may nevertheless proceed to consider and decide upon the complaint or if it decides that there is insufficient evidence it may, before reaching a decision, call for further evidence from either party or other persons, to be submitted orally or in writing.
- (g) The formalities associated with legal procedure shall be followed where it is necessary to protect the member against whom the allegations are made. The formal rules of evidence shall not be applied. The object of the investigation shall be to ascertain the truth and substance of the matter and to that end, the rules of natural justice shall be observed.
- (h) The Chief Executive shall ensure the Association maintains a written record of all complaints received and investigated, a precis of the evidence produced or heard and also a record of all decisions of the Board.
- (i) All communications to members or associate members shall be authorised by the Chief Executive upon the directions of the Board and shall be by registered or certified mail or personal service.
- (j) Any member or associate member so charged, shall receive a copy of the determination of the Board in the matter within seven days of each determination.
- (k) Notwithstanding the foregoing, the Board shall have the authority to instruct the Chief Executive to initiate proceedings against any member or associate member.
- (l) Any member or associate member found guilty of an offence under this Rule, shall have the right of appeal to the Federal Council.
- (m) Notice of such appeal must be lodged with the Chief Executive stating the grounds upon which the appeal is based within thirty days of the decision appealed against. Otherwise, the right of appeal shall lapse and the decision shall continue in force.

74 - DELETED

SECTION 10 - RULES

75 - NEW RULES AND ALTERATIONS OF RULES

- (a) Subject to sub-rule (d) hereof, no new rules shall be made nor shall any of the rules of the Association for the time being be altered, added to, amended or rescinded except by the Federal Council. The required majority for amendments to these rules shall be a simple majority of eligibility federal councillors.
- (b) Any proposal to alter, amend, add to or rescind the Rules shall be submitted to the Federal President to enable it to be circulated to all Federal Councillors and Branches by the Chief Executive at least 28 days before the date on which the meeting or the postal ballot of Federal Council to consider the proposal is scheduled to begin.
 - Provided that a proposal to alter, amend, add to or rescind the Rules may be considered and determined by Federal Council without such notice where two-thirds of Federal Councillors agree.
- (c) Any proposal to alter, amend, add to or rescind the rules may be proposed by any Branch Council or Section Committee to Federal Council at any time between meetings of the Federal Council.

Such proposed rules and/or amendments shall be submitted to the Federal President and shall be circulated in accordance with (b) hereof.

(d) No new rule (or amendment, addition or rescission) shall be made which alters any section rights set out in sections 4 & 8 of these rules without the section first approving any such change in accordance with the rules governing those sections.

76 - INTERPRETATION OF RULES

Where a dispute arises about the meaning of any rule, subject to any authoritative interpretation of the rules by a competent court or industrial tribunal, the Federal Council shall be the body to determine the true meaning of that rule.

SECTION 11 - AFFILIATION & REPRESENTATION

77 - AFFILIATION AND REPRESENTATION

- (a) Federal Council, a National or Branch Section Committee, Branch or sub- Branch shall be authorised to affiliate with any industrial organisation or peak body of bona fide trade unions or such other body as is in accordance with the objects of the Association.
- (b) The Board, or any Branch, Division or Section shall not be affiliated with or represented by any organisation cause or movement or at any meeting which is party-political or sectarian in relation to the Media section.
- (c) Federal Council, a National or Branch Section Committee, or Branch shall not affiliate with any industrial organisation or peak body of bona fide trade unions in relation to Journalist members of the Association except where:
 - (i) At the date of amalgamation the Australian Journalists Association was affiliated with the relevant peak body;
 - (ii) the national or branch Media Section Committee (as the case may be) approves the affiliation.
- (d) A Branch, Division or Section shall not affiliate with or be represented by or on any other organisation, cause or movement unless Federal Council or the Board has granted approval.

SECTION 12 - ELECTIONS

78 - TERMS OF OFFICE

(a) The terms of office for each office shall be as follows:

(i)	Honorary Federal Officers	2 Years
(ii)	Other Federal Councillors	2 Years
(iii)	Honorary Branch Officers	2 Years
(iv)	Other Branch Councillors	2 Years
(v)	Section Representatives	2 Years
(vi)	Ethics Panel member	4 Years
(vii)	National Stunt Committee*	2 Years

^{*} Equity section members graded as stunt performers, stunt co-ordinators and safety supervisors;

(b) Notwithstanding (a), an incumbent officer shall hold office for the term specified in (a) or until a declaration of the ballot for that office occurs, whichever is the later.

(c) No employee of the Association may hold any honorary office in the Association.

79 - ELECTIONS

- (a) Not later than June 30 in each even-numbered year, the Board shall:
 - (i) Fix dates for nomination and election of Federal and Branch officers as required by these Rules.
 - (ii) Appoint a Federal Returning Officer for the conduct of the elections. The Returning Officer shall not be a holder of any office in, nor be an employee of, the Association or a Branch, Section or Division.
 - (iii) Determine a date for close of voting
- (b) The Federal Returning Officer shall appoint a Branch Returning Officer to conduct elections for each Branch. The Branch Returning Officer will not be a holder of any office in, nor be an employee of the Association or a Branch, Section or Division.

Notice of Elections

- (c) The Returning Officer shall:
 - (1) In each even-numbered year for honorary positions (or when appropriate in the case of a casual vacancy), circulate a notice to all members or take such other measures as are necessary calling for nominations of financial members entitled to nominate in accordance with these rules as candidates for election as:
 - (i) Federal President
 - (ii) Federal President (Media) (to be elected by members of the Media Section)
 - (iii) Federal President (Actors Equity) (to be elected by members of the Equity Section)
 - (iv) Federal President ECS (to be elected by members of the ECS section)
 - (v) Federal President (Musicians) (to be elected by members of the Musicians Section)
 - (vi) Federal Vice-Presidents (5) (the number for each section or group of sections to be determined by Rule 80)
 - (vii) Branch Officers
 - (viii) One Board member elected by and from the financial membership of each Branch with more than 900 financial members as at June 30 immediately prior to the biennial elections and One Board member elected by and from the financial membership of all other Branches
 - (ix) Branch Secretaries (where determined by Federal Council)
 - (x) State delegates to Federal Council/ Board as determined by Rule 40 from those States where Federal Council has not determined to form a Branch.
 - (xi) Delegates from the Sections of the Association to Federal Council (the number to be determined by Rule 80)
 - (xii) Delegates from the Sections of the Association to Branch Council (the number to be determined by Rule 80)
 - (xiii) National Stunt Committee 12 (Equity Section Stunt performer 4, Stunt co-ordinator 4, Safety Supervisor members 4)
 - (2) The notice shall stipulate that a member cannot stand for more than one of each of the positions specified in sub-rule (c), excepting that a member nominating for a Branch Council position other than Branch President or Branch Secretary or in the NSW and Victoria Branch Vice-President, may also nominate for the position of Section Delegate to Federal Council.

. .			. •	
N	om	เทล	IT10	ns

	(3)	The notice shall further stipulate that where there are three or more positions to be filled in any election (other than those applying to the Professional Sports Section or Professional Sports Branch) one of each three of the positions shall be filled by a woman according to the following formula:
		 3 - 5 positions: at least one woman 6 - 8 positions: at least two women 9 - 11 positions: at least three women 12 - 14 positions: at least four women 15 - 17 positions: at least five women
	(4)	The notice shall further stipulate that where a section is entitled to two or more delegates to Federal Council, they shall be elected according to the following formula:
		2 delegates from at least 2 states 7 delegates from at least 3 states 12 delegates from at least 4 states
	(5)	The notice shall further stipulate that where at least two vice-presidents are to be elected under $(c)(1)(vi)$ from any section or sections, at least one of those two shall be a woman, unless the President from the relevant section is a woman.
	(6)	If insufficient eligible candidates nominate to meet the provisions of parts (3) and (4) of this sub-rule, then the provisions shall not apply.
	(7)	The notice shall specify the time and date for the opening and closing of nominations and the name and address of the Branch Returning Officer appointed to receive the nominations. The notice shall be circulated at least 14 days prior to the time and date for the closing of nominations.
		Nominations
(d)		nations must be in writing and contain the given names and/or other identifying names and of employment and address of each candidate. Nominations:
	(i)	must be signed by at least one other financial member of the Branch and contain the addresses of the signatories;
	(ii)	must be accompanied by the written consent of the member nominated;
	(iii)	may be accompanied by a statement to a maximum of 150 words; and
	(iv)	Nominations must be submitted in the following form:
		Date
		I hereby nominate (block letters) a financial member of the Branch as a candidate for election as (state the position to which election is desired)
		Signature
		Name (Block Letters)
		Address

I hereby consent to the above nomination.	
Signature	
Address	
Place of Employment	-

(e) The Branch Council in a Branch with less than 500 financial members shall have discretion to decide whether sub-clause (2) of Clause (c) of this rule shall apply or whether a member may stand for not more than two of the following positions: Branch President, Branch Vice-President, Branch Treasurer, Branch Secretary or the Branch Council. The Branch Committee shall decide the sequence of election.

Close of Nominations & Defective Nominations

(f) The Returning Officer shall close receipt of nominations at the time fixed. If the Returning Officer conducting such an election finds a nomination to be defective he or she shall, before rejecting the nomination, notify the person concerned of the defect, and, where it is practicable to do so, give him or her the opportunity of remedying the defect where practicable, within seven days after his or her being so notified. The Returning Officer shall submit a report in writing on all nominations received by him or her to the next meeting of the Branch Council in the case of all nominations for positions in that Branch and the Board in the case of all nominations for Federal Officers.

Contested Election

- (g) Should the number of valid nominations received exceed in any case the number required to fill the office or position concerned such nominations shall be submitted to a secret postal ballot of all financial members of the Branch or of the Association in the case of Federal Officers for election, except where a offices are to be filled by a section representative, in which case only members of the relevant section(s) shall be eligible to vote.
- (h) The Returning Officer shall:
 - (i) close the roll of voters 7 days before the opening of nominations and give instructions for the preparation of a list of names and last known addresses of financial members entitled to vote.
 - (ii) arrange for the printing of declaration envelopes, prepaid reply envelopes and ballot papers to be distributed by post to each eligible voter; the declaration and prepaid envelopes must comply with the forms prescribed by the relevant legislative requirements.
 - (iii) upon receiving advice in writing from any eligible member that the member shall be absent from his or her usual address during the period of the ballot, forward a ballot paper, a declaration envelope, prepaid reply envelope and candidates' statements (if provided) to such address as advised by the eligible member.
- (i) The Returning Officer shall draw lots to determine the order in which the names of candidates shall appear on the ballot paper.
- (j) The given names and/or other identifying names and the place of employment of each candidate for election shall be included on the ballot paper for the guidance of members in voting. This information shall be supplied by a candidate with his or her nomination. Each candidate may also prepare and include with his or her nomination a statement containing his or her Association and employment/professional history and place of employment to a maximum of 150 words. The Returning Officer shall issue a copy of each statement (including where applicable, the candidates photograph) with each ballot paper.

Page 60 of 65 Pages

System of Voting

- (k) The system of voting to apply to elections in the Alliance shall be the preferential system. Each voter is required to vote for at least the number of vacancies to be filled in each position.
- (l) After completing the ballot paper, the voter shall place the paper in the declaration envelope, complete the declaration on the envelope and insert the declaration envelope in the prepaid reply envelope.
- (m) At the close of the ballot, the returning officer shall check the declarations against the roll of voters. The following procedure shall then be followed for the counting of the ballots:-

Election of One Candidate Only

- (1) Where one candidate only is to be elected, the Returning Officer shall observe the following procedure to determine the successful candidate:
 - (i) A candidate who receives more than half the number of first preference votes cast shall be the successful candidate.
 - (ii) Should no candidate be successful on the first round, the candidate who receives the least number of first preference votes shall be excluded from the count and his or her second preference votes shall thereupon be distributed among the remaining candidates. A candidate then receiving more than half the total number of votes cast shall be thereupon be the successful candidate.
 - (iii) The above procedure shall be continued until one candidate has received the requisite number of votes to become the successful candidate.
 - (iv) If on any count two or more candidates each receive the same number of votes the candidate who received the greater number of first preference votes shall remain in the count. If two or more candidates receive an equal number of first preference votes the Returning Officer shall decide by lot which candidate shall remain in the count.

Election of More Than One Candidate

Where two or more candidates are to be elected the Returning Officer shall observe the following procedure to determine the successful candidate:

The votes shall be classified into two categories as follows:

- (i) The preference votes for the number of vacancies to be filled shall be termed "primary" votes, and shall have equal value in the first count and be credited to the
 - candidate for whom they are cast, whether marked 1, 2, 3, etc. according to the number of vacancies. The preference votes beyond those referred to in (1) shall be termed "secondary" votes, and shall have rank according to their numerical number and shall be allocated in rank order unless the ranking secondary vote has been previously allocated.
- (ii) The "primary" votes shall first be counted and a list shall be prepared of the candidates in order according to the primary votes cast for them. The candidate who is lowest on the list thus compiled shall be excluded from the count.
- (iii) Each ballot paper on which such excluded candidate received a "primary" vote shall then be examined to determine its "secondary" vote and the preference so found shall be allotted to the appropriate remaining candidate on the first count.

- (iv) On the conclusion of the second count, the above procedure of exclusion of candidates from the count and the distribution of their secondary votes shall continue until the required number of successful candidates has been determined.
- (v) If, in any count, the next available preference vote of an excluded candidate is cast in favour of an excluded candidate, such preference vote shall be disregarded and the next available preference vote cast in favour of a remaining candidate shall be added to the votes credited to that candidate.
- (vi) If, in any count, two or more candidates each receive the same number of votes and one of them has to be excluded, the Returning Officer shall decide by lot which candidate shall remain in the count.
- (vii) If at the conclusion of all necessary counts, the provisions of Rule 79(c)(3) and (4) have not been applied, the Returning Officer shall apply the provisions of the Rule. Where there is a conflict between the provisions of these sub-rules, then the provisions of Rule 79(c)(3) shall prevail.
- (3) (i) Where one candidate only is to be elected (that is, for the offices listed in (c)(1)(i) to (v)), the Returning Officer shall observe the procedure set out in sub-paragraph (1) of this rule.
 - (ii) Where two or more candidates are to be elected (that is, for the offices listed in (c)(1)(vi)), the Returning Officer shall observe the procedure set out in sub-paragraph (2) of this rule, provided that, if, at the conclusion of all necessary counts for the offices listed in (c)(1)(i) to (v), the provisions of Rule 79(c)(5) have not been applied, the Returning Officer shall apply the provisions of the Rule to the extent necessary in the count for positions listed in (c)(1)(vi). Where there is a conflict between the provisions of sub-rule (c)(5), then the provisions relating to minimum numbers of women shall prevail.

Appointment & Conduct of Scrutineers

- (n) Any candidate shall be entitled to appoint a scrutineer to inspect any aspect of the conduct of the election by the Returning Officer.
- (o) A scrutineer shall not interfere with the conduct of the ballot or the counting of votes. If he or she considers that any vote is invalid or that there is any irregularity in the counting, he or she may bring the matter under the notice of the Returning Officer who shall record in his or her report to the Federal President or the Branch Secretary/Regional Director as the case may be any objection raised by a scrutineer.

Returning Officer's Report & Declaration of Ballot

- (p) The Federal Returning Officer shall report the result of the ballot for Federal Officers to the Board.
- (q) After the Board has received the report of the Federal Returning Officer on the election of Federal Officers, the Federal President shall declare the result of the elections. If a vacancy then exists the Board shall take whatever action it considers necessary or desirable to fill the vacancy.
- (r) A member who has been declared elected or re-elected as a Federal Officer shall assume the title and carry out the duties of his or her office immediately upon the cessation of the term of office of his or her predecessor or, in the case of a casual vacancy, after the close of the meeting of the Board at which the result of the election is declared.
- (s) Each Branch Returning Officer shall declare the ballot and shall report the results of the ballot for positions in that Branch to the Branch Council.
- (t) The Branch Council on receiving the report of the Returning Officer on the result of the ballot shall submit it to the Annual General Meeting.

Page 62 of 65 Pages

80 - FORMULA FOR ELECTION OF FEDERAL, BRANCH AND SECTION DELEGATES AND VOTING AT FEDERAL COUNCIL

- (u) If there are not sufficient nominations to fill the offices and positions listed in sub-clause (c) of this Rule or it is demonstrated that a successful candidate has become unable or ineligible to assume the office or position to which he or she has been elected, the Branch Council shall take action to fill the vacancy for the balance of the term, in accordance with sub-rule (w).
- (v) Any candidate defeated on a ballot may demand a recount of votes by lodging with the Returning Officer an application in writing within three days of the declaration of the ballot by the Branch Returning Officer or the Board as the case may be.

Casual Vacancies

- (w) Should there be a casual vacancy for any office, the vacancy so created will be filled:
 - (i) by appointment by the Branch Council or the Board as the case may be, provided that where the unexpired part of the term of office so vacant exceeds 12 months or three quarters of the term of office, whichever is the greater, an election shall be conducted in accordance with this rule.
 - (ii) any person so elected or appointed to a casual vacancy shall hold the office until the expiration of the balance of the term left vacant.

80 - FORMULA FOR ELECTION OF FEDERAL, BRANCH AND SECTION DELEGATES AND VOTING AT FEDERAL COUNCIL

- (a) The Board shall determine the number of Federal Council delegates to which each national section is entitled by applying the following formula:
 - (i) The annual income of each national section from entrance fees and membership subscriptions shall be ascertained for the previous financial year.
 - (ii) The 'notional' number of members of each national section shall be ascertained by dividing the amount of income for each section by \$200.00 (or another amount as determined by the Board).
 - (iii) The respective proportions of the notional members of each national section shall be ascertained.
 - (iv) The proportional formula so obtained in respect of national sections shall be applied to the number fifty.
 - (v) The result rounded to the nearest whole number which is one or greater shall be the number of delegates to Federal Council from the respective sections.
- (b) The Board shall determine the number of Branch Council delegates to which each section is entitled by applying the following formula:
 - (i) The annual income of each section within the Branch from entrance fees and membership subscriptions shall be ascertained for the previous financial year shall be ascertained
 - (ii) The 'notional' number of members of each section shall be ascertained by dividing the amount of income for each section by \$200.00 (or another amount as determined by the Board).

83 - MEMBERS RIGHT TO VOTE IN BALLOT

- (iii) The respective proportions of the notional members of each section shall be ascertained.
- (iv) The proportional formula so obtained shall be applied to the number twenty-five (or such lesser number as determined by Federal Council or the Board).
- (v) The result rounded to the nearest whole number which is one or greater shall be the number of delegates to Branch Council from the respective sections.
- (vi) In accordance with clause (iv) of this sub-rule, Federal Council may determine that the lesser number be zero in which case there will be no section delegates to the Branch Council.
- (c) The Board shall determine the number of Federal Vice-Presidents to which each section or grouping or sections is entitled by applying the following formula:
 - (i) The annual income of each of the Media, Equity, ECS and Musicians Sections from entrance fees and membership subscriptions shall be ascertained for the previous financial year.
 - (ii) The 'notional' number of members of each section or grouping of sections shall be ascertained by dividing the amount of income for each section by \$200.00 (or other amount as determined by the Board).
 - (iii) The respective proportions of the notional members of each section or grouping of sections shall be ascertained.
 - (iv) The proportional formula so obtained in respect of section or grouping of sections shall be applied to the number five.
 - (v) The result rounded to the nearest whole number which one or greater shall be the number of federal vice-presidents from the respective sections or groupings of sections.

81 - AVOIDANCE OF IRREGULARITIES

Notwithstanding the provisions of this Rule a Returning Officer may take such action and give such directions as he or she considers necessary in order to ensure the secrecy of the ballot and that no irregularities occur in or in connection with the election or to remedy any inconsistency or inadequacy that may arise in the application of this Rule.

82 - OFFICERS ILLEGALLY ELECTED

Should any office of any Branch Council or the Board or Federal Council or Sectional Committee be illegally elected, any business transacted by such Officer or body of which such illegally-elected person is a member, shall nevertheless be held to be properly transacted and the legality of his or her act shall not be capable of being challenged or called into question unless it was done in bad faith.

83 - MEMBERS RIGHT TO VOTE IN BALLOT

Financial members entitled to vote in elections for federal officials of the Association shall have the right to vote in all ballots conducted under law for the amalgamation of the Association with any other association or organisation.

Page 64 of 65 Pages

84 - TRANSITIONAL RULES

- (a) The Association has determined that no officers shall be employees of the Association pursuant to Rule 5(g) with effect from biennial elections of 2014-2015.
- (b) The appointed chief executive shall not be an officer of the Association under these rules or the Fair Work (Registered Organisations) Act 2009;
- (c) To the extent that any of the duties laid out in Rule 50 or in any other Rule may only be implemented by an Officer under these Rules or the Fair Work (Registered Organisations) Act 2009, the Federal President shall be the relevant Officer, subject to the delegation of these powers in accordance with these rules.

END OF RULES

Page 65 of 65 Pages



The Afghan Files

Defence leak exposes deadly secrets of Australia's special forces

By the National Reporting Team's Dan Oakes and Sam Clark

Updated 11 Jul 2017, 8:49am Published 11 Jul 2017, 6:02am The Afghan Files: Defence leak exposes deadly secrets of Australia's special forces - ABC News (Australian Broadcasting Corporati...

undreds of pages of secret defence force documents leaked to the ABC give an unprecedented insight into the clandestine operations of Australia's elite special forces in Afghanistan, including incidents of troops killing unarmed men and children.

The ABC can reveal that some of the cases detailed in the documents are being investigated as possible unlawful killings.

The Afghan Files

9/14/2018

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1
Leaked documents expose deadly secrets of
Australian special forces

NOW READING

#2
An interrogation, a shooting and no witnesses

NOW READING

#4
#5
The spy and the SAS soldier with a loaded
Glock

Who is the enemy? Australia's secretive rules
of engagement

#7
Relations between Australia's special forces units on 'knife edge'

This comes a day after the ABC revealed the alleged cover up of the killing of an Afghan boy and another alleged incident in which a father and son were shot dead during a raid.

The documents, many marked AUSTEO — Australian Eyes Only — suggest a growing unease at the highest levels of Defence about the culture of Australia's special forces as they prosecuted a bloody, secretive war against insurgents across a swathe of southern Afghanistan.

One document from 2014 refers to ingrained "problems" within special forces, an "organisational culture" including a "warrior culture" and a willingness by officers to turn a blind eye to poor behaviour.

Another document refers to a "desensitisation" and "drift in values" among elite Special Air Service soldiers serving in Afghanistan, while others allude to deep divisions between the two elite units which primarily comprise the special forces - the SAS based in Perth and 2 Commando Regiment based in Sydney.

A large proportion of the documents are reports on at least 10 incidents between 2009-2013 in which special forces troops shot dead insurgents, but also unarmed men and children.

The Inspector General of the Australian Defence Force is investigating at least two of the incidents as part of its inquiry into the conduct in Afghanistan of special forces, which includes alleged unlawful killing.

Those two incidents — which both occurred in September 2013 — are the deaths of a man and his six-year-old child during a raid on a house, as revealed yesterday by the ABC, and the killing of a detainee who was alone with an Australian soldier and allegedly tried to seize his weapon.

A report into another 2013 incident in which an Afghan man riding a motorcycle was killed by Australian troops, and a female passenger possibly injured, states that Afghan authorities were becoming increasingly agitated over Australians allegedly killing unarmed civilians, and threatened to stop working with Australians.

Inside the Afghan Files ABC News

The documents also provide fresh details of some notorious incidents, including the severing of the hands of dead Taliban fighters by Australian troops.

The report shows Federal Liberal MP Andrew Hastie, then a SAS officer and commander of the soldier who cut off the hands, immediately expressed alarm about what happened and reported the incident up the chain of command.

The incident also caused tension between the SAS and Australian Defence Force Investigative Service (ADFIS), with the commanding officer of the SAS Regiment writing an angry letter to the head of ADFIS, in which he claimed ADFIS was seeking to charge SAS members over the incident in order to obscure their own culpability in what happened.

Another letter, sent in 2013 by a senior officer of 2 Commando to Chief of Army David Morrison, exposes the rift between the SAS and 2 Commando.

The letter, in response to claims made by SAS Victoria Cross winner Mark Donaldson in his autobiography, said relations between the two units were on a "perilous knife edge" and in "an extremely unhealthy state".

The most dense and complex documents are those that seek to codify what tests Australian soldiers have to apply before they shoot to kill.

In 2013, sparked by an incident the previous year in which Australians killed two unarmed Afghan men, a series of directives and memos was issued by the Defence Force hierarchy stressing the need to be certain that Afghans were "directly participating in hostilities" before shooting them.

The documents indicate just how difficult this certainty could be to arrive at, particularly regarding 'spotters', or Afghans who kept watch and relayed information to Taliban fighters, without necessarily being armed.

Spotters could be shot for riding a motorcycle in a 'stop-start' fashion, talking on a radio or "manoeuvring to gain a tactical advantage", according to the documents. But as Australia began to step back from operations in Afghanistan, purportedly to allow the Afghan security forces to take responsibility for security in Uruzgan province, an Australian officer hinted that Afghan patience might be wearing thin.

"This shift may require a review of the burdens of proof as they pertain to the necessity of engaging spotters perceived to be directly participating in hostilities," he wrote after an Afghan man on a motorcycle was shot and killed, but the Australian soldier responsible cleared.

"The necessity of [special forces] to press the tactical advantage of the engagement needs to be weighed against the political disadvantage created by civilian casualty allegations against [Coalition forces] at this stage of the campaign."

Delve further into the documents and read the full stories uncovered as part of the ABC's investigation into The Afghan Files.

What the documents reveal about killings of unarmed Afghans

A helicopter attack killing boys and their donkeys, a detainee allegedly lunging for a knife shot dead and a boy mistakenly killed as he hid under blankets are all detailed in the documents.

They show that on a number of occasions Defence investigations only occurred because locals complained to Afghan authorities, and those authorities demanded answers from the Australian forces, or because journalists or NGOs raised concerns.

Some of the incidents detailed have been publicly acknowledged by Defence previously, usually in response to media reporting, but the outcomes of investigations are seldom made public - until now.

Read summaries of 10 cases between 2009-2013 in which special forces troops shot dead insurgents, but also unarmed men and children.

READ THE SUMMARIES

An interrogation, a shooting and no witnesses

Inside a hut, in the far east of Afghanistan's Uruzgan Province, an Australian soldier was left alone with a captured insurgent.

But while others outside prepared for a helicopter transfer, the detainee was shot dead.

The ABC can reveal the secretive defence inquiry probing allegations of unlawful killings in Afghanistan is now investigating the incident.

'What the f*** are you doing': Chaos over severed hands

It was one of the most notorious incidents in Australia's recent military history — the severing of hands of dead Taliban fighters in Afghanistan.

When it was first reported by the media in August, 2013, it caused a public furore and deep concern within Defence.

Now, for the first time, secret defence documents obtained by the ABC reveal the full story of how and why the "chopped hands" controversy came about.

The spy and the SAS soldier with a loaded Glock

Even in a warzone like Afghanistan, spies and soldiers need to relax, to let their hair down.

And so it was that on December 7, 2013, a handful of officers from the Australian Secret Intelligence Service and nine Australian soldiers — deployed to guard the spies — decided to put a lamb on the barbie.

But what started as a convivial dinner in covert premises in Kabul ended badly with an SAS trooper pulling his handgun on a female ASIS officer.

Who is the enemy?

From the very beginning of the war in Afghanistan, Australian troops were faced almost every day with decisions that had to be made within a split second.

The farmer smiling at you as you patrolled though his village could have an AK-47 stashed behind a nearby wall. The youth watching silently as you left your base could be reporting your movements to the insurgents.

The Taliban didn't wear uniforms and often did not carry weapons on them. They travelled on motorbikes and in utes. They shook your hand by day and laid improvised explosive devices by night.

Now, Defence documents obtained by the ABC give an insight into the ambiguities and difficulties faced by troops on the ground.

'Unhealthy' relations between elite teams

They are the most celebrated and prestigious units in the Australian Army.

The SAS - the Special Air Service Regiment - and the 2nd Commando Regiment are Australia's special forces elite, the soldiers tasked with the most difficult missions in warzones like Afghanistan.

But now Defence Department documents leaked to the ABC reveal that relations between the two units — which also have a crucial role in domestic counter-terrorism operations have reached an all time low.

READ THE STORY

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read them.

Contact us on Signal: 0419 242 515

WhatsApp

9/10

9/14/2018 The Afghan Files: Defence leak exposes deadly secrets of Australia's special forces - ABC News (Australian Broadcasting Corporati...

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

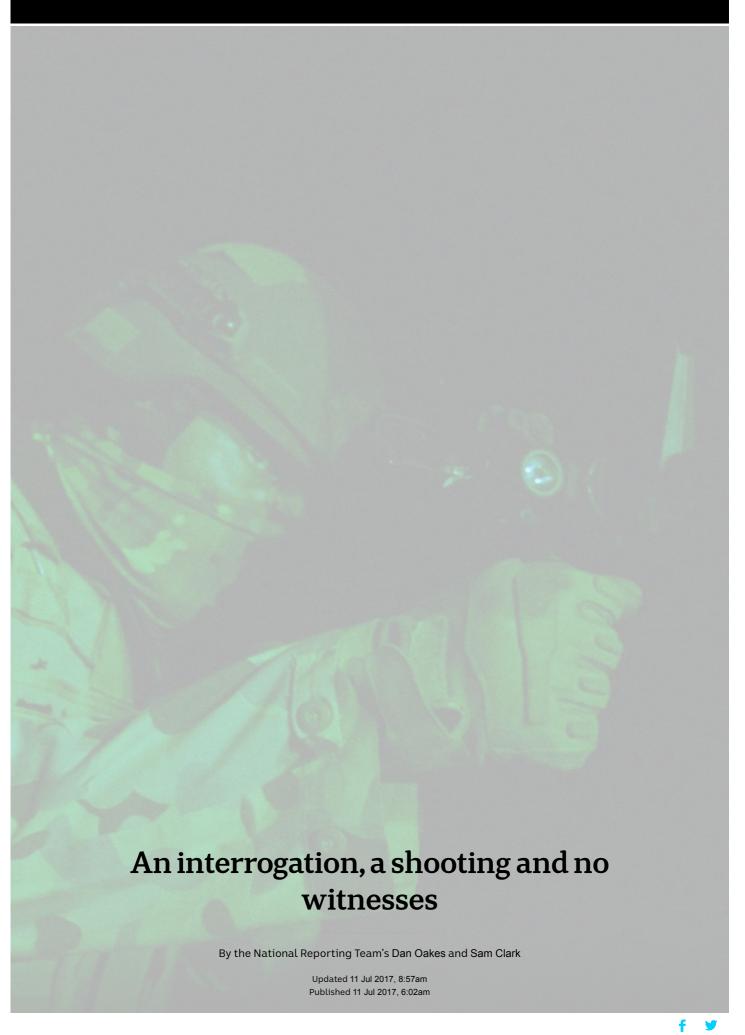
The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of	#2 An interrogation, a shooting and no witnesses	#3 What the documents reveal about killings of
Australian special forces NOW READING		unarmed Afghans
#4	#5	#6
The spy and the SAS soldier with a loaded	Who is the enemy? Australia's secretive rules	Chaos over severed hands
Glock	of engagement	
#7		
Relations between Australia's special forces units	s on 'knife edge'	

Photos: Margaret Burin

10/10





secretive inquiry probing allegations of Australian war crimes in Afghanistan is investigating the killing of a Taliban detainee by an Australian soldier in 2013.

It was revealed on 7.30 last night that the inquiry is already investigating the possibility that Australian soldiers covered up their killing of a 14 or 15-year-old Afghan boy in 2012, and also investigating the death of man called Bismillah Azadi and his six-year-old son in 2013.

Defence has confirmed to the ABC that the inquiry, headed by NSW Supreme Court judge Paul Brereton on behalf of the Inspector General of the Australian Defence Force, is also "reviewing" the death of the detainee which has never been publicly disclosed until now.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#2 #1 #3 Leaked documents expose deadly secrets of An interrogation, a shooting and no witnesses What the documents reveal about killings of Australian special forces unarmed Afghans #4 #5 #6 The spy and the SAS soldier with a loaded Who is the enemy? Australia's secretive rules Chaos over severed hands Glock of engagement Relations between Australia's special forces units on 'knife edge'

According to a "quick assessment" report obtained by the ABC, the man and two other "persons of interest" were captured during a clearance operation carried out by Afghan and Australian troops in the far east of Uruzgan province.

The Afghan troops interrogated them and told the Australians the men were Taliban and needed to be taken back to the main base at Tarin Kowt for questioning.

At some point one Australian soldier was left alone with one detainee in a hut.

According to the report, the Australian removed the cuffs from the Afghan in order to transfer him to a helicopter and the detainee allegedly tried to grab the Australian's rifle.

There were no witnesses to the killing and the quick assessment cleared the Australian of any wrongdoing.

The commanding officer of the special operations task group wrote on the quick assessment report: "I don't believe an [Australian Defence Force Investigative Service] investigation will 'value add' at this stage due to their inability to compel witnesses to give statements (ie. the members will exercise their right to remain silent, as has been evidence in previous cases)."

"If a serious incident is deemed to have occurred, ADFIS will be involved as a matter of course by the inquiry officer."

Inside the Afghan Files ABC News

However, investigators from ADFIS who arrived in Afghanistan soon afterwards declared they were investigating a potential war crime of "wilful killing". They demanded the weapon used to kill the Afghan detainee be handed over for examination.

The commanding officer of the special operations task group — on the advice of the Defence lawyer assigned to the task group — refused, saying the investigators' warrant was flawed as it listed the wrong offence, and that the killing was a clear cut case of self-defence.

He also said that the weapon had been used in operations since the killing and he therefore failed to see how forensically testing it would be of any use. The investigators then allegedly threatened to take the weapon by force.

The situation was only defused when the commanding officer reluctantly handed over the weapon. He and the legal officer were later investigated for allegedly obstructing an ADFIS investigation but counter-claimed that they had been threatened by the investigators. It was also later determined that the warrant was, indeed, faulty.

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read them.

Contact us on Signal: 0419 242 515

WhatsApp

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

The Afghan Files

#7

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of Australian special forces #2
An interrogation, a shooting and no witnesses

NOW READING

#3
What the documents reveal about killings of unarmed Afghans

The spy and the SAS soldier with a loaded Glock

Who is the enemy? Australia's secretive rules of engagement

#6 Chaos over severed hands

Relations between Australia's special forces units on 'knife edge'

Header photo: Margaret Burin

What the documents reveal about killings of unarmed Afghans

By the National Reporting Team's Dan Oakes and Sam Clark

Updated 11 Jul 2017, 10:45am Published 11 Jul 2017, 6:02am



n occasion, the killing of Afghan civilians or unarmed insurgents was investigated by the Australian Defence Force.

Usually, this was an inquiry conducted by an officer from outside the unit.

Often the inquiry officer's job was made more difficult by the fact that, due to the security situation, it wasn't possible to visit the scene of the killing and interview locals who witnessed the incident.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 #3 #2 Leaked documents expose deadly secrets of An interrogation, a shooting and no witnesses What the documents reveal about killings of Australian special forces unarmed Afghans NOW READING #4 #5 #6 The spy and the SAS soldier with a loaded Who is the enemy? Australia's secretive rules Chaos over severed hands Glock of engagement #7 Relations between Australia's special forces units on 'knife edge'

The ABC has obtained a number of the inquiry reports and other documents which show that on a number of occasions the inquiries occurred only because locals complained to Afghan authorities, and those authorities demanded answers from the Australian forces, or because journalists or NGOs raised concerns.

Yesterday, the ABC revealed that Defence's Inspector General (IGADF) is investigating the killing of two children in separate incidents in 2012 and 2013. It is not clear whether all of the incidents listed below are being investigated by the Inspector General's inquiry.

Sometimes, particularly after 2011, when concerns began to grow in Canberra about the actions of Australia's special forces in Afghanistan, staff from the Australian Defence Force Investigative Service (ADFIS) were sent to investigate incidents.

This culminated in September 2013, when in the space of a week Australian special forces soldiers killed a man and his sleeping child, and an Afghan detainee was shot dead after allegedly trying to seize the weapon of an Australian SAS trooper.

On at least one of these occasions, the commanding officer of the Special Operations Task Group in Tarin Kowt refused to hand over evidence to ADFIS investigators without a warrant, leading to an ugly confrontation between officers from special forces and ADFIS investigators.

Some of the incidents detailed below have been publicly acknowledged by Defence previously, usually in response to media reporting, but the outcomes of investigations are seldom made public.

Heavily redacted inquiry reports were sometimes released, but political considerations were taken into account when that decision was made.

For example, advice to the Defence Minister about the inquiry into the killing of two mullahs by SAS members in 2012 said "publishing additional detail through release of a redacted report would increase the risk to Australia's relations with Afghanistan".

In that case, Afghan officials from then-president Hamid Karzai down had complained bitterly and publicly about the killings, stating that the dead men were not Taliban and the deadly raid was not authorised by the Afghan Government.

Inquiry officer inquiries invariably found that Australian soldiers had acted within their rules of engagement, and that no further action should be taken.

The following are summaries of the inquiry reports found among the hundreds of pages of secret Defence documents leaked to the ABC.

Three men killed, including one hiding in hay stack

Date: 2/4/2009

Location: Jalbay, Uruzgan Province

Description: Australians hunting for a "medium value" target arrived at the village of Jalbay in helicopters after dark. The Taliban target was not there, but the Australians killed three men, including one who was hiding in a hay stack, one hiding in a chaff pile, and another trying to take cover in a line of trees nearby. The Australians later said that the men who were hiding in the chaff pile and hay stack were in a "firing position", but no weapons were found afterwards.

Outcome: Inquiry found the Australian soldiers had acted within the rules of engagement, yet admitted no weapons were found, and that a number of intelligence sources said the men were civilians, not insurgents. The inquiry officer also claimed that an alleged lack of protest by locals over the killings, and the fact the dead men supposedly did not behave like "uninvolved" Afghan civilians when the soldiers arrived, meant they were likely to have been "associates" of the Taliban member being targeted.

Apache helicopter destroys vehicle that switched off lights

Date:10/6/2009

Location: Noy Juy, Mirabad

Description: After heavy fighting between Australian troops and insurgents, the Australians saw suspected fighters leaving the area in a number of vehicles at dusk. Radio chatter intercepted by Australian soldiers suggested that insurgents had been instructed to turn the headlights of their Toyota Hilux off as they retreated from the area. Soon after this, Australian soldiers on the ground and the crew of a Dutch Apache attack helicopter saw a vehicle switch its lights off as it drove away from the area. The Apache helicopter destroyed the Hilux. The headlights of another vehicle were seen to be switched off and the Apache destroyed that car as well. Media reports later suggested civilians were killed.

Outcome: Inquiry found the killing of the suspected insurgents fell within the rules of engagement. A legal assessment of the incident suggested that the civilian casualties may have resulted from a large explosion witnessed earlier in the day, however, this seems to contradict claims of locals who say they were targeted by two helicopters.

Detainee whose handcuffs 'separated' shot dead

Date: 3/10/2010

Location: Zangitan, Kandahar Province

Description: Australian troops detained two men. One Australian soldier questioned the detainees through an interpreter. The interpreter left the room, followed by one detainee walking and then the Australian. The detainee then allegedly reached up and grabbed a knife from a ledge just above the doorway. The detainee, whose plastic handcuffs had "separated" then struggled with the Australian, before the Australian shot him several times and killed him. It was not until two years later, after a journalist asked questions, that a Defence quick assessment discovered that dead man was a detainee, and had not been killed during a battle. ADFIS then investigated the incident.

Outcome: It was determined that the man was a detainee when he was killed, and the chief of joint operations, Lieutenant General Ash Power, said in a brief in August 2012 that he was "disappointed with the operational decision making and reporting procedures at the time of the incident". However, it was determined that the Australian was within his rights to shoot the detainee dead.

Man and boy killed 'returning from local medical clinic'

Date: 27/3/2011

Location: Sah Zafar, Chora Valley

Description: Australian and Afghan troops conducting a 'cordon and callout operation' were sent to a location where it was hoped they would capture a high-value Taliban target. As they moved along a road they were shot at from a concealed area. The Australians returned fire and immediately moved up to the location from where the shots originated. There they found a dead man and a fatally injured child. Locals in a "distressed state" arrived at the scene and told the Australians that the dead man was the boy's uncle, and that he was returning with his nephew from the local medical clinic. Australian soldiers tested the dead man's hands and found traces of nitrate, which they said proved he had handled explosives and was an insurgent. However, this was later disproved, as there was no evidence the man was an insurgent, and nitrates are present within commonly-used fertilisers in Afghanistan. The report says the commanding officer and the officer who carried out the initial 'quick assessment' had an "incomplete" understanding of the technology. Bags containing medication were also found at the scene of the killing, lending further credence to the locals' story.

Outcome: The inquiry found the Australian troops were acting within the rules of engagement when they killed the man, but was heavily critical of the process by which he was labelled an insurgent after his death.

Afghan boy survives being shot through face

Date: 1/5/2012

Location: Deh Rafshan area of Uruzgan Province

Description: Australians were carrying out a "capture/kill" mission targeting a mid-level insurgent commander and bomb maker in the Deh Rafshan area of Uruzgan Province. The insurgent leader was holding a meeting with "four known key insurgents", so the Australians set up a number of "blocking positions" to contain them. An Australian sergeant saw two Afghans who he believed were trying to evade the cordon, and both he and an Afghan soldier called on them in Pashtu to stop. They kept walking towards some elevated ground, and the Australian, believing they would gain a tactical advantage if they reached the higher ground, fired a single shot. The men kept moving, and a 13-year-old boy, drawing water from a well nearby, walked after them in order to convince them to stop. The Australian fired at the men again, and they finally stopped. When he approached the men he found the 13-year-old boy with a gunshot wound to neck and an exit wound through his mouth. No weapons were found, and the men were ultimately released. The boy survived.

Outcome: The inquiry report found the Australian soldier had acted within the rules of engagement. However, it says that at a meeting held with village elders after the shooting, the boy's father said he witnessed a "heated argument" between two Australian soldiers, which he believed to be about the shooting.

> On the hunt for deadly Afghan soldier, two men killed

Date: 31/8/2012

Location: Sula

Description: Australian troops were hunting for an Afghan soldier who had killed three Australian troops on August 29. During the operation, an SAS trooper wrestled Mullah Jalil Akhund to the ground. The inquiry report said Mullah Jalil Akhund was initially compliant, but then tried to grab the Australian's weapon, so the Australian soldier shot him dead. Another man, Mullah Janan Akhund, was allegedly seen by two Australian special forces soldiers talking on a radio as an Australian helicopter approached the area. According to the

http://www.abc.net.au/news/2017-07-11/unarmed-men,-children-among-casualties-of-elite-forces/8424944

report, he "failed to comply with a number of directions to stop and was assessed by the SOTG members to be manoeuvring to gain tactical advantage through a covered position and potentially accessing a cache of weapons", so the Australians killed him.

Outcome: The inquiry found that the Australians acted according to their rules of engagement. However, it also found that the Australian troops were using International Security Assistance Force (ISAF) rules of engagement instead of Australian. It also revealed that Australians were relying on their own experience to determine when an Afghan was demonstrating insurgent "tactics, techniques and procedures", and then killing them, but that those criteria had not been endorsed by senior officers. A "communications pack" accompanying the report recommended that the report not be made public "following consideration of Australia's national interests".

Helicopter strike kills boys and donkeys

Date: 28/2/2013

Location: Char Chineh District, Uruzgan Province

Description: Australian and Afghan troops were conducting a sweep through a remote region. The Australians reportedly picked up radio chatter from insurgents indicating an "imminent threat", and pinpointed two insurgents 1.3 kilometres away from a checkpoint they had set up. They called in a helicopter strike, but then saw the helicopter's fire hit an area a few hundred metres from where they believed the insurgents were. They halted the air strike and went to where the shots had hit, finding two dead Afghan boys and three dead donkeys **Outcome:** Despite the ADF saying no Australian was to blame, a NATO enquiry carried out in the days afterwards found the Australian commander on the ground and the pilot of the American attack helicopter "did not fulfil their obligations" when they failed "to coordinate observation and fire onto the same point".

442 8/12

Motorcyclist gunned down for stopping and starting

Date: 9/3/2013

Location: Southern region of Uruzgan Province

Description: During an armed reconnaissance of "insurgent high activity zones" with their Afghan partner troops, Australian troops saw a motorbike carrying two people moving in a "stop/start" fashion. One Australian said he tried using hand gestures and verbal commands to get the motorcyclist to stop but that the motorcycle was heading to an area that "would provide a tactical advantage within the greenbelt". A second Australian shot and killed the rider, while the female passenger fell off and sat on the ground, seemingly unhurt. The Australian did not tell anybody at the time that he had shot the motorcyclist, and it was erroneously reported that Afghan troops were responsible.

Outcome: The inquiry found that the killing fell within the rules of engagement, but that Afghan officials were becoming increasingly agitated about incidents in which Australian troops killed unarmed Afghans. The report said there should be consideration given to changing to the rules of engagement around unarmed suspected "spotters".

Detainee shot dead in hut prompts war crime probe

Date: 23/09/2013

Location: Patan, Chenartu District

Description: Australian and Afghan soldiers detained three "persons of interest". They were handcuffed and taken to a nearby area to be questioned. The first two men were questioned inside a hut and then sent outside. The third man was questioned and a helicopter was arranged to fly the three suspected insurgents for further questioning. While alone with the third detainee, a special forces soldier removed the plastic handcuffs from the man. The Australian soldier said that as soon as he removed the cuffs the detainee grabbed for his rifle. The soldier, who was alone with the detainee, called out for assistance but before help arrived he shot and killed the detainee.

Outcome: A "quick assessment" of the incident found that the soldier operated within the rules of engagement, however just days after the incident ADFIS investigators arrived in Afghanistan, telling the commanding officer of special forces that the soldier was under investigation for the war crime of wilful killing. They demanded the soldier's weapon for forensic testing, and the commanding officer refused, saying the killing was in self-defence, and that the warrant supplied by the ADFIS investigators was invalid. The weapon was later given to the investigators, and the commanding officer and his legal officer investigated for allegedly hindering an ADFIS investigation. Nobody was ever charged, and the warrant was later found to have been flawed. Defence has referred this case to the Inspector General's inquiry.

Child found under blankets with bullet wound

Date: 26/9/2013

Location: Spin Kecha village, north west Uruzgan Province

Description: While searching a compound as part of an operation targeting a high value Taliban target, special forces soldiers saw a man, later named as Bismillah Azadi, allegedly pointing a pistol at them. Bismillah was shot and killed by two special forces soldiers, but they were unaware of a child hidden in blankets near him. The child was later discovered with a single gunshot wound to the abdomen and within five minutes was pronounced dead. A payment to the child's family of \$US1,500 was made.

Outcome: Inquiry found there was insufficient evidence to conclude that Bismillah was a member of the Taliban or an insurgent. However, the fact that he had pointed a loaded pistol at Australian troops and the absence of a local outcry following his death was cited as reason to suspect that he was supportive of the insurgency. The inquiry also concluded that the Australian soldiers who fired on Azadi had fired in self defence and exercised appropriate restraint. Defence has referred this case to the Inspector General's inquiry.

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read them.

Contact us on Signal: 0419 242 515

WhatsApp

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of Australian special forces

An interrogation, a shooting and no witnesses

#3
What the documents reveal about killings of unarmed Afghans

NOW READING

The spy and the SAS soldier with a loaded Glock

Who is the enemy? Australia's secretive rules of engagement

Chaos over severed hands

445

#2

Relations between Australia's special forces units on 'knife edge'

Header photo: Margaret Burin

The spy and the SAS soldier with a loaded Glock

What started as a convivial dinner in covert premises in Kabul ended badly with an SAS trooper pulling his handgun on a female spy.

By the National Reporting Team's Dan Oakes and Sam Clark

Updated 11 Jul 2017, 8:57am Published 11 Jul 2017, 6:02am ${f E}$ ven in a warzone like Afghanistan, spies and soldiers need to relax, to let their hair down.

And so it was that on December 7, 2013, a handful of officers from the Australian Secret Intelligence Service and nine Australian soldiers — deployed to guard the spies — decided to put a lamb on the barbie.

The beer and spirits were flowing freely.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of Australian special forces	#2 An interrogation, a shooting and no witnesses	#3 What the documents reveal about killings of unarmed Afghans
#4	#5	#6
The spy and the SAS soldier with a loaded	Who is the enemy? Australia's secretive rules	Chaos over severed hands
Glock	of engagement	
NOW READING		
#7		
Relations between Australia's special forces units	on 'knife edge'	

Two Afghan interpreters were present and at one stage, some Canadians joined the party.

But what started as a convivial dinner in covert premises in Kabul ended badly with an SAS trooper pulling his handgun on a female ASIS officer.

The ABC first reported the incident in 2014 but little detail was made public.

Now, a secret report obtained by the ABC paints a much fuller picture about what happened that night including how the SAS trooper allegedly held his loaded Glock pistol under the chin of the female spy.

It also reveals that some Australian troops in Afghanistan regularly drank alcohol — some of it supplied by the Australian Embassy — in direct contravention of standing orders.

The 36-page report is marked Secret AUSTEO (Australian Eyes Only).

It says that on the night in question three members of "another government agency" and nine defence force personnel were at the BBQ.

Soldier put muzzle directly under spy's chin

The report says alcohol was consumed during the evening.

There was evidence both the man and the woman involved "were to some degree intoxicated".

Neither is named in the report. They are referred as A35 (the soldier) and Officer L.

It says that around 11:00pm A35 headed back to his room "carrying his pistol in his hand, because his holster was in his room".

"Officer L followed soon after him.

"As she entered the courtyard she alleges in a written statement that A35 pointed his pistol directly at her.

"She alleges he then lowered the pistol, while further conversation took place, before raising it again and placing the muzzle directly under her chin. She saw that his finger was not on the trigger, and did not believe he intended to fire.

"However, she was aware that a magazine was attached to the pistol, was conscious that they had both been drinking and was worried about the potential for an accident."

A35 was 'talking with hands'

The report says A35 denied placing the weapon under her chin but admitted he was "possibly waving (the pistol) around and 'talking with his hands'."

Officer L walked away and when at what she thought was a safe distance, turned and called A35 "a complete dickhead".

She immediately told a colleague who noticed that she was "visibly shaking and had a quavering voice".

The reasons for the incident were not made clear, although Officer L told investigators A35 was interested in a relationship, something he denied. A35 countered that Officer L was known as "a flirt".

The report found that while ASIS officers were allowed to consume alcohol under certain circumstances, ADF personnel were not, except on special occasions such as ANZAC Day.

All the Defence Force members present on the night — except A35 — initially denied they had been drinking.

However, they later changed their story and said the ADF chain of command was "well aware" that members of the detachment drank alcohol.

They added that senior members in their chain of command also drank.

They told investigators alcohol was needed as a "currency" to gather information from intelligence agencies and the armed forces of other countries, and it was unworkable to have defence force personnel and ASIS agents living and working together under different alcohol restrictions.

Incident followed order of large amount of alcohol

The report said that early in the inquiry, investigators had been informed one large alcohol order had been requested and supplied to ADF members through the Australian Embassy's duty free facility.

"The order included 12 cases of beer and 40 bottles of spirits."

Both the ASIS officer and the SAS member were sent back to Australia within days of the incident.

Other documents obtained by the ABC show that the Army hierarchy was concerned about turning the matter over to the Australian Defence Force Investigative Service because it could end up in a public hearing, and compromise operational security (OPSEC).

However the then Chief of the Defence Force, General David Hurley, cautioned against this approach.

"I think we are placing too much emphasis on the OPSEC aspect of this incident. There appears sufficient evidence for [Special Operations Command and Chief of Army] to act ref the consumption of alcohol and the 'blind eye' turned to it by the [chain of command]," General Hurley writes.

"The provision of false evidence is more serious and could be forwarded to ADFIS (Australian Defence Force Investigative Service) — the OPSEC issue need not be a barrier to this. We need to smarten our response to these matters."

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read them

Contact us on Signal: 0419 242 515

WhatsApp

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of Australian special forces

An interrogation, a shooting and no witnesses

What the documents reveal about killings of unarmed Afghans

The spy and the SAS soldier with a loaded Glock

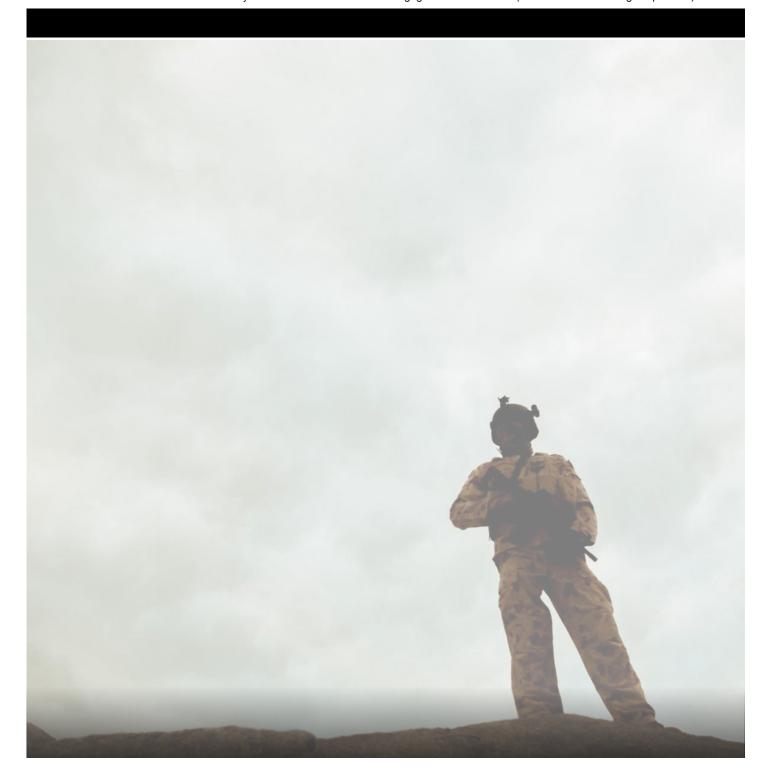
Who is the enemy? Australia's secretive rules of engagement

Chaos over severed hands

NOW READING

Relations between Australia's special forces units on 'knife edge'

Header photo: Margaret Burin



Who is the enemy? Australia's secretive rules of engagement

By the National Reporting Team's Dan Oakes and Sam Clark

Updated 15 Jul 2017, 1:18pm Published 11 Jul 2017, 6:02am

 $\begin{tabular}{ll} \textbf{D} icture this: you are an Australian special forces soldier on operations in Afghanistan. \end{tabular}$

Out of the corner of your eye you've spotted a person you believe to be a "squirter".

451 1

Do you shoot?

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

And if you do open fire on the "squirter", are you operating within the Australian Defence Force Rules of Engagement?

From the very beginning of the war in Afghanistan, Australian troops were faced almost every day with decisions that had to be made within a split second.

The farmer smiling at you as you patrolled though his village could have an AK-47 stashed behind a nearby wall. The youth watching silently as you left your base could be reporting your movements to the insurgents.

The Taliban did not wear uniforms and often did not carry weapons on them. They travelled on motorbikes and in utes. They shook your hand by day and laid improvised explosive devices by night.

Now, Defence documents obtained by the ABC give an insight into the ambiguities and difficulties faced by troops on the ground.

Which brings us back to the squirter.

In Australian military terms, a "squirter" is a person seen moving quickly away from an object of interest.

That person might be moving to gain a tactical advantage.

If you do decide to pull the trigger — and shoot a civilian — will your superiors find that you operated within the ROE — the all-important Rules of Engagement?

The ROE: a tightly-held secret

No army wants to let its enemy know when it will pull the trigger and when it will hold fire.

Obviously, any person pointing a weapon at an Australian was a valid target.

But documents obtained by the ABC show the Australian Defence Force instructed its members that unarmed Afghans might be legitimately killed if they were DPIH — "directly participating in hostilities".

Much paper and ink was expended on defining this term but in the context of day-to-day operations in Afghanistan it often pertained to two distinct patterns or types of activity: moving in a "tactical" fashion or to an area where weapons might potentially be stored, and "spotting" for Taliban fighters.

This meant that if you were an Afghan riding a motorcycle in a certain fashion near Australian troops, or were seen talking on a radio or mobile phone, you could be considered fair game.

The documents seen by the ABC stress that mere suspicion, or instinct, was not enough, though. There had to be a solid basis for that suspicion, based on knowledge of insurgent "tactics, techniques and procedures".

In April 2013, the Chief of the Defence Force, the Chief of Joint Operations and the head of the Joint Taskforce 633 (Australia's troops deployed in the Middle East), all issued directives stressing that Australian soldiers must have a high degree of confidence that a targeted person is directly participating in hostilities.

"An ADF member is exposed to criminal and disciplinary liability, including potentially the war crime of murder ... for opening fire on a person when there is a substantial risk that the person is not DPH," General David Hurley, then the CDF, wrote.

Given the potential consequences, it is perhaps unsurprising that — with the exception of one infamous incident — in more than a decade of Australian involvement in Afghanistan, not one Australian soldier appears to have been subjected to legal or disciplinary action over the killing of a civilian.

In May 2009, an internal inquiry found that Australian soldiers who killed three men during an assault on a compound were cleared despite the fact that one of the dead was hiding in a pile of chaff, another was running away from the compound and the third was hiding in a hay stack.

None of the three were armed, no weapons were found nearby and none of the eight Afghan men captured alive was questioned about the identities of the dead men.

The officer who carried out the inquiry did not travel to the scene or question the local inhabitants.

Despite all this, he determined the dead men "acted in a manner consistent with taking a direct part in hostilities."

When Australian SAS troopers hunting for the killer of three Australian soldiers in October 2012 killed two Afghan men, the Minister for Defence, David Johnston, was told in a briefing paper: "The scope of the legal concept of direct participation in hostilities ... is necessarily subjective in nature ... there is no compelling reason to second-guess the judgement of the soldiers involved."

On that occasion, one of the dead men, Mullah Janan Akhund, was seen talking on a radio as an Australian helicopter was about to land, then "assessed by SOTG members to be manoeuvring to gain tactical advantage through a covered position and potentially accessing a cache of weapons".

He was shot multiple times in the head and chest by two Australians, including Victoria Cross winner Ben Roberts-Smith.

The other man, Mullah Jalil Akhund, allegedly tried to wrest a weapon from an SAS trooper after being detained and was killed with "close range and deadly fire".

Nonetheless, the inquiry officer in that case did "identify a number of concerns in relation to the application of Australian ROE with respect to individuals taking a direct part in hostilities".

It was this incident that prompted General Hurley's warning to his troops that they could be tried for war crimes if they killed civilians without sufficient justification, and the clarification of rules of engagement that went out to all Australian forces in April 2013.

Civilian killings turning locals against troops

One other incident provides a window into the growing realisation that the killing of civilians was turning the local population against Australia and its allies.

On March 10, an Australian commando shot and killed a man on a motorcycle during an operation south-east of the main Australian base at Tarin Kowt. A female passenger was injured.

It was not until the provincial chief raised the incident a day later that Australian commanders realised their man had killed the Afghan motorcyclist.

A report on a subsequent meeting between Australian Special Forces personnel and the chief of police, Matiullah Khan, noted that he was agitated about "shooting civilians, especially females who do not target [Coalition Forces] or [Afghan National Security Forces]."

A later report compiled by a NATO investigation team noted that the local head of the Afghan national intelligence service, the NDS, "... echoed Matiullah Khan's sentiments, stating that Uruzgan citizens already blamed the National Directorate of Security for civilian casualty incidents arising from Special Operation raids."

The commando who killed the Afghan motorcyclist was cleared on the basis that intercepted communications revealed insurgents were active in the area, and the motorcyclist had exhibited behaviour — ignoring commands to stop and watching the Australian troops — that was consistent with "spotter" behaviour.

However, the author of the NATO report, an Australian officer, hinted that the patience of Afghan authorities with the killing of civilians might be wearing thin.

"The President of Afghanistan's recently declared delegation of responsibilities to Provincial security officials shows the national acceptance of [Afghan National Security Forces] as the lead security agency. This shift makes discretionary [Coalition] unilateral operations less acceptable to the Afghan population and [Government]," he wrote.

"This shift may also require a review of the burdens of proof as they pertain to the necessity of engaging spotters perceived to be directly participating in hostilities.

"The necessity of [special forces] to press the tactical advantage of the engagement needs to be weighed against the political disadvantage created by civilian casualty allegations against [Coalition forces] at this stage of the campaign."

It is not known if a formal review of Australia's Rules of Engagement took place following this recommendation.

Editor's note July 15, 2017: This article has been edited from the original published on Tuesday, July 11, 2017.

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read them.

Contact us on Signal: 0419 242 515

WhatsApp

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 #2 #3
Leaked documents expose deadly secrets of Australian special forces #3

#4 #5
The spy and the SAS soldier with a loaded Glock #5
Relations between Australia's special forces units on 'knife edge' #3

What the documents reveal about killings of unarmed Afghans

#6
Chaos over severed hands

#6
Chaos over severed hands

Header photo: Margaret Burin

'What the f*** are you doing': Chaos over severed hands

By the National Reporting Team's Dan Oakes and Sam Clark

Updated 11 Jul 2017, 10:25am Published 11 Jul 2017, 6:02am t was one of the most notorious incidents in Australia's recent military history — the severing of dead Taliban fighters' hands in Afghanistan.

When it was first revealed by the ABC in August, 2013, it caused a public furore and deep concern within Defence.

Now, for the first time, secret defence documents obtained by the ABC reveal the full story of how and why the "chopped hands" controversy came about.

The documents — one of which is marked "SECRET AUSTEO, INQUIRY IN CONFIDENCE" — reveal the incident caused bitter infighting within defence and sparked allegations of a "drift" in values within Australia's elite special forces.

REPORT OF THE INQUIRY OFFICER

INQUIRY INTO INCIDENT INVOLVING SENSITIVE SITE EXPLOITATION BY MEMBERS OF SOTG ON 28 APR 13

F69031

The documents state that on April 28, 2013, special forces were in search of a particular insurgent — an Australian National Priority Target codenamed Objective Rapier, a senior insurgent commander responsible for numerous attacks.

According to the documents, helicopters and a total of 120 soldiers were involved in the operation, including troops from the SAS and commandos.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of Australian special forces

An interrogation, a shooting and no witnesses

What the documents reveal about killings of unarmed Afghans

The spy and the SAS soldier with a loaded Glock

Who is the enemy? Australia's secretive rules of engagement

Chaos over severed hands

457

#2

Relations between Australia's special forces units on 'knife edge'

One of the SAS officers in the patrol was Captain Andrew Hastie, now a federal Liberal MP.

The documents say that during the fighting in the southern province of Zabul, four insurgents were killed.

An SAS corporal searched the first body, finding a Makarov pistol.

The report of the defence inquiry into the matter says: "[He] then severed a single hand of the EKIA (enemy killed in action) with a scalpel."

He repeated the process with two other EKIAs, cutting off their right hands.

Australian troops are required to collect fingerprints and eye scans of every Taliban fighter who is killed, if it is possible to do so.

But the mutilation or mistreatment of the bodies of the dead is a violation of the laws of war.

The report says: "In his evidence (the SAS corporal) said that once again he had severed the hands of EKIAs 2 and 3 of his own volition, as there was time pressure to retrieve the biometric material and to get back to the helicopters for extraction."

"At this point in time patrol commander (a sergeant) ... arrived at EKIA 3, and seeing the two hands on the ground, exclaimed words to the effect:

"What the f*** are you doing?"

Cutting off hands 'a tactical necessity'

The patrol commander told Defence investigators the soldier with the scalpel was "speechless" but a colleague replied: "This is a tactical necessity. This is a procedure to conduct latent fingerprints in the laboratory to take explosive residues."

The report states that Captain Hastie, then the commander of Troop B, observed a severed hand "at the site of the EKIA 3" and also asked what was going on.

When Captain Hastie and the sergeant returned to their base they discussed the incident at length and asked another SAS member to find out if the practice was permitted under Defence rules and regulations.

Cpt Hastie told his men not to sever any more hands and the next day reported the incident to his commanding officer.

The report paints a picture of confusion and growing alarm as news of what the SAS member had done began to radiate from the base at Tarin Kowt.

It says the solider "... exercised poor judgment, in that he failed to adequately appreciate the possible strategic consequences of those actions, in particular the potential responses from local nationals, (the Afghan Government), the Australian public and the media."

As the report makes clear, a training session just nine days before the patrol went out played a key and controversial role in what later transpired.

The training session was conducted by an Australian Defence Force Investigative Service (ADFIS) sergeant posted to Afghanistan as a crime scene officer as well as a civilian fingerprint expert. A number of SAS members and a Defence scientist also attended the session.

'You're sweet with us bringing back a hand?'

What was discussed remains hotly disputed.

Some SAS members claimed that the two experts explicitly sanctioned the removal of hands, one SAS trooper claiming that the experts described it as the "gold plate solution". Another said someone asked, "So you're sweet with us bringing back a hand?" to which the reply was, "Yes … you've got to do what you've got to do on the ground".

The Defence scientist who was present — described in the report as "possibly the most independent person at the training" — characterised the advice given by the experts as, "Here are a range of techniques that can be used to gather evidence from a scene. It's up to those guys, under the tactical situation that they're experiencing, to determine what is the most appropriate technique to use."

The civilian expert said he had only discussed body parts being examined in the context of "post-blast" investigations and denied ever discussing the severing of hands.

The ADFIS Sergeant said that when the subject of severing hands came up, he agreed that it would be a good method of securing fingerprints, but cautioned that the SAS members had to ask their superiors whether it was acceptable.

The sergeant also said he was not surprised the SAS members left the training thinking the severing of hands was legitimate, as "... that was all they were focused on".

This division between the SAS members and the experts who provided the briefing was reflected later in a letter from the commanding officer of the SAS Regiment to head of ADFIS, in which he accused ADFIS investigators of attempting to save the reputation of their colleague at the expense of the SAS.

"To be clear, I believe the ADFIS team were deliberately seeking to charge members of my team to prevent any adverse action on members of their own. This is a perception shared by persons outside my chain of command as well," the SAS officer wrote in October 2013.

As the inquiry progressed, it became clear that Australian troops in Afghanistan had not been explicitly instructed about whether the collection of body parts for biometric testing was acceptable.

New guidelines were quickly put in place emphasising that "the mutilation and otherwise maltreatment of human remains" is not permitted.

Despite this, the officer who carried out the inquiry wrote that some SAS members still sought clarification about whether the practice was acceptable in any circumstances.

"The above position could be attributed to a common desire by the members to support [the SAS trooper who severed the hands], following his employment of the technique. That type of support is not surprising considering the nature of the unit and its operations. However, the views expressed appeared to go beyond mere support for [him] and demonstrated a drift in values, or at least a degree of desensitisation."

Other, more senior personnel who were interviewed by the inquiry were less ambivalent.

Cpt Hastie is quoted as saying, "My gut instinct was okay, that's a strange practice." Another SAS member said, "There's no uncertainty. I wouldn't cut f***ing people's hands off, sir."

The inquiry officer said in conclusion that he could not identify what had caused any "value shift" in the SAS members, but noted that they regularly see dead and dismembered bodies, and themselves regularly killed and injured people.

"The significance of [this] is that these members require very clear direction in relation to what they can and can't do, and the members request as much," he wrote.

"Additionally, it would be imprudent for commanders to assume that these members are in a position to make value judgements, in a way that will align with the judgement of the commanders, and others."

More than four years after the incident, it is not clear if any disciplinary action was ever taken against the SAS trooper who severed the hands.

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read them.

Contact us on Signal: 0419 242 515

WhatsApp

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 #2 #3
Leaked documents expose deadly secrets of Australian special forces #4 #5
The spy and the SAS soldier with a loaded Glock #5 #6 Chaos over severed hands
Glock #6 Chaos over severed hands

#8 #8 #6 Chaos over severed hands

#8 NOW READING

#7

Relations between Australia's special forces units on 'knife edge'

Header photo: Margaret Burin



http://www.abc.net.au/news/2017-07-11/relations-between-australias-special-forces-units-unhealthy/8496616

They are the most celebrated and prestigious units in the Australian Army.

The SAS — the Special Air Service Regiment — and the 2nd Commando Regiment are Australia's special forces elite, the soldiers tasked with the most difficult missions in warzones like Afghanistan.

The Afghan Files

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#1 Leaked documents expose deadly secrets of Australian special forces	#2 An interrogation, a shooting and no witnesses	#3 What the documents reveal about killings of unarmed Afghans
#4 The spy and the SAS soldier with a loaded Glock	#5 Who is the enemy? Australia's secretive rules of engagement	#6 Chaos over severed hands
#7 Relations between Australia's special forces units on 'knife edge' NOW READING		

But now Defence Department documents leaked to the ABC reveal that relations between the two units — which also have a crucial role in domestic counter terrorism operations — were severely damaged by the war in Afghanistan.

The tensions between the SAS, based in Perth, and the commandos, based in Sydney, are revealed in letters written in 2013 by a former senior commando officer to the then Chief of Army, David Morrison and to Victoria Cross (VC) winner, SAS Corporal Mark Donaldson.

The letters from the senior officer, obtained by the ABC, were prompted by Corporal Donaldson's book, The Crossroad.

The book included details of operations involving the two units in which the VC winner criticised the conduct and professionalism of the commandos.

The two units operated alongside each other in Afghanistan as part of Australia's Special Operations Task Group on an operation called CASTNET.

The most controversial claim was that during an operation in Helmand Province, commandos used explosives to enter Afghan homes, after saying they wouldn't do so.

As a result Australian troops were exposed to attack from insurgents, Corporal Donaldson wrote.

'Extremely unhealthy' culture among teams

The former senior commando officer initially wrote to Corporal Donaldson saying he was "incredibly disappointed" with the criticisms, that they were not true and that the SAS had been told explosives were going to be used.

He told Corporal Donaldson: "Relationships between the two units are at an extremely unhealthy state ..."

"The culture of your unit, my unit and SOCMND (Special Operations Command) is on a perilous knife edge."

Receiving no reply, he wrote to General Morrison on November 25, 2013.

The former senior commando officer said the book contained factual errors.

"Furthermore it unfairly maligns officers and commandos and may place in doubt their role in effectively implementing Australian Government policy."

He said it "unjustly criticises the commando reputation and dishonours their service".

In doing so, he said, it "exacerbates a systemic internal cultural divide".

The book "appears to undermine the reputation of the 2nd Commando Regiment and therefore the ongoing trust and support of the nation to which we belong".

In his reply, General Morrison stressed the book was a personal memoir and not an official military history and that "a degree of editorial latitude" had to be given to the author.

He also said he was concerned about the former commando officer's comments about a "cultural divide" and that he would take this up with senior officers.

While in his letter to Corporal Donaldson, the former commando officer was critical of the book, he praised his army service and noted that the VC winner was a "truly humble and self-effacing individual".

He also said, rather curiously, "Furthermore I noted your VC is one in which there is no doubt that it was deserved".

A spokesperson for Pan Macmillan Australia, the publisher of The Crossroad, did not respond to a request for comment.

Got a confidential news tip?

Signal

A free, instant messaging and phone calling service. The content of the messages are encrypted end-to-end, meaning no-one but us can read

Contact us on Signal: 0419 242 515

WhatsApp

An instant messaging service owned by Facebook that offers end-to-end encryption. While the messages are private, WhatsApp stores some data like phone numbers and timestamps.

Contact us on WhatsApp: 0419 242 515

No system is 100 per cent secure, but these services can be used to protect your identity. Please read the terms and conditions of these services to work out the best method of communication for you.

The Afghan Files

#1

This is one story in a seven-part series based on leaked documents exposing Australian special forces troops' role in the Afghanistan war. For context, they are best read in order.

#2

http://www.abc.net.au/news/2017-07-11/relations-between-australias-special-forces-units-unhealthy/8496616

#3

9/14/2018	Relations between Australia's special forces units on 'a perilous knife edge' - ABC News (Australian Broadcasting Corporation)				
Leaked docum Australian spe	nents expose deadly secrets of cial forces		What the documents reveal about killings of unarmed Afghans		
#4 The spy and th Glock	ne SAS soldier with a loaded	#5 Who is the enemy? Australia's secretive rules of engagement	#6 Chaos over severed hands		
#7 Relations betw	veen Australia's special forces unit	s on 'knife edge'			

Header photo: Margaret Burin

Image:

7.30 Report

Afghan veteran raises disturbing allegations over the killing of civilians in Afghanistan

Posted Mon 10 Jul 2017, 8:23pm Updated Mon 10 Jul 2017, 8:23pm

A defence force insider tells 7.30 of a disturbing culture of recklessness and cover-up that he says emerged among an influential minority of Australian Special Forces in Afghanistan.

Transcript

plusminus

STAN GRANT, PRESENTER: Since 2001, the long military campaign in Afghanistan has cost the lives of 41 Australian soldiers. What we don't often hear about are the deaths of Afghan civilians.

Tonight, 7.30 exclusively reveals details of some of those deaths, and allegations that one of them was covered up by Australian Defence personnel - an insider who was asked to remain anonymous has told 7.30 of the disturbing culture that he says emerged among an influential minority of Australian Special Forces soldiers - a culture of recklessness and cover-up.

As Dan Oakes reports, a secretive military inquiry established last year to look into so-called rumours of unlawful killings is now investigating concrete information about a number of civilian deaths. A warning - this story contains an image of a deceased child.

(Gunfire)

(Choppy footage of war)

DAN OAKES, REPORTER: The challenges of waging war in Afghanistan are well-documented...

GLENN KOLOMEITZ, FORMER ARMY LAWYER: It's a very complex and highly ambiguous operating environment.

DAN OAKES: What isn't well-documented is that some Australian soldiers now stand accused of using that ambiguous environment to act outside the laws of war.

GLENN KOLOMEITZ: It's not like conflicts of the past, where you had a defined, uniformed enemy out in the field of battle with whom you engaged and the winner goes home.

DAN OAKES: Glenn Kolomeitz did two tours of Afghanistan as a legal officer advising Australian soldiers, and still represents veterans who have returned home.

GLENN KOLOMEITZ: It's important to remember here the vast majority of these soldiers - most, if not all - have some degree of post-traumatic stress disorder or mental-health conditions. In the course of running these cases for these soldiers, I have been made aware of possible breaches of the rules of engagement.

DAN OAKES: Do you know if any of these involve the killing of civilians.

GLENN KOLOMEITZ: Um, that's something I can't legally speak about.

DAN OAKES: Tonight, we reveal serious allegations that Australian soldiers may have committed unlawful killings during Australia's longest war, and claims that the death of an unarmed Afghan civilian was covered up.

ACTOR PORTRAYING ARMY WHISTLEBLOWER "CORPORAL JONES": I saw innocent people killed who didn't need to die or deserve to die, in circumstances that were unwarranted and, ultimately, avoidable.

DAN OAKES: This man is an actor. But the words he speaks are those of a highly decorated Australian veteran of the war in Afghanistan, who is not allowed to speak publicly, but can remain silent no longer.

We'll call him Corporal Jones.

Corporal Jones enlisted in the Australian Army in the 1990s, and soon set his sights on joining Australia's elite Special Forces.

"CORPORAL JONES": Special Forces was that avenue that pushed for perfectionism, professionalism, and obviously it was at the forefront of the military.

DAN OAKES: He got his wish, serving on multiple tours of Afghanistan, where Special Forces soldiers did some of the toughest and most lethal work of the war.

"CORPORAL JONES": If we look at the whole context of Afghanistan, it's a very remote, isolated environment to operate in.

(Blurry footage of soldiers running in Afghanistan)

SOLDIERS: Go, go, go!

DAN OAKES: Corporal Jones says an influential minority of Australian soldiers exploited that isolation, and his uneasiness with some of the things he witnessed them do has prompted him to speak publicly.

Ultimately, the behaviour of some elements of special operations led to indiscriminate, reckless and avoidable deaths of innocent civilians.

GLENN KOLOMEITZ: We were fighting an enemy who appeared to be a civilian. In fact, in the letter of the law, they were, in fact, civilians who were unlawfully taking part in the fight - so they dressed as civilians and would operate amongst the civilian population.

DAN OAKES: Glenn Kolomeitz saw firsthand how Australian troops in Afghanistan operated in combat, and gave them legal advice about what they could and couldn't do.

SOLDIER: Sweep down along that line...

GLENN KOLOMEITZ: The main role is to enable the commanders on the ground, in planning their operations, to conduct their operations within the bounds of the rules of engagement, of the law.

DAN OAKES: But Kolomeitz left Afghanistan in 2010, and missed the fallout on the ground of one of the most infamous moments of our war there.

(Excerpt from ABC News report from 2010)

JUANITA PHILIPS, PRESENTER: An Australian soldier has been charged with manslaughter over the deaths of five Afghan children and a male civilian.

DAN OAKES: The soldier charged was Lance Corporal David Millar. Millar was involved in a raid targeting a Taliban leader in February 2009. While under fire and acting on orders, he threw two grenades into a compound that housed an Afghan family.

Five children and a man were killed, a tragic outcome that still haunts David Millar.

DAVID MILLAR: I was horrified, numb, just... struggling to grasp...

DAN OAKES: However, the case fell over after Millar's lawyer successfully argued that the charges were defective.

But Corporal Jones says the fact that Millar had been charged in the first place angered troops in Afghanistan, and sent them a chilling message:

"CORPORAL JONES": Commanders in the field realised that even if they do the right thing, their guys could be held out and skinned alive. So as a result, the protectionism started to occur where civilian casualty incidents - which are unavoidable and unforeseeable in war - were not reported, and subsequently covered up to ensure the guys on the ground were protected.

DAN OAKES: Corporal Jones believes that once deaths started to be covered up by some Special Forces soldiers, it opened the door to the reckless killing of innocent civilians by Australians.

"CORPORAL JONES": These deaths were would ultimately go unreported. And if there was a circumstance where questions were raised over a death, they can be quite easily manipulated into believing they were legitimate engagements.

DAN OAKES: Corporal Jones is not alone. 7.30 has spoken to ten other former and current soldiers. Reluctant to break the code of secrecy expected of Special Forces, they wouldn't go on camera, but they agreed that a culture of recklessness infected some elements of Special Forces in Afghanistan around who was a legitimate target and who wasn't.

(Footage of live battle in Afghanistan)

Behind closed doors, Defence has called a full inquiry by its Inspector-General into the culture of Special Forces. It's understood the inquiry is investigating the killing of at least two children. Using a

number of sources, 7.30 has pieced together an account of one alleged killing that is being investigated by the Inspector-General.

(Night vision footage)

It was October 2012, in the sparsely populated back blocks of Kandahar province. With the help of their night-vision scopes, Australian troops were moving through the area, which was described by one person with knowledge of the incident as "a relatively benign environment".

The precise sequence of events that followed is still being investigated, but the pre-dawn calm was shattered by a volley of gunshots, allegedly from an Australian weapon.

(Gunfire)

A boy lay dead. 7.30 has been told these photographs were taken by the Australian troops who allegedly killed him. They recorded the precise location of his death and the position of his body among the rocks.

Photographing the bodies of Afghans killed was standard practice for Australian soldiers.

What wasn't standard practice is what allegedly happened next. 7.30 has been told the killing was never reported up the chain of command, despite no evidence that the boy was armed and, therefore, may have been a civilian.

When I was given these pictures, I decided to crosscheck the story I'd been told about what they depicted. So I engaged in a journalist in Afghanistan to find the family of the boy in the photos.

Six weeks ago, that journalist travelled to a town near where the boy was killed.

(An elderly Afghan man sitting on a rug looking at a photo of the dead boy)

JOURNALIST (translated): Is it him?

AFGHAN MAN (translated): Yes, if God wills, it is him.

DAN OAKES: This is Mossa Jan, a respected elder from the village. He says the boy in the photo was his nephew.

AFGHAN MAN (translated): He was a small boy, a small boy. He had no guilt, he had no sins.

We will be happy for (the soldier) to go to court.

Look at him with your own eyes, you can see it.

JOURNALIST: This photo was taken of the body; he is not alive.

DAN OAKES: Mossa Jan says the boy's name was Khan Mohammed. He was 14 or 15 years old, and he was killed by foreign troops while picking wild figs. He says no villagers heard the shooting, but his family believe he was killed during the day, just before his body was found.

However, an Australian source with knowledge of the incident - and the photographs - show the shooting happened at night.

According to Mossa Jan's account, Khan Mohammed's death was unjustified. So in an effort to find out whether there was a different version of these events, we asked Defence for information about the incident.

Remarkably, it said it had no record of a civilian casualty in that place at that time, despite the fact that the photographs were accompanied by GPS coordinates.

7.30 can reveal that, in addition to the Inspector-General, the Australian Federal Police, the body that investigates alleged war crimes, is now considering a full investigation of the killing of Khan Mohammed.

The Inspector-General's inquiry, headed by New South Wales Supreme Court Judge Paul Brereton, is being carried out in secret. It has all the powers of a royal commission. 7.30 understands that a number of former and serving soldiers have spoken to its investigators. Corporal Jones is one of them. He believes Australian authorities need to investigate.

"CORPORAL JONES": The locals don't have mechanisms to report. They are fearful. There's certainly no incentive for them to report. There's no mechanism in place for them to report these incidents. So that, in itself, is an enabler to facilitate these incidents.

DAN OAKES: Khan Mohammed's death isn't the only one under the spotlight of the Inspector-General. 7.30 has learnt that the inquiry is also looking into a second incident involving potential civilian casualties.

In September 2013, Australian soldiers shot and killed a man named Bizmillah Azadi during a compound clearance. As the soldiers searched his body, they found his wounded 6 year old son in blankets nearby. He died minutes later.

These deaths were reported. A classified inquiry has found that Azadi had pointed a pistol at the soldiers, and was probably a Taliban sympathiser. However, due to security concerns, the inquiry officer did not travel to the scene or interview the family of the dead. The soldiers were cleared of any wrongdoing.

With the help of the Afghan journalist, we contacted Bizmillah Azadi's family. They claimed he was unarmed and was not a Taliban member, and that Australian soldiers had apologised for the killing, saying they'd made a mistake.

Despite the classified inquiry clearing the soldiers involved, Defence has confirmed to 7.30 that the deaths of Azadi and his son have been referred to the Inspector-General.

Corporal Jones says, as the recklessness in Afghanistan spread, he became concerned by another disturbing development: the growing emphasis on the number of enemy killed in action.

"CORPORAL JONES": The measure of success for operations turned out to be more about body count - the kill count.

DAN OAKES: He says it was never official policy, but other former Special Forces soldiers have confirmed to 7.30 the kill count became a criterion of success, which they believe increased the chances of civilians being killed.

No commander would come out and say, "We need to raise our body count status for this trip." But every time a rotation was presented, or spoken about its measure of success, the first slide shown on any briefing would be the enemy killed in action.

DAN OAKES: 7.30 has uncovered a paper trail which shows that there were significant issues with the way that Australian soldiers were interpreting the rules of engagement in Afghanistan. Apparently prompted by an incident in 2012 in which Australians killed two unarmed mullahs, Defence Force Chief David Hurley issued an amplification of rules of engagement, stating Australian troops can only shoot if they had a high degree of confidence a civilian was participating in hostilities.

He said soldiers who killed civilians where there was doubt about whether they were directly participating in hostilities risked prosecution for the war crime of murder.

When we asked Defence about why the amplification was sent, a spokesperson said the rules of engagement were reviewed on an ongoing basis.

But Corporal Jones says that, by this stage, some Special Forces soldiers were, in fact, fabricating evidence with the use of drop weapons.

"CORPORAL JONES": If a person was engaged in questionable circumstances, it was easy enough to place a pistol with the body, take a photo of it, and then write it off as a legitimate battlefield kill.

DAN OAKES: Corporal Jones says that dropped weapons were often pistols carried by some Australian Special Forces troops on patrol for the purpose of creating evidence that a killing was justified after the fact. While Jones never witnessed a soldier plant such a weapon, he says their use was common knowledge amongst the troops.

"CORPORAL JONES": The carriage of drop weapons was common amongst some elements, and openly discussed in that forum.

DAN OAKES: 7.30 has confirmed with two other Afghanistan veterans that drop weapons were widely talked about by Australians on the ground. Former army lawyer Glenn Kolomeitz says any allegation about breaches of the rules of engagement should be thoroughly investigated, but warns against a witch-hunt targeting individual soldiers.

GLENN KOLOMEITZ: Many of these blokes are suffering from post-traumatic stress disorder or other mental health conditions as a result of what they've seen and what they've done. That context can't be ignored. They are our soldiers who have done a very demanding job for us in a very demanding operational theatre, and they need to be looked after, regardless of the allegations.

DAN OAKES: Corporal Jones says whether the inquiry finds evidence of unlawful killings or not, it's crucial that what he calls a culture of brutality and unaccountability is tackled head-on.

"CORPORAL JONES": By focusing on specific incidents, or specific individuals, we're only removing the tip of the iceberg; what lies beneath the water will be what sinks Special Operations command

Credits

Author <u>Dan Oakes</u>

· Author Sam Clark

7.30

- link Stories
- *link* About Us
- *link* Contact Us

Connect with 7.30

- 7.30 Facebook
- <u>7.30 Twitter</u>

Connect with Leigh Sales

- Leigh Sales Facebook
- @leighsales

Subscribe to Podcast

Catch up with RSS or on iview

21/09/2019



BENCH INFORMATION CHARGE

FOLDER: 200144

CC 18/41388 Case No:

For hearing on:

Defendant:

MCBRIDE, DAVID WILLIAM

- NFA

Alias:

Date of Birth:

15/12/1963

Occupation:

Informant:

BRUMBY, IAN/ROBERT

Act and Section under which proceedings taken order charge laid:

CTH - CRIMINAL CODE ACT 1995

Section:

131.1.01

OFFENCE THEFT

OFFENCE FROM: 01/01/2013

OFFENCE TO: 26/02/2018

Between about 1 January 2013 and about 26 February 2018 at Griffith and other places in the ACT, David William McBride did dishonestly appropriate property belonging to a Commonwealth entity with the intention of permanently depriving the entity of the property, contrary to s 131.1(1) of the Criminal Code (Cth).

BENCH INFORMATION/CHARGE

For Hearing on:

SEVENTH DAY OF MARCH, 2019 AT 09:45 IN THE FORENOON A.C.T. MAGISTRATES COURT IN THE AUSTRALIAN CAPITAL TERRITORY

Case No. CC2019/2900

Defendant:

DAVID WILLIAM MCBRIDE

NO FIXED ABODE

Date of Birth:

15 DEC 1963

Occupation:

PROCEEDINGS IN THIS MATTER WILL BE CARRIED ON BY THE DIRECTOR OF PUBLIC PROSECUTIONS UNDER THE PROVISIONS OF

SECTION 6 OF THE DIRECTOR OF PUBLIC

PROSECUTIONS ACT

Informant:

TURNER, PHILIP JAMES, Badge No. 10547

Date and Time apprehended: Charged Before Court

Bail Bond Number:

Act and Section under which proceedings taken or charge laid:

IN CONTRAVENTION OF SECTION 70(1) OF THE CTH - CRIMES ACT 1914

CCA070.01

OFFENCE

THAT HE, IN THE AUSTRALIAN CAPITAL TERRITORY, BETWEEN 14 APRIL 2016 AND ABOUT 31 MAY 2016, BEING A COMMONWEALTH OFFICER PUBLISHED ANY FACT OR DOCUMENT WHICH CAME INTO HIS KNOWLEDGE OR POSSESSION BY VIRTUE OF BEING A COMMONWEALTH OFFICER, AND WHICH IT IS HIS DUTY NOT TO DISCLOSE.

DATE ADJUDICATION:

BENCH INFORMATION/CHARGE

For Hearing on:

SEVENTH DAY OF MARCH, 2019 AT 09:45 IN THE FORENOON A.C.T. MAGISTRATES COURT

IN THE AUSTRALIAN CAPITAL TERRITORY

Case No. CC2019/2899

Defendant:

DAVID WILLIAM MCBRIDE

NO FIXED ABODE

Date of Birth:

15 DEC 1963

Occupation:

PROCEEDINGS IN THIS MATTER WILL BE CARRIED ON BY THE DIRECTOR OF PUBLIC PROSECUTIONS UNDER THE PROVISIONS OF

PROSECUTIONS UNDER THE PROVISIONS OF SECTION 6 OF THE DIRECTOR OF PUBLIC

PROSECUTIONS ACT

Informant:

TURNER, PHILIP JAMES, Badge No. 10547

Date and Time apprehended: Charged Before Court

Bail Bond Number:

Act and Section under which proceedings taken or charge laid:

IN CONTRAVENTION OF SECTION 73A(1) OF THE CTH - DEFENCE ACT 1903

DA073.001

OFFENCE

THAT HE, IN THE AUSTRALIAN CAPITAL TERRITORY, BETWEEN 14 APRIL, 2016 AND 01 OCTOBER, 2016 BEING A MEMBER OF THE DEFENCE FORCE, DID COMMUNICATE INFORMATION TO ANOTHER PERSON, NAMELY DANIEL OAKES AND THAT INFORMATION WAS A PLAN, DOCUMENT OR INFORMATION RELATING TO ANY NAVAL, MILITARY OR AIRFORCE INFORMATION AND THAT COMMUNICATION WAS NOT IN THE COURSE OF HIS DUTIES.

DATE ADJUDICATION:

BENCH INFORMATION/CHARGE

For Hearing on:

SEVENTH DAY OF MARCH, 2019 AT 09:45 IN THE FORENOON A.C.T. MAGISTRATES COURT IN THE AUSTRALIAN CAPITAL TERRITORY

Case No. CC2019/2898

Defendant:

DAVID WILLIAM MCBRIDE .

NO FIXED ABODE

Date of Birth:

15 DEC 1963

Occupation:

PROCEEDINGS IN THIS MATTER WILL BE

CARRIED ON BY THE DIRECTOR OF PUBLIC PROSECUTIONS UNDER THE PROVISIONS OF

SECTION 6 OF THE DIRECTOR OF PUBLIC

PROSECUTIONS ACT

Informant:

TURNER, PHILIP JAMES, Badge No. 10547

Date and Time apprehended: Charged Before Court

Bail Bond Number:

Act and Section under which proceedings taken or charge laid:

IN CONTRAVENTION OF SECTION 73A(1) OF THE CTH - DEFENCE ACT 1903

DA073.001

OFFENCE

THAT HE, IN THE AUSTRALIAN CAPITAL TERRITORY, BETWEEN 01 AUGUST, 2014 AND 31 DECEMBER, 2014 BEING A MEMBER OF THE DEFENCE FORCE, DID COMMUNICATE INFORMATION TO ANOTHER PERSON, NAMELY ANDREW CLARK AND THAT INFORMATION WAS A PLAN, DOCUMENT OR INFORMATION RELATING TO ANY NAVAL, MILITARY OR AIR FORCE INFORMATION AND THAT COMMUNICATION WAS NOT IN THE COURSE OF HIS DUTIES.

DATE ADJUDICATION:

BENCH INFORMATION/CHARGE

For Hearing on:

SEVENTH DAY OF MARCH, 2019 AT 09:45 IN THE FORENOON A.C.T. MAGISTRATES COURT IN THE AUSTRALIAN CAPITAL TERRITORY

Case No. CC2019/2897

Defendant:

DAVID WILLIAM MCBRIDE

NO FIXED ABODE

Date of Birth:

15 DEC 1963

Occupation:

PROCEEDINGS IN THIS MATTER WILL BE

CARRIED ON BY THE DIRECTOR OF PUBLIC PROSECUTIONS UNDER THE PROVISIONS OF

SECTION 6 OF THE DIRECTOR OF PUBLIC

PROSECUTIONS ACT

Informant:

TURNER, PHILIP JAMES, Badge No. 10547

Date and Time apprehended: Charged Before Court

Bail Bond Number:

Act and Section under which proceedings taken or charge laid:

IN CONTRAVENTION OF SECTION 73A(1) OF THE CTH - DEFENCE ACT 1903

DA073,001

OFFENCE

THAT HE, IN THE AUSTRALIAN CAPITAL TERRITORY, BETWEEN 01 AUGUST, 2014 AND 31 DECEMBER, 2014 BEING A MEMBER OF THE DEFENCE FORCE, DID COMMUNICATE INFORMATION TO ANOTHER PERSON, NAMELY CHRIS MASTERS AND THAT INFORMATION WAS A PLAN, DOCUMENT OR INFORMATION RELATING TO ANY NAVAL, MILITARY OR AIRFORCE INFORMATION AND THAT COMMUNICATION WAS NOT IN THE COURSE OF HIS DUTIES.

DATE ADJUDICATION:

IN THE SUPREME COURT OF THE AUSTRALIAN CAPITAL TERRITORY CRIMINAL JURISDICTION

No SCC 127 of 2019



THE QUEEN

against

DAVID WILLIAM MCBRIDE

THE COMMONWEALTH DIRECTOR OF PUBLIC PROSECUTIONS, who prosecutes in this behalf for Her Majesty the Queen, INFORMS THE COURT AND CHARGES THAT between about 1 December 2013 and about 26 February 2018, in Griffith and other places in the Australian Capital Territory and New South Wales, David William MCBRIDE, did dishonestly appropriate property belonging to a Commonwealth entity with the intention of permanently depriving the entity of the property, contrary to section 131.1 (1) of the *Criminal Code* (Cth).

2nd COUNT

AND FURTHER THAT between about 1 August 2014 and about 31 December 2015, in New Acton and other places in the Australian Capital Territory, David William MCBRIDE, being a member of the Defence force, did communicate information to another person, namely Chris MASTERS, and that information was a plan, document or information relating to any naval, military or air force information and that communication was not in the course of his duties, contrary to section 73A (1) of the *Defence Act 1903* (Cth).

3rd COUNT

AND FURTHER THAT between about 1 August 2014 and about 31 December 2015, in Forrest and other places in the Australian Capital Territory, David William MCBRIDE, being a member of the Defence force, did communicate information to another person, namely Andrew CLARK, and that information was a plan, document or information relating to any naval, military or air force information and that communication was not in the course of his duties, contrary to section 73A (1) of the *Defence Act 1903* (Cth).

4th COUNT

AND FURTHER THAT between about 4 April 2016 and about 31 May 2016, in Deakin in the Australian Capital Territory, David William MCBRIDE, being a Commonwealth officer, did publish a fact or document which came into his knowledge or possession by virtue of him being a Commonwealth officer and which it is his duty not to disclose, contrary to section 70 (1) of the *Crimes Act* 1914 (Cth).

5th COUNT

AND FURTHER THAT between about 2 May 2016 and about 11 July 2017, in Griffith and other places in the Australian Capital Territory, David William MCBRIDE, being a member of the Defence force, did communicate information to another person, namely Daniel OAKES, and that information was a plan, document or information relating to any naval, military or air force information

and that communication was not in the course of his duties, contrary to section 73A (1) of the *Defence Act 1903* (Cth).

DATED this & the day of August 2019

Rebekah Anne O'MEAGHER

For the Commonwealth Director of Public

Prosecutions

IN THE SUPREME COURT OF THE AUSTRALIAN CAPITAL TERRITORY CRIMINAL JURISDICTION

Cor

Date of Plea ...

WITNESSES:

No. SCC 127 of 2019

THE QUEEN

Against

DAVID WILLIAM MCBRIDE

JURORS

INFORMATION FOR

- CC2018/41388 theft Criminal Code (Cth) s 131.1 (1)
 CC2019/2897 unlawfully giving or obtaining information as to defences Defence Act 1903
- (Cth) s 734 (1) s 738 (1)
- (Cth) s 73A (1)

 4. CC2019/2900 disclosure of information by Commonwealth officers *Crimes Act 1914* (Cth) s 70 (1)
 - 5. CC2019/2899 unlawfully giving or obtaining information as to defences *Defence Act 1903* (Cth) s 73A (1)

10.

6

ω.

12.

Verdict		Date of Sentence		Sentence		

March 7 2019 - 1:39PM

'I'm not afraid of going to jail': Ex-Defence lawyer charged over document leak

Alexandra Back

Crime

A former Australian military lawyer and captain in Britain's elite Special Air Service has been charged over the leak of documents exposing alleged unlawful government conduct.

David William McBride, 55, appeared in the ACT Magistrates Court on Thursday where he was charged with the leaks to journalists Dan Oakes, Andrew Clark and Chris Masters.



Whistleblower David William McBride has been charged for leaking defence documents to journalists. Photo: Alexandra Back

He has not entered any pleas.

The charges relate in part to an ABC investigation published in 2017 called "The Afghan Files: Defence leak exposes deadly secrets of Australia's special forces".

The investigation was said to give an unprecedented insight into the clandestine operations of Australia's special forces, including incidents of possible unlawful killings.

Speaking outside court, Mr McBride said he had admitted handing over the documents but would defend the charge on legal grounds.

"I saw something illegally being done by the government and I did something about it," he said.

"I'm seeking to have the case looking purely at whether the government broke the law and whether it was my duty as a lawyer to report that fact."

Mr McBride is charged with theft and three counts of breaching the Defence Act, for being a person who is a member of the the defence force and communicating a plan, document or information.

The charges, if prosecuted on indictment, attract an unlimited fine or imprisonment for any term as the maximum penalties.

If dealt with summarily the penalties are six months in prison or a small fine.

Mr McBride faces a further charge under old secrecy provisions in the federal Crimes Act, which make it an offence for a Commonwealth official to disclose information without authorisation.

That law has since been revoked and replaced in the Criminal Code, broadening its scope and increasing the penalties that apply in certain cases.

Mr McBride said he first sought an internal inquiry through defence and then went to police. When police did not act he went to the media.

Mr McBride said he gave the documents to the ABC, the Sydney Morning Herald and Chris Masters but only the ABC published a report.

The prosecution of Mr McBride will draw inevitable comparisons with that of the former Australian spy Witness K and his lawyer Bernard Collaery.

The pair are also being pursued by the Commonwealth Director of Public Prosecutions accused of revealing information about the Australian Secret Intelligence Service.

Witness K revealed an illegal bugging operation by the Australian government on East Timor during negotiations over an oil and gas treaty.

The pair face a maximum two years in jail if found guilty, a penalty since increased to 10 years. National security claims over the brief of evidence have delayed the defence access to it and the case's progress.

A preliminary hearing for that case will be heard in secret.

On Thursday, a Legal Aid lawyer for Mr McBride told the court some of the relevant material was classified and his office was having difficulty finding a lawyer with the necessary clearance.

The one option so far was the director of the service Dr John Boersig, the lawyer Hugh Jorgensen said.

Mr McBride said the government's claim of classified material was a smokescreen and there was no reason why the case shouldn't be held in the open.

Mr McBride said he had been living in Spain when he was arrested at the airport in Sydney on his way home in September last year.

Aware of the risk of arrest, he had returned home to attend a father daughter dance.

Mr McBride studied at Sydney University before going to Oxford. He then joined the British army, spending six years with the Blues and Royals, the Queen's household cavalry.

He also served with the SAS and did tours of duty in Northern Ireland and Afghanistan.

"I have a duty to look after Australia, if that means reporting illegal activity by the top brass of the ADF I'm going to do it, I'm not afraid of going to jail," he said.

"If I was afraid of going to jail, why would I have been a soldier?"

He is next due in court on May 13.

May 31 2019 - 11:42AM

Ex-Defence whistleblower charged over leak to journalists committed to stand trial

• Alexandra Back

Crime

The case of a former Australian military lawyer charged over the leak of documents to journalists was committed on Thursday to stand trial in the ACT Supreme Court.

David William McBride, 55, is accused of theft and three counts of breaching the Defence Act, for being a person who is a member of the defence force and communicating a plan, document or information, an offence that carries and unlimited fine or prison time as penalty when heard on indictment. He is also charged under old secrecy provisions in the federal Crimes Act, which make it an offence for a Commonwealth official to disclose information without authorisation.



Whistleblower David William McBride has been charged for leaking defence documents to journalists.

The leaks were to journalists Dan Oakes, Andrew Clark and Chris Masters. The charges relate in part to an ABC investigation published in 2017 called "The Afghan Files: Defence leak exposes deadly secrets of Australia's special forces."

Mr McBride has pleaded not guilty to all charges. He does not deny passing information on but will defend the charge on legal grounds. He said on an earlier occasion: "I saw something illegally being done by the government and I did something about it."

He was previously represented by Legal Aid, but appeared in court on Thursday representing himself. He told The Canberra Times of concerns about his Legal Aid lawyers being permitted to access the necessary documents, and his discomfort in using a large amount of the organisation's resources, for what could be a long period of time.

The ACT Magistrates Court heard on Thursday that Mr McBride would consent to a set of orders proposed by the Commonwealth attorneygeneral under the national security information laws that will govern how sensitive material is handled during the case.

Once the consent orders are made Mr McBride will be able to access the brief, the court heard.

Chief Magistrate Lorraine Walker committed the case for trial in the ACT Supreme Court.

The first directions hearing in the higher court is listed for June 13.

The Guardian



This article is more than 1 month old

Afghan Files whistleblower David McBride's trial delayed to protect state secrets

Prosecutor says agreement must be reached about how to deal with 'national security information' in case

Paul Karp

Thu 13 Jun 2019 12.49 AEST

Former defence lawyer David McBride has still not seen a full brief of evidence against him, as his trial for blowing the whistle on alleged unlawful killing in Afghanistan will be delayed to protect state secrets.

At a hearing in Canberra on Thursday, the crown prosecutor revealed that despite being committed for trial two weeks ago, McBride is in the "unusual position" of not having the full brief because an agreement must first be reached about how to deal with "national security information" in the case.

McBride is facing five charges of leaking classified material to three senior journalists at the ABC and the then Fairfax Media newspapers, which formed the basis of "The Afghan Files", an ABC expose in 2017 revealing allegations of serious misconduct by Australian special forces in Afghanistan.

McBride does not dispute leaking the material but will argue that he was acting on his duty to report illegal conduct by the government.

Outside the court McBride complained that the case is "not about secrets, it's about lies". But inside the supreme court, where he is self-represented, McBride raised no objections to proposed orders to determine the bounds of national security information "in chambers" – in private with the judge – before he receives the full brief.

Counsel for the attorney general said this would allow the case to proceed "in a way that doesn't compromise security or defence".

McBride told reporters that, despite being arrested nine months ago, he had not seen a full brief of evidence and claimed "that means they don't have a case against me yet".

He explained he had not objected to a private determination on national security information because "it may take forever for that side issue to run".

"I've decided that I have faith in the judiciary of this country and if it means we have to have a closed court I'm prepared to have a closed court."

McBride vowed that he would "never take a plea" despite it being "suggested to me before".

McBride said he was afraid of his "conscience", which he said had "almost killed me in the past for things I did do, [that I] shouldn't have done" but the prospect of jail did not, despite acknowledging it is "going to be bad".

"It was very bad the one night I spent there - but I can't do the wrong thing just for selfish motives."

McBride said the case was not about information that was "truly national security" related.

"None of it is about our secret mind-reading powers - it's all about what happened 10 years ago on a mountaintop in Afghanistan ... it's not national security, it's just nationally embarrassing."

The case was adjourned until 27 June for a further mention.

More people in Australia...

... like you, are reading and supporting The Guardian's independent, investigative journalism than ever before. And unlike many new organisations, we have chosen an approach that allows us to keep our journalism accessible to all, regardless of where they live or what they can afford. But we need your ongoing support to keep working as we do.

The Guardian will engage with the most critical issues of our time - from the escalating climate catastrophe to widespread inequality to the influence of big tech on our lives. At a time when factual information is a necessity, we believe that each of us, around the world, deserves access to accurate reporting with integrity at its heart.

Our editorial independence means we set our own agenda and voice our own opinions. Guardian journalism is free from commercial and political bias and not influenced by billionaire owners or shareholders. This means we can give a voice to those less heard, explore where others turn away, and rigorously challenge those in power.

We need your support to keep delivering quality journalism, to maintain our openness and to protect our precious independence. Every reader contribution, big or small, is so valuable. **Support The Guardian from as little as \$1 - and it only takes a minute. Thank you.**

Support The Guardian









Topics

- Law (Australia)
- Australian Broadcasting Corporation
- Australian media
- Fairfax Media
- news

Transcript of video uploaded to the website of the *Gold Coast Bulletin*, titled *"RAW: Whistleblower David McBride speaks outside court"*, dated 18 July 2019, available at the following URL: https://www.goldcoastbulletin.com.au/news/national/raw-whistleblower-david-mcbride-speaks-outside-court/video/1cc9e8e46602db9e9b322e7263989491

Why they won't declassify these documents. They're over 10 years old in most cases. There is no reason that any of our enemies could use them against us. It's impossible. And I want the government to tell Australia what they are hiding.

Q: So do you have any idea what will be in the brief of evidence, who the witnesses will be?

I know exactly what'll be in the brief of evidence. It'll be documents that I gave to the journalists and some that I didn't, which I felt helped proved my case. The witnesses will largely be Defence officials saying that they did a check of the computer systems and they can prove that these are the documents which I printed off. Hopefully a lot of that we won't need to test in court. I will just got (sic) to admit it and say yes I did take the documents from the system. If they do have any senior leadership witnesses, which I doubt, but if they do, that'll be good because I'd like to cross examine them.

Q: Do you think the journalist will be actively involved in the crown's case?

According to the directions at the moment, no they can't be, because the definition of national security information is extremely wide. It's things you learn in basic training at Kapooka which are not obviously anything to do with national security, where the mess all is. Everything that has got any kind of military designation is considered too hot for journalists to hear, and that's got to be wrong. And in the meantime, I may be applying either to the High Court or the most appropriate court to compel the feds to sensibly reclassify that information.

Q: Will you still be representing yourself?

Yes, I think I'm going to keep representing myself. As I said, I want to take the battle to Defence. I've already admitted I gave the documents. My justification is that it was my duty to do so because the government was breaking the law and my duty is to the people of Australia, not to the government of Australia. I haven't met a lawyer yet who is prepared to take them on. Maybe Amal Clooney if she's available but presumably she's not. I can't afford her, so I'll do it myself.

Q: Can I ask a basic question about – so you admit that you gave those documents to ABC journalists but you are pleading not guilty.

That's right. Because the offence is not giving the documents to the journalist. The offence [someone says something which is inaudible] yes that's right. Not guilty because the offence is not the fact that I gave the documents to the journalist. The fact – the essence of the offence is that I damaged national security and it wasn't my duty to do so. Now, firstly I'd say I didn't damage national security; I acted in the interests of national security. If the government breaks the law, if the government commits war crimes, it's actually a duty of a lawyer and an officer to speak up about it.



13 September 2018

Daniel Oakes
Senior Reporter
ABC National Reporting Team
Via email: Oakes.Daniel@abc.net.au

Dear Mr Oakes,

I write to you regarding a matter currently under investigation by the Australian Federal Police (AFP) relating to the alleged unauthorised disclosure, communication and receipt of classified Australian Defence Force (ADF) documents and information.

An investigation was commenced following a referral to the AFP from the then Chief of the Defence Force (Air Chief Marshal Mark Binskin) and the then acting Secretary for Defence (Phillip Prior) dated 11 July 2017. A number of classified documents and information central to the allegations were featured in ABC articles co-authored by yourself and Mr Samuel Clark, namely:

- Inside the Afghan Files (ABC promotional video dated 10 July 2017;
- Rules of Engagement (ABC 7.30 report dated 10 July 2017; and
- The Afghan Files (ABC internet series dated 11 July 2017).

The classified documents and information was not authorised for release or disclosure. I can confirm you are a suspect in relation to the following alleged offences:

- Receiving prescribed information, contrary to section 79(6) of the Crimes Act 1914 (Cth)
- Unlawfully obtaining information as to defences, contrary to section 73A(2) of the Defence Act 1903 (Cth).

The AFP are now requesting for you to participate in a formal record of interview under criminal caution and rights in respect of these allegations. You are under no obligation to take part in an interview. You may seek legal advice to assist your decision.

Luculd appreciate if you or your logal	representative could advice Endoral Agent Ion Brumby on
(02) or via email at	representative could advise Federal Agent Ian Brumby on and Federal Agent Philip Turner on (02)
or via email at	of your decision within seven (7) days of
receiving this correspondence.	
Yours sincerely	
Andrew Smith	
Detective Superintendent	
Offshore and Sensitive Investigations	
Crime Operations	

CRIME OPERATIONS - OSI
47 Kings Avenue Barton ACT 2601

Australian Federal Police Telephone: (02) afp.gov.au ABN 17 864 931 143 Email:



13 September 2018

Samuel Clark

Producer

ABC National Reporting Team

Via email: Clark.Samuel@abc.net.au

Dear Mr Clark,

I write to you regarding a matter currently under investigation by the Australian Federal Police (AFP) relating to the alleged unauthorised disclosure, communication and receipt of classified Australian Defence Force (ADF) documents and information.

An investigation was commenced following a referral to the AFP from the then Chief of the Defence Force (Air Chief Marshal Mark Binskin) and the then acting Secretary for Defence (Phillip Prior) dated 11 July 2017. A number of classified documents and information central to the allegations were featured in ABC articles co-authored by yourself and Mr Daniel Oakes, namely:

- Inside the Afghan Files (ABC promotional video dated 10 July 2017;
- · Rules of Engagement (ABC 7.30 report dated 10 July 2017; and
- The Afghan Files (ABC internet series dated 11 July 2017).

The classified documents and information was not authorised for release or disclosure. I can confirm you are a suspect in relation to the following alleged offences:

- Receiving prescribed information, contrary to section 79(6) of the Crimes Act 1914 (Cth)
- Unlawfully obtaining information as to defences, contrary to section 73A(2) of the Defence Act 1903 (Cth).

The AFP are now requesting for you to participate in a formal record of interview under criminal caution and rights in respect of these allegations. You are under no obligation to take part in an interview. You may seek legal advice to assist your decision.

(02)	or via email at	and Federal Agent Philip Turner on (02)
	or via email at	of your decision within seven (7) days of
receiving	this correspondence.	-
Yours sinc	cerely	

Andrew Smith
Detective Superintendent
Offshore and Sensitive Investigations
Crime Operations

CRIME OPERATIONS - OSI 47 Kings Avenue Barton ACT 2601 Australian Federal Police Telephone: (02) afp.gov.au ABN 17 864 931 143 Email:



13 September 2018

Gaven Morris
Director News, Analysis and Investigations
Australian Broadcasting Corporation
Via email: Morris.Gaven@abc.net.au

Dear Mr Morris,

I write to you regarding a matter currently under investigation by the Australian Federal Police (AFP) relating to the alleged unauthorised disclosure, communication and receipt of classified Australian Defence Force (ADF) documents and information.

An investigation was commenced following a referral to the AFP from the then Chief of the Defence Force (Air Chief Marshal Mark Binskin) and the then acting Secretary for Defence (Phillip Prior) dated 11 July 2017. A number of classified documents central to the allegations were featured in ABC articles co-authored by Mr Daniel Oakes and Mr Samuel Clark, namely:

- Inside the Afghan Files (ABC promotional video dated 10 July 2017;
- Rules of Engagement (ABC 7.30 report dated 10 July 2017; and
- The Afghan Files (ABC internet series dated 11 July 2017).

The AFP is aware of communications between yourself and Brigadier Chris Smith (then Chief of Staff to the Chief of the Defence Force) in relation to the aforementioned ABC reporting. Investigations into this matter are on-going, however the AFP are now seeking your assistance as a witness, to provide a statement and any associated supporting material in respect of those communications.

Any assistance you may provide would be on a voluntary basis. There is no legal obligation for you to provide a statement, however any assistance would be appreciated. AFP investigators are in a position to facilitate the taking of any statement at a place and time convienient to you.

I would ap	preciate if you or your legal re	presentative could advise Federal Agent Ian Brumby on
(02)	or via email at	and Federal Agent Philip Turner on (02)
	or via email at	of your decision within seven (7) days of
receiving t	this correspondence.	

Yours sincerely

Andrew Smith
Detective Superintendent
Offshore and Sensitive Investigations
Crime Operations

CRIME OPERATIONS - OSI 47 Kings Avenue Barton ACT 2601 Australian Federal Police Telephone: (02) afp.gov.au ABN 17 864 931 143

Email:



Our Ref: 18432 Your Ref:

4 October 2018

Federal Agent Ian Brumby Australian Federal Police 47 Kings Avenue BARTON ACT 2601

By email:

Dear Mr Brumby

ABC publications concerning "The Afghan Files"

We refer to our letter dated 18 September 2018.

Mr Oakes and Mr Clark decline your request for an interview. In addition, in the circumstances, Mr Morris respectfully declines your request to assist the investigation.

Yours sincerely

Michael Rippon Senior Lawyer

ABC Legal

E: rippon.michael@abc.net.au

Genevieve Hartney

From: BRUMBY, Ian

Sent: Thursday, 24 January 2019 2:52 PM

To: Michael Rippon

Subject: AFP Investigation - ABC publications concerning "The Afghan Files" [SEC=UNCLASSIFIED]

Follow Up Flag: Follow up Flag Status: Flagged

UNCLASSIFIED

Good afternoon Michael,

Thank you for taking the time to speak today.

As discussed, the AFP investigation with regards to the Afghan Files and associated publications in ongoing. We are currently at a point where the AFP will seek the issuance of 3E Search Warrants to be executed on ABC premises, for material which we believe will provide evidence of indictable offences against the laws of the Commonwealth.

To expedite this process and create minimal interference to the ABC, it's premises and staff, I propose that the manner of how we execute the warrant be similar to other organisations that are prepared to assist, that being –

- 1. You respond to this email agreeing to provide assistance as would be required by the search warrant; namely search ABC premises for any material that satisfies the conditions to be specified in the warrant and collate any such material that may be found, and any other material found at the premises in the course of the search where there are reasonable grounds to believe it is evidential material in relation to an offence to which the warrant will relate.
- 2. I will then forward a copy of the conditions of the warrant which describe what we would be seeking from the ABC.
- 3. We would seek your agreeance on a date range of between 2 3 weeks to allow for the collation of material.
- 4. When we are notified that all material relevant to the warrant has been collected, AFP members would attend at the ABC Head Office in Sydney and provide the sworn warrant and obtain the material sought under the search warrant.

If you are happy with this proposal, could you please advise and I will endeavour to provide a copy of the warrant conditions as soon as possible. We are not seeking any material from the ABC outside of that identified in the search warrant.

If you have any questions or concerns at any point, please feel free to contact me.

Regards,

Ian

FEDERAL AGENT IAN BRUMBY

OFFSHORE AND SENSITIVE INVESTIGATIONS CRIME OPERATIONS
Tel +61(0) 2 www.afp.gov.au



POLICING FOR A SAFER AUSTRALIA

UNCLASSIFIED

WARNING

This email message and any attached files may contain information that is confidential and subject of legal privilege intended only for use by the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the message to the intended recipient be advised that you have received this message in error and that any use, copying, circulation, forwarding, printing or publication of this message or attached files is strictly forbidden, as is the disclosure of the information contained therein. If you have received this message in error, please notify the sender immediately and delete it from your inbox.

AFP Web site: http://www.afp.gov.au

Genevieve Hartney

From: BRUMBY, Ian

Sent: Monday, 1 April 2019 2:34 PM

To: Michael Rippon

Subject: AFP Investigation - The Afghan Files [SEC=UNCLASSIFIED]
Attachments: AFP Letter (2) - Daniel Oakes.pdf; AFP Letter (2) - Samuel Clark.pdf

Importance: High

Follow Up Flag: Follow up Flag Status: Completed

UNCLASSIFIED

Good afternoon Michael,

Please find attached two requests for your clients, Messrs Daniel Oakes and Samuel Clark, to consent to a forensic procedure (finger and palm prints).

I will be out of the office for the next month, however if you could please notify Detective Sergeant Matt Neesham or Federal Agent Phil Turner of your clients decision within the next 7 days, that would be appreciated.

Regards,

Ian

FEDERAL AGENT IAN BRUMBY

OFFSHORE AND SENSITIVE INVESTIGATIONS CRIME OPERATIONS
Tel +61(0) 2
www.afp.gov.au



POLICING FOR A SAFER AUSTRALIA

UNCLASSIFIED

WARNING

This email message and any attached files may contain information that is confidential and subject of legal privilege intended only for use by the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the message to the intended recipient be advised that you have received this message in error and that any use, copying, circulation, forwarding, printing or publication of this message or attached files is strictly forbidden, as is the disclosure of the information contained therein. If you have received this message in error, please notify the sender immediately and delete it from your inbox.

AFP Web site: http://www.afp.gov.au



1 April 2019

Mr Daniel Oakes Senior Reporter ABC National Reporting Team

By email: rippon.michael@abc.net.au

Dear Mr Oakes,

Further to the letter from Detective Superintendent Andrew Smith, dated 13 September 2018, regarding the alleged unauthorised receipt of classified Australian Defence Force (ADF) documents and information.

I am satisfied on the balance of probabilities that you are a suspect for an indictable offence, namely:

- Receiving prescribed information, contrary to section 79(6) of the Crimes Act 1914 (Cth);
- Unlawfully obtaining information as to defences, contrary to section 73A(2) of the Defence Act 1903 (Cth); and
- Receiving, contrary to section 132.1(1) of the Criminal Code Act 1995 (Cth)

As such, I am requesting your consent to a forensic procedure being the copying of your finger and palm prints.

There are reasonable grounds to believe that this forensic procedure is likely to produce evidence tending to confirm or disprove that you committed the indictable offence, and forensic material has been recovered from documents which can be compared to the forensic material to be obtained by this procedure.

Under the Crimes Act 1914, I am satisfied that the request for consent is justified in all the circumstances.

You may refuse to consent to the carrying out of the forensic procedure. If you do not consent, an application may be made to a Magistrate by the Australian Federal Police for an order authorising the carrying out of the forensic procedure.

If you refuse to give consent, fail to give consent, or withdraw your consent to the forensic procedure, evidence of this refusal or failure to consent is not admissible in proceedings against you, except to establish or rebut an allegation that police or another person involved in the investigation acted contrary to law in carrying out that investigation.

CRIME OPERATIONS

GPO Box 401, Canberra ACT 2601

Australian Federal Police Telephone: 02 ABN 17 864 931 143

Email:

Should you consent to the carrying out of the forensic procedure, arrangements will be made for you to attend the AFP Melbourne Office at a convenient time and date.

I would appreciate if you or your legal representative could advise Federal Agent Phil Turner via email at or Detective Sergeant Matt Neesham via email at of your decision within seven (7) days of receiving this correspondence.

Should you have any questions about the foregoing, please do not hesitate to contact me.

Yours sincerely

lan Brumby

Ian Brumby
Federal Agent
Offshore and Sensitive Investigations
Crime Operations
Australian Federal Police

CRIME OPERATIONS
GPO Box 401, Canberra ACT 2601

Australian Federal Police Telephone: 02 afp.gov.au ABN 17 864 931 143 Email:



1 April 2019

Mr Samuel Clark Producer ABC National Reporting Team

By email: rippon.michael@abc.net.au

Dear Mr Clark,

Further to the letter from Detective Superintendent Andrew Smith, dated 13 September 2018, regarding the alleged unauthorised receipt of classified Australian Defence Force (ADF) documents and information.

I am satisfied on the balance of probabilities that you are a suspect for an indictable offence, namely:

- Receiving prescribed information, contrary to section 79(6) of the Crimes Act 1914 (Cth);
- Unlawfully obtaining information as to defences, contrary to section 73A(2) of the *Defence Act 1903 (Cth);* and
- Receiving, contrary to section 132.1(1) of the Criminal Code Act 1995 (Cth)

As such, I am requesting your consent to a forensic procedure being the copying of your finger and palm prints.

There are reasonable grounds to believe that this forensic procedure is likely to produce evidence tending to confirm or disprove that you committed the indictable offence, and forensic material has been recovered from documents which can be compared to the forensic material to be obtained by this procedure.

Under the Crimes Act 1914, I am satisfied that the request for consent is justified in all the circumstances.

You may refuse to consent to the carrying out of the forensic procedure. If you do not consent, an application may be made to a Magistrate by the Australian Federal Police for an order authorising the carrying out of the forensic procedure.

If you refuse to give consent, fail to give consent, or withdraw your consent to the forensic procedure, evidence of this refusal or failure to consent is not admissible in proceedings against you, except to establish or rebut an allegation that police or another person involved in the investigation acted contrary to law in carrying out that investigation.

CRIME OPERATIONS

GPO Box 401, Canberra ACT 2601

Australian Federal Police
Telephone: 02

afp.gov.au

ABN 17 864 931 143

Should you consent to the carrying out of the forensic procedure, arrangements will be made for you to attend the AFP Melbourne Office at a convenient time and date.

I would appreciate if you or your legal representative could advise Federal Agent Phil Turner via email at or Detective Sergeant Matt Neesham via email at of your decision within seven (7) days of receiving this correspondence.

Should you have any questions about the foregoing, please do not hesitate to contact me.

Yours sincerely

Crime Operations

Australian Federal Police

Ian Brumby
Federal Agent
Offshore and Sensitive Investigations

CRIME OPERATIONS
GPO Box 401, Canberra ACT 2601

Australian Federal Police Telephone: 02 afp.gov.au

ABN 17 864 931 143 Email:

COMMONWEALTH OF AUSTRALIA

CRIMES ACT 1914: SECTION 3E

SEARCH WARRANT FOR SEARCH OF A PREMISES



To: Ian Robert Brumby a constable within the meaning of the *Crimes Act 1914*, who is the executing officer in relation to this warrant;

And to any other constable whose name may be written on this warrant in accordance with section 3C(1) of the *Crimes Act 1914*, in which event that constable shall be the executing officer in relation to this warrant:

Whereas I	Martin Kane	
	Registrar	

an issuing officer within the meaning of section 3E of the *Crimes Act 1914*, am satisfied by information on oath that there are reasonable grounds for suspecting that there is (or will within the next 72 hours be) at the premises located at:

The Australian Broadcasting Corporation (ABC), ABC Ultimo Centre, 700 Harris Street, Ultimo in the State of New South Wales

evidential material, as defined in the *Crimes Act 1914*, which satisfies ALL of the following three conditions namely:

First condition: Things which are:

originals or copies of any one or more of the following, including any of them which are stored on a computer, or on a computer storage device, or on any other type of storage medium or storage device:

- Handwritten/digital notes
- Diary/ies
- Correspondence internal and external
- · Emails and other electronic forms of messaging
- Minutes
- Reports
- · Briefing Documents
- Assessments
- Graphics, sketches, photographs or imagery/vision drafts and final
- Story pitch
- Planning logs
- Broadcast and online schedules
- Raw or unedited footage in its entirety

- · Journalist's piece to camera
- Scripts drafts and finals including voice overs
- Story boards/plans
- Status updates
- Website content
- · Documents classified as 'Secret'

Together with any manual, instruction, password or other thing that assists to gain access to or interpret or decode any of the above things.

Second condition: And which relate to any one or more of the following:

- David McBRIDE
- Daniel (Dan) OAKES
- Samuel (Sam) CLARK
- Gaven MORRIS
- Chris SMITH
- Australian Broadcasting Corporation (ABC)
- National Reporting Team
- Australian Defence Force (ADF)
- Department of Defence
- The Australian Army
- Special Forces
- Special Operations Command (SOCOMD)
- Special Operations Task Group (SOTG)
- Special Air Service Regiment (SASR)
- 2nd Commando Company (2CDO)
- Headquarters Joint Operations Command (HQJOC)
- Operation SLIPPER
- Afghanistan
- The 7.30 Report
- The Afghan Files
- Inside the Afghan Files
- Rules of Engagement
- The Ops Room
- Ghost Three Zero
- Chief of the Defence Force (CDF)
- · Acting (and/or) Secretary of Defence
- Chief of Army (CA)

- Chief of Joint Operations (CJOPS)
- http://theopsroom.com
- https://www.abc.net.au/news/2017-07-11/inside-the-afghan-files/8696182
- https://www.facebook.com/abcnews.au/videos/inside-the-afghan-files/10156950722999988/
- https://www.abc.net.au/7.30/afghan-veteran-raises-disturbing-allegationsover/8695400
- https://www.abc.net.au/news/2017-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642
- https://www.abc.net.au/news/2017-07-11/defence-inquiry-investigatingkilling-of-taliban-detainee-in-hut/8616602
- https://www.abc.net.au/news/2017-07-11/unarmed-men,-children-amongcasualties-of-elite-forces/8424944
- https://www.abc.net.au/news/2017-07-11/the-spy-and-the-sas-solider-with-a-loaded-glock/8496608
- https://www.abc.net.au/news/2017-07-11/afghan-files-australias-secretiverules-of-engagement/8496672
- https://www.abc.net.au/news/2017-07-11/afghan-files-shed-light-onnotorious-severed-hands-case/8496654
- https://www.abc.net.au/news/2017-07-11/relations-between-australiasspecial-forces-units-unhealthy/8496616

Third condition:

And as to which there are reasonable grounds for suspecting that they will afford evidence as to the commission of the following indictable offence(s) against the laws of the Commonwealth:

Between 14 April 2016 and 1 October 2016, David William McBride gave Daniel Michael Oakes military information, contrary to section 73A(1) of the *Defence Act* 1903 (Cth).

Between 14 April 2016 and 1 October 2016, Daniel Michael Oakes unlawfully obtained military information, contrary to section 73A(2) of the *Defence Act 1903* (Cth).

Between 1 March 2013 and 20 December 2014, David William McBride stole property belonging to the Commonwealth, contrary to section 131.1(1) of the *Criminal Code Act 1995* (Cth).

About Between 14 April 2016 and 1 October 2016, Daniel Michael Oakes dishonestly received stolen property from David William McBride, knowing or believing that the property was stolen, contrary to section 132.1 of the *Criminal Code Act 1995* (Cth).

About 1 May 2016, David William McBride unlawfully disclosed a fact or document which came into his knowledge by virtue of him being a Commonwealth officer,

contrary to section 70(1) of the Crimes Act 1914 (Cth)

I hereby issue this warrant which authorises you to enter and search the premises described above.

AND by virtue of section 3F(1) of the *Crimes Act 1914* this warrant authorises the executing officer or a constable assisting to do all of the following;

- enter the premises described above at anytime and execute the warrant;
- if the premises are a conveyance, to enter the conveyance, wherever it is;
- search for and record fingerprints found at the premises and to take samples of things found at the premises for forensic purposes;
- search the premises for any evidential material that satisfies ALL of the three conditions specified above and to seize any such evidential material that may be found;
- seize any other thing found at the premises in the course of the search that the
 executing officer or the constable assisting believes on reasonable grounds to
 be:
 - evidential material in relation to an offence to which the warrant relates;
 - (ii) evidential material in relation to another offence that is an indictable offence; or
 - (iii) evidential material (within the meaning of the *Proceeds of Crime Act 2002*) or tainted property (within the meaning of that Act).

if the executing officer or the constable assisting believes on reasonable grounds that seizure of the thing is necessary to prevent its concealment, loss or destruction or its use in committing an offence;

seize any other thing found at the premises in the course of the search that the
executing officer or the constable assisting believes on reasonable grounds to be
a seizable item, in that it is a thing that would present a danger to a person or
that could be used to assist a person to escape from lawful custody.

AND by virtue of section 3F(2A) of the *Crimes Act 1914* this warrant authorises the executing officer or a constable assisting to do all of the following:

- to use:
 - a computer, or data storage device, found in the course of a search authorised under the warrant; or
 - a telecommunications facility operated or provided by the Commonwealth or a carrier; or
 - o any other electronic equipment; or
 - a data storage device;

for the purpose of obtaining access to data (the *relevant data*) that is held in the computer or device found in the course of a search authorised under the warrant at any time when the warrant is in force, in order to determine

whether the relevant data is evidential material of a kind specified in the warrant; and

- if necessary to achieve the purpose mentioned above to add, copy, delete or alter other data in the computer or device found in the course of a search authorised under the warrant; and
- if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - to use any other computer or a communication in transit to access the relevant data; and
 - o if necessary to achieve that purposes to add, copy, delete or alter other data in the computer or the communication in transit; and
- to copy any data to which access has been obtained, and that:
 - o appears to be relevant for the purposes of determining whether the relevant data is evidential material of a kind specified in the warrant; or
 - is evidential material of a kind specified in the warrant; and
- to do any other thing reasonably incidental to any of the above authorised by section 3F(2A).

AND by virtue of section 3F(2B) of the *Crimes Act 1914* this warrant authorises the executing officer or a constable assisting to do all of the following:

- to use:
 - a computer found in the course of a search authorised under the warrant; or
 - a telecommunications facility operated or provided by the Commonwealth or a carrier;
 - any other electronic equipment;

for the purpose of obtaining access to data (the *relevant account-based data*) that is account-based data in relation to:

- a person who is the owner or lessee of the computer found in the course of a search authorised under the warrant; or
- a person who uses or has used the computer found in the course of a search authorised under the warrant;
- a deceased person who, before the person's death, was the owner or lessee of the computer found in the course of a search authorised under the warrant; or
- a deceased person who, before the person's death, used the computer found in the course of a search authorised under the warrant;

in order to determine whether the relevant account-based data is evidential material of a kind specified in the warrant; and

 if necessary to achieve the purpose mentioned above - to add, copy, delete or alter other data in the computer found in the course of a search authorised under the warrant; and

- if, having regard to other methods (if any) of obtaining access to the relevant account-based data which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - to use any other computer or a communication in transit to access the relevant account-based data; and
 - o if necessary to achieve that purpose-to add, copy, delete or alter other data in the computer or the communication in transit; and
- to copy any data to which access has been obtained, and that:
 - appears to be relevant for the purposes of determining whether the relevant account-based data is evidential material of a kind specified in the warrant; or
 - is evidential material of a kind specified in the warrant; and
- to do any other thing reasonably incidental to any of the above authorised by section 3F(2B).

This warrant does not authorise the executing officer or a constable assisting to conduct a search of a person who is at or near the premises when the warrant is executed.

And, by virtue of section 3G of the Crimes Act 1914, in executing this warrant:

- the executing officer may obtain such assistance as is necessary and reasonable in the circumstances;
- the executing officer, and any constable assisting in the execution of this
 warrant who is a police officer, may use such force against persons or things as
 is necessary and reasonable in the circumstances; and
- any person who has been authorised by the executing officer to assist in the
 execution of this warrant, but who is not a police officer, may use such force
 against things as is necessary and reasonable in the circumstances;

And the executing officer or a constable assisting may exercise such other of the powers available under Division 2 of Part IAA of that Act as are appropriate in the circumstances of the case;

And if you exercise the power under section 3L(4) of the *Crimes Act 1914* to secure electronic equipment on the premises, and if you then leave the premises, this warrant authorises a further entry to the premises to allow an expert to operate the equipment, provided that the further entry is made within 24 hours or such further period as may be authorised under that Act.

The offences to which this warrant relates are those specified above in the third condition.

Legal Professional Privilege

NOTE: This warrant is issued in recognition that a claim for legal professional privilege may be made in respect of documents covered by this warrant and on the understanding that, if that occurs, the executing officer will, as far as is reasonably practicable, follow the course of action set out in the document entitled "Claims for Legal Professional Privilege: Premises other than those of a Lawyer, Law Society or Like Institution" a copy of which is attached to this warrant.

NOTE the following:

"Evidential material" is defined in section 3C(1) of the Crimes Act 1914 to mean:

a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form.

"Thing relevant to an indictable offence" is defined in section 3(1) of the *Crimes Act 1914* to mean:

- (a) either of the following:
 - anything with respect to which an indictable offence against any law of the Commonwealth or of a Territory has been committed or is suspected, on reasonable grounds, to have been committed;
 - (ii) anything with respect to which a State offence that has a federal aspect, and that is an indictable offence against the law of that State, has been committed or is suspected, on reasonable grounds, to have been committed; or
- (b) anything as to which there are reasonable grounds for suspecting that it will afford evidence as to the commission of any such offence; or
- (c) anything as to which there are reasonable grounds for suspecting that it is intended to be used for the purpose of committing any such offence;

"Thing relevant to a summary offence" is defined in section 3(1) of the Crimes Act 1914 to mean:

- (a) either of the following:
 - anything with respect to which a summary offence against any law of the Commonwealth or of a Territory has been committed or is suspected, on reasonable grounds, to have been committed;
 - (ii) anything with respect to which a State offence that has a federal aspect, and that is a summary or simple offence against the law of that State, has been committed or is suspected, on reasonable grounds, to have been committed; or
- (b) anything as to which there are reasonable grounds for suspecting that it will afford evidence as to the commission of any such offence; or
- (c) anything as to which there are reasonable grounds for suspecting that it is intended to be used for the purpose of committing any such offence.

Statement of rights of the occupier

A statement of the rights of the occupier of premises is attached to this warrant.

This warrant may be executed at any time.

The time at which this warrant expires is midnight at the end of the seventh day after the day on which the warrant is issued (or lesser period). in the State of New South Wales

this ______ day of June 2019

Martin Kane
Registrar

Other person employed in a court who is authorised to issue search warrants.

Firstly, I want to start by assuring the public that the AFP actions over the last two days have been independent and impartial at all times. The AFP has been investigating these matters since July 2017, and April 2018 respectively. The matters primarily relate to secrecy offences under Part 6 and Part 7 of the Crimes Act 1914. The AFP's role, as I'm sure everyone is aware, is to investigate breaches of Commonwealth criminal law. We investigate laws passed by the Parliament, using powers granted to us by the Parliament. Our investigations are an objective search for the truth. It involves the discovery and presentation of evidence in an exhaustive, comprehensive, and organised matter [sic].

00:59

And this often includes the execution of search warrants. No sector of the community should be immune for [sic] this type of activity or evidence collection more broadly. This includes law enforcement itself, the media, or indeed, even politicians. There are criminal allegations being investigated and we cannot ignore them. We are duty bound to conduct these investigations impartially and thoroughly. Not to do so, would be a breach of our oath of office as police officers. These search warrants were authorised by an appropriate member of the judiciary, this is result [sic] of supporting documentation being presented to the court which provides sufficient suspicion that a criminal offence has been committed and evidentiary material is likely to be found at certain locations. The execution of these search warrants and the timing of these search warrants was a considered decision aimed at lawfully locating evidence and seizing that evidence in a manner which will withstand the scrutiny of a court of law.

02:09

The collection of evidence and investigation process undertaken by my staff and police more broadly in the AFP and indeed across the state and territory jurisdictions, when conducting investigations, must be done in accordance with the law. Throughout the execution of the search warrants, in collaboration with the people affected, the AFP in these particular matters took additional care to protect the confidentiality of other personal or professional information that was not subjected to the warrant. Both of these investigations relate to national security information, how it was handled, and who had access to it. The material subject to these investigations and search warrants relates to documents classified as both top secret and secret. The compromise of such material could cause exceptionally grave damage or serious damage to the national interest, organisations, or indeed, individuals.

03:09

The point of difference with these two particular investigations, or the most particular point of difference, is parts of the document were actually published. I need to emphasise in the strongest possible terms that not the government nor any minister has directed the actions of these investigations. As a standard practice, the AFP notified the minister's office it was investigating these matters at the time these matters were referred to the AFP. We did not provide regular updates on operational activities, nor did we tell them we have obtained search warrants and planned to execute these warrants. Notification of the search warrants being executed occurred after the activity had commenced. This was an operational decision and in accordance with our governance and standard practice. These investigations are typically complex and lengthy.

04:04

The timing of these investigations or these activities was influenced only by the progress of the investigation to date, and sufficient information being available to support the application of a search warrant. Any inference that suggests our decisions were influenced by anyone else outside the organisation is strongly refuted. I reject the claim over the last few days that we are trying to intimidate journalists or conduct a campaign against the media. The AFP is a strong supporter of press freedom. The media plays an important role in today's society in keeping the Australian community informed. And finally, and probably as importantly as anything else I've said, I'd like to state that my members over the last few days have been subjected to unprecedented scrutiny in relation to these particular matters. They have my strongest support for their actions and their activities. They have acted professionally and respectfully under challenging circumstances.

05:01

And I'm happy to take any questions.

Q: Can you confirm that by adding the words "add, copy, delete, alter" in warrants, including the one that was executed on the ABC, it gives the AFP the capacity to hack computers sometimes remotely without people knowing, and then removing that capacity later?

A: No, it doesn't and I'll explain why that's actually been added. I think it's a very good question, certainly one that I think is worthy of some discussion, noting that it has been discussed at length in the media today. Obviously, we operate now in a very technological savvy environment. Every time we execute search warrants, we are doing so because people have iPhones and the like. If we access a document, say on your phone, as soon as we access that, by the very nature of accessing it, we have altered it. If we copy it and we move it somewhere else, we have altered it. We have altered the metadata. The reason why that particular clause has been added to the legislation, is so that when we seize the document, it is altered. But the inference that we can remotely alter documentation or that we can change the way things are presented in their real sense is totally refuted. And I might add that particularly in relation to these particular search warrants, we have seized documentation that is currently locked down. That being that it is in the hands of the investigators, and we have signed an undertaking with the lawyers of both the ABC and News Corp, that we will not talk about those matters, we will not look at those particular files, or those documentation [sic], until such time as the lawyers from those relevant agencies and the lawyers from the AFP have gone through and looked at the privilege issue. And clearly at that stage if there is any inference there there's been alteration of documents that will be disclosed at that time. But I really refute the fact that the legislation has enabled us to do that. I think I've explained why the legislation has been changed. Now we're operating in an extremely complex environment, and I think that we need the legislation sometimes needs to keep pace with it and we'll do our best in relation to ensuring that.

07:20

Q: Were you planning other raids and have they been put on hold?

A: Look, I'm not going to give a blow by blow description in relation to where the investigation is at, and I think in fairness, nor would you expect me to. The investigation is complex, it is ongoing.

1489567_1

Potentially, yes we may do more search warrants. But again, as I said earlier, the legislation we are operating on here is extremely complex, and as such, we're required to examine what we're doing in a very thoughtful way, and if we determine it appropriate to execute more search warrants in relation to this investigation, we will do so, without fear or favour.

07:57

Q: Who is the subject of your investigation? Who could be liable for prosecution? Could the organisations' journalists be liable for prosecution?

A: Again, I think it's important to say at this phase that we are in the evidence collection phase of the investigation. Now, clearly, we've got a long way to go. But certainly, in relation to who is - we've got a person before the court already. It's in the public domain. In relation to what has been referred to as The Afghan Files matter. That matter is ongoing. I'm not going to rule in or rule out anyone being subject to further charges. I think that's inappropriate.

Q: Just for clarification though, it can be a crime to publish this material, can't it?

A: Look, it can be. But I think we also need to Chris here in relation to this particular issue, we need to look at the public interest issue. And I think you know I'm going to raise that because I'm sure you people are going to at some stage. Public interest is something that we look at in relation to our investigations from the outset. And it's something that we will consider in the course of producing our brief of evidence. I might also add that it's in the Commonwealth Director of Public Prosecutions' guideline in relation to whether or not they can commence a prosecution based on public interest. So we've got two fairly in-depth things that we need to overcome before we go down that path. But I think, you know, you guys have read the legislation. You guys understand exactly the potential possibility, but it is an offence to actually have that particular material still on websites. Yes, it is.

09:22

Q: You have chosen to reveal to us a couple of instances where there was contact with the executive government. Specifically at the outset of the investigations. Given you can reveal that much, can you tell us how much if any contact there has been with members of the executive on these two investigations over the intervening period, after two years, or are you saying today there was no other contact with the executive before those warrants were issued?

A: That's exactly what I'm saying. Look, this is not unusual in relation to these type [sic] of investigations. We are required under our national guideline to inform the minister when we receive investigations of this nature. We undertook that. But it's also important to note that, you know, sensitive investigations such as this, we utilise a fair amount of discretion not to brief the minister, or the minister's office I should say. And that's the undertaking in this particular instance.

Q: So from the outset of the investigation, no member of the executive or their staff was briefed or updated in any way on either investigation?

A: That's correct.

10:34

1489567_1

Q: You sought the warrant for the ABC action through a court registrar in Nowra, why would you seek the warrant through a court registrar in Nowra instead of a magistrate or a judge in Sydney or Canberra?

A: Look, important question and I think that it's one that I'm happy to answer. Now, in the ACT, we certainly obtain the warrant from the magistrate, which is in accordance with the judicial process that exists within the Australian Capital Territory. In New South Wales, the judicial process is different, in that the warrants are issued by court registrars. So in this instance, we actually attended Queanbeyan Local Court in New South Wales and we obtained the warrant from the registrar there who also acts in a capacity in Nowra.

11:18

Q: What's the alleged harm to national security in these cases and why doesn't the Australian public have a right to know about plans to increase spying or alleged unlawful killing?

A: What we're investigating is the fact that code worded and top secret and secret information was disclosed to the Australian community. The substance of that is to our investigation process is somewhat irrelevant. The issue of whether or not the public has a right to know is really not an issue that comes into our investigation process. We're given a complaint in these instances by secretaries of other departments, we look at the criminality and then we investigate that. Now, we're not going to make a judgement and nor should we make a judgement, and indeed nor can we make a judgement in relation to whether a referral is a good referral or a bad referral. But in this particular instance, it was deemed that a likelihood of an offence being committed had been done so. And therefore we commenced an investigation.

12:20

Q: On that point, you mentioned in your opening remarks about how these documents had been published.

A: Yes.

1489567_1

Q: The actual. Can you explain why is that so different? If these documents actually hadn't been published on the papers and on websites, would that perhaps suggest that these cases may not have gone ahead?

A: No, I didn't say that. I think what is important to note that what sets these two, if you like, above others, is the fact the information was published online. Or in the newspaper, as the case may be. It doesn't take away from the fact it was still a breach of the national security guidelines in that top secret and secret information had been released by a member of Commonwealth employment to a member of the media.

Q: You mentioned that these investigations can be lengthy, but surely waiting so long before conducting a raid would increase the probability that the evidence is misplaced or destroyed, wouldn't it?

A: I think one thing I will say at the outset is they're search warrants, not raids, and even if we look at the Macquarie dictionary, we'll see that raid has a certain connotation which I find in relation to

these particular issues not quite right. But in relation to the gathering of a search warrant takes a fair amount of time. It's not a simple matter of just deciding to do a search warrant. There's a fairly lengthy evidence collection phase before we go to the fact of executing a search warrant. And I will say that the execution of a search warrant in itself isn't necessarily the finalisation of the investigation. There are other things that we will continue to do. So if you like, it's a continuum that may change. Sometimes the search warrant will be very early, sometimes it will be in the middle of the investigation, and indeed sometimes the execution of a search warrant will be at the end. The timing of the execution of the search warrant is really irrelevant. The fact of the matter is the evidence that we obtained during the execution of the search warrants was also electronic, and electronic footprint is much more difficult to remove than a piece of paper.

14:19

Q: Taking it back to something you said a little earlier because you were finishing when you said it is an offence to have this material on websites. So can I take you back to that again. So, a crime therefore has been committed by the media organisations. Is it your intention to prosecute the journalists?

A: We haven't made a decision one way or the other.

Q: But a crime has been committed. In your view, that crime of having that material on the website has been committed.

A: We will need to go through the process of proving the elements of the offence. One of the critical issues for us is who is responsible for the uploading of that document on the computer, when it was done, et cetera, et cetera. So there's a fairly significant process, but I also did speak about public interest, and the fact of the matter is, regardless of where our investigation leads us to, there's a number of other steps that need to take place before we get to the phase that we're actually putting someone before the court. And I think that's being lost. The search warrant is a part of the process. It's a very minute part of the process indeed, but indeed it's a public part of the process. So whilst the collection of information is still ongoing, we can't lose sight of the fact that we've got a long way to go.

15:26

Q: The Attorney-General yesterday said Annika Smethurst was not the subject of an investigation per se. Based on your answers to the press, are you saying she could still face criminal prosecution. Was the Attorney-General wrong to say that yesterday?

A: No, because the way that the search warrants were crafted under the old legislation is indeed the Attorney-General is correct. The new legislation which was put in place towards the end of last year means that the publication of those things is an offence. We're probably not going to look at that particular offence in this instance.

Q: One of these cases is two years old. The other is 14 months old, and you served these warrants on two successive days, three weeks after a federal election. Are you asking us to take that as entirely coincidental?

1489567_1

A: Well the execution of the search warrants in two consecutive days is not coincidental. That was planned. I must be very clear on that.

Q: Why?

A: I will get to that. The timing of the search warrants is irrelevant. I think that we would be having this press conference in relation to this particular activity whether we executed the search warrants before the election, during the election campaign, or indeed after, what we are now. The reason it was done consecutively, it was simply a matter of resourcing. I needed a number of investigators for both search warrants. More importantly, I needed digital forensics capability. Now obviously the AFP is a complex organisation. We do large scale investigations, obviously you know, this is part of it. But we also do counter-terrorism investigations, child protection, serious and organised crime and to crowd those resources for two full days, four people, four digital forensic people, is quite difficult. So, I'm still going, thank you. The issue for me was that this operation has taken a number of months to get to the phase where we are today. The suggestions that we, you know, the timing from my perspective is irrelevant. I honestly believe we would be having this discussion regardless of when I executed the search warrants.

17:32

Q: Just to follow that question, can you please tell us, did you or the AFP, any of your officers, take into account the timing of the federal election, in deciding when to apply to execute the search warrants? Just second to that, you say your officers took extra care in executing these warrants. How does rifling through the underwear drawer of a female reporter constitute taking extra care?

A: I will try to answer both of those, and if I fail, please pick me up and I'll come back to it. The timing, as I said, I understand why people are saying that the timing is suspicious or fishy or whatever the term is. But for me, the timing was about quarantine [sic] those resources to ensure that we were able to do the execution of the search warrants in an expedient manner to ensure that the integrity of the investigation wasn't lost. As I said, the ability for us to get the digital forensics resources ready to go is not an easy one. Noting the fact that my resources are also being used on national security investigations such as terrorism, organised crime, et cetera. In relation to the conduct of the search warrant in Ms Smethurst's house, we were looking for USBs. USBs by their nature, are quite small and are quite easy to conceal in different locations. That's why the search was conducted in accordance with our standard procedure in that we would always search those particular locations. We ensured due to her privacy, et cetera, that when that search of that particular location in her house was undertaken, it was done by two female officers. One reason why the search warrant took so long, both at her house and also at the ABC, is we were very, very careful in relation to the execution of the search warrant that we ensured that we were only targeting the information that was relevant to the search warrant. Only relevant to the search warrant. Same with all your phones and all your tablets, I'm sure there's other very sensitive information on there that you would not like in the public domain. The reason why it took us so long is the fact that we made it very clear with her assistance and her lawyer's assistance to ensure we only targeted bits relevant to the warrant, and the rest of the information we haven't.

19:46

Q: Can you confirm that before you executed the search warrant, you also executed journalist warrants to access metadata from either/or Annika Smethurst and the ABC journalists?

A: I asked that question this morning and I was advised we did not. But, if that is incorrect, we will correct the record. But my advice this morning was we did not use journalist warrants in relation to this matter.

Q: Further on the ABC, you've already said that you've been investigating this for many, many months. Why didn't you continue your legal letters with the ABC, and seek to resolve this by subpoena rather than through the theatre and optics of a raid, or to use your terminology, the execution of a search warrant?

A: That's a good question and I'm glad you raised it. We've been in negotiation, we were in negotiation with the ABC for a considerable period of time in relation to the execution of the search warrant on their location. We received advice from their legal counsel in March of this year that they were of the view that they were no longer going to assist us and we were at loggerheads. We were of the view, based on the fact that we didn't see a way forward, that the only way to continue the investigation was to execute the search warrant as we did yesterday. I might add that the only way it was turned into a public display was based on what the ABC did when we arrived yesterday. Now they knew we were coming. It was a warrant by consent, for want of a better term. Agreed time for my officers to attend the location and undertake the search warrant, which they did. The ABC filmed it, which is their right, and they continued to tweet during the execution of the search warrant, which again is their right. And I think that goes to show the fact that, the fact that that was allowed to occur, without any hindrance whatsoever, does show the AFP supports freedom of the press.

21:49

Q: Can you explain the rationale behind starting your ABC search warrants at head offices, as opposed to with Annika Smethurst, turning her apartment upside down?

A: Look, that goes into the sequence of the investigation. The investigations are slightly different. I'm not going to give you a song and dance in relation to why we do things in a certain order, but as I said, there are other strategies at play here in relation to these particular matters that dictated the order in which we do things. And as I said, we believe, through a thorough investigation, through a very strong investigation plan which was put in place in relation to these matters, that that was the appropriate course of conduct in this instance.

Q: Can you confirm that even receiving these documents would be a crime and how can we have freedom of the press if that's the case?

A: Well it's not a crime in itself, depending on the circumstances in which it took place. I might add even it's not directly relevant - but it is relevant to some extent. There is a public interest disclosure regime which exists across the Commonwealth for public servants, and indeed any members of the public that may wish to prevail themselves of that. We have investigated many similar matters over the course of the last few years where people have availed themselves of the Public Interest Disclosure Act, and as such, the AFP has not proceeded with any action. The two persons involved in this investigation, who are alleged, and I do use the word alleged strongly, were involved in the disclosure of the material to journalists, did not avail themselves of the PID. That is still a matter for

1489567_1

people to, for whistleblower activity for utilisation of the PID. But I think it's incumbent upon me also to say that it's important that people realise the reason why we are so strongly in our view of - certainly protecting top secret and secret information is that the Australian government, or particularly the Australian law enforcement intelligence communities, rely on secret and top secret information from our international partners, particularly Five Eyes partners, to ensure the fact that we keep the Australian community safe. Now if we can't be seen to protect our own internal information, we are concerned that the information flow to us dries up, and that's the fact [inaudible].

24:12

Q: In regards to the ABC, if you knew the source of the information already, in regards to David McBride, why did you need to go into the ABC to determine that source, and how is that not just a show of force, designed to intimidate the media and stop other whistleblowers from coming forward?

A: Look, I disagree with the premise but I understand where you're coming from. I'm sympathetic to the views of the journalists in relation to this particular issue, but we're in a different prism here. I'm trusted as a senior official of the law enforcement agency to execute lawful executioning [sic] powers. Now if it's an issue in relation to the law, and we think the law is inappropriate, well then we need to change the law. But as the law stands at the moment, we have to execute it. Now as far as executing the search warrant with a number of police officers all dressed in plain clothes, by appointment, I don't think that's intimidation.

Q: Whether they're wearing plain clothes or not, it's a show of force to go in and do what you were doing, is it not?

A: No I disagree. I think the fact is it was done through appointment, they knew we were coming. I don't agree it's a use of force.

Q: [inaudible] people wearing plain clothes is intimidating?

A: We're going to agree to disagree on that.

25:20

Q: How many leak investigations, leaks to the media, in the last three years, have been referred to the AFP, and given your point about resources and things like counter-terrorism, we're in a heightened threat environment, is it really the police's best use of time to conduct these sorts of witch-hunts?

A: Look, we get numerous leaking referrals to us and to be honest we get too many. But as I said, the premise of us investigating these matters is to ensure that the international community knows that we take the leaking of information, sensitive information, seriously. Because if we don't take it seriously, it closes down an avenue of people providing the Australian community or the Australian intelligence and law enforcement agencies very sensitive information which ultimately does save lives. I can't stress that enough.

Q: Have you advised Annika Smethurst, Samuel Clark or Daniel Oakes that there could be a criminal prosecution as a result of your investigations going forward?

A: Look, I don't know what the investigators said during the course of the search warrant so it would be inappropriate for me to comment.

Q: [inaudible] your earlier answer to a question about the timing, I appreciate what you've said about resourcing and, you know, specialist skills being available at the right time, but can you please say whether the timing of the election was ever a factor in your decision on the timing of seeking and executing the warrants? You said to Tim earlier that the AFP never updated the government or anyone in the executive about the investigation. Can you tell us did anyone from the government or any department head contact the AFP seeking an update?

A: Certainly, the timing is irre-I made the decision of timing. That was my decision in my substantive position.

Q: Did you factor in the election?

A: No, I did not. I did not factor in the election. In relation to notifications of government, I can assure you there were no updates. In relation to updates of secretaries of government agencies, to the best of my - certainly I did not update them, but I have to be careful here, because I would be surprised if our investigators at some stage did not have some conversations with the referring agencies as I would expect.

27:35

Q: It strikes me that a story about the behaviour of our SAS troops abroad that might have involved the murder of innocents, and a discussion of whether one of our agencies might be re-tasked to spy on Australian citizens are of prime public importance. Are you saying that the public interest would have been better served had those two pieces of journalism not appeared?

A: No I've never said. What I'm saying is we have investigated a criminal offence. And I said, I think I've said at the outset, and correct me if I didn't, that we're investigating the criminality. Now the issue of public interest is a matter that we do consider and I have said that. But we considered that at various phases through the investigation. I will also say that in relation to one of those matters in particular, there is also some very sensitive personal information that has found its way into the hands of people who probably shouldn't have it. And I'm concerned about that, as are those individual members. We've got to take into consideration, as I said as well, individual privacy here is paramount as well.

Q: So when will the merit of these stories be factored in, Assistant Commissioner, and how? When and how will the public merit of the stories be weighed?

A: It's a good question. I think the public interest as I said is part of the consideration that we do during the course of our investigation. If we determine there is sufficient evidence to run a prosecution, and we've got a long way to go before we get there, it is then a consideration of the Commonwealth Director of Public Prosecution before they determine whether or not it's in the public interest to prosecute. And ultimately if they decide it is, then it's a matter for the judiciary. So

1489567_1

it's a 3-step process. We investigate many crimes in the AFP where we know there could be a defence immediately. I use the example of common assault. When we investigate a common assault, we know in the back of our mind immediately that there's things such as self-defence, immediately could be proven or could be waived [sic]. It doesn't stop us from investigating the matter. What I'm trying to get my point across here, is that we're in the process of investigation. We're in the process of discovery. We're in the process of evidence collection. We've got a long way to go before we get to the stage of a prosecution or a brief of evidence.

29:52

Q: Are you still investigating the curious leak of some ASIO advice, cabinet level ASIO advice, to the Australian newspaper earlier this year?

A: I honestly don't have the answer to that question. Last question.

Q: Do you agree that it's peculiar that no people holding public office or politicians have been the subject of search warrants in relation to the previous cabinet leaks?

A: No. I mean, as I said, we follow an investigative process, and in those particular instances during the course of the investigation we deemed it wasn't necessary to undertake search warrants.

Q: Given Mr McBride has sort of openly admits [sic] that he has handed documents to the ABC journalists named on the warrant yesterday, why did the AFP feel it necessary to go into the ABC and do that? What sort of link are you establishing there, where the accused person who has been committed to trial says yep, there is a link, it was me?

A: I think in relation to that one, we still have to follow the evidence trail. We still need to ensure that just because someone says they did something, doesn't mean they actually did, so there's still a fair way-

Q: [inaudible 30.59] admit to a crime?

A: People do it, surprisingly people actually do it quite regularly.

Thanks everyone.

Q: How much does it cost to carry out the search warrants?

A: That's too early for us to tell. The investigation's still ongoing. We've still got a way to go before we can cost it. Thanks everybody.



THE HON PETER DUTTON MP MINISTER FOR HOME AFFAIRS

Minister for Home Affairs – Ministerial Direction to Australian Federal Police Commissioner relating to investigative action involving a professional journalist or news media organisation in the context of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer

This Ministerial Direction is issued under subsection 37(2) of the Australian Federal Police Act 1979 (the AFP Act). This Ministerial Direction is intended to complement any previous Ministerial Direction issued under subsection 37(2) with effect from the date this Ministerial Direction commences. This Ministerial Direction does not constrain investigation by the Australian Federal Police (AFP) of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer.

This Ministerial Direction outlines the Government's expectations for the AFP in relation to investigative action involving a professional journalist or news media organisation in the context of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer.

A key function of the AFP is, and must remain, the enforcement of the criminal law, without exception. In its performance of this function, however, I expect the AFP to take into account the importance of a free and open press in Australia's democratic society and to consider broader public interest implications before undertaking investigative action involving a professional journalist or news media organisation in relation to an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer.

In particular, where consistent with operational imperatives, I expect the AFP to exhaust alternative investigative actions, including in relation to any other persons that may be involved in the matter, prior to considering whether any investigative action involving a professional journalist or news media organisation is necessary. Where possible, I also expect the AFP to continue to seek voluntary assistance, if relevant, from professional journalists or news media organisations.

I also expect the AFP to strengthen its guidance and processes about the types and level of information required from a Government department or agency in referring an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer to the AFP for investigation. This should include an explicit requirement that the referring department or agency provides a harm statement indicating the extent to which the disclosure of the material would be expected to significantly compromise Australia's national security.

This stronger framework around the referral process should enable the AFP to comprehensively assess all relevant information and make an informed decision about whether and in what way to proceed with a criminal investigation, having due regard to relevant public interest considerations. In undertaking that assessment, the AFP must have regard to any whole-of-government guidance that may be issued concerning the levels of harm caused to Australia's national interest by disclosure of the various types of information held across Government.

Dated & August 2019

Peter Dutton

The Hon Peter Dutton MP

Minister for Home Affairs

CHAPTER 52.

ct to prevent the Disclosure of Official Documents Information. | 26th August 1889. |

it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Tem-, and Commons, in this present Parliament assembled, and by authority of the same, as follows:

(1.) (a.) Where a person for the purpose of wrongfully Disclosure of obtaining information-

information.

- (i.) enters or is in any part of a place belonging to Her Majesty the Queen, being a fortress, arsenal, factory, dockyard, camp, ship, office, or other like place, in which part he is not entitled to be; or
- (ii.) when lawfully or unlawfully in any such place as afore. said, either obtains any document, sketch, plan, model, or knowledge of any thing which he is not entitled to obtain, or takes without lawful authority any sketch or plan; or
- (iii.) when outside any fortress, arsenal, factory, dockyard, or camp belonging to Her Majesty the Queen, takes or attempts to take without authority given by or on behalf of Her Majesty, any sketch or plan of that fortress, arsenal, factory, dockyard, or camp; or
- (b.) where a person knowingly having possession of, or control over, any such document, sketch, plan, model, or knowledge as has been obtained or taken by means of any act which constitutes an offence against this Act at any time wilfully and without lawful authority communicates or attempts to communicate the same to any person to whom the same ought not, in the interest of the State, to be communicated at that time; or
- (c.) where a person after having been entrusted in confidence by some officer under Her Majesty the Queen with any document, sketch, plan, model, or information relating to any such place as aforesaid, or to the naval or military affairs of Her Majesty, wilfully and in breach of such confidence communicates the same when, in the interest of the State, it ought not to be communicated;

he shall be guilty of a misdemeanor, and on conviction be liable to imprisonment, with or without hard labour, for a term not exceeding one year, or to a fine, or to both imprisonment and a

(2.) Where a person having possession of any document, sketch, plan, model, or information relating to any fortress, arsenal, factory, dockyard, camp, ship, office, or other like place belonging to Her Majesty, or to the naval or military affairs of Her Majesty, in whatever manner the same has been obtained or taken, at any time wilfully communicates the same to any person to whom he knows the same ought not, in the interest of the State, to be communicated at that time, he shall be guilty of a misdemeanour, and be

liable to the same punishment as if he committed an offence under the foregoing provisions of this section.

(3.) Where a person commits any act declared by this section to be a misdemeanour, he shall, if he intended to communicate to a foreign State any information, document, sketch, plan, model, or knowledge obtained or taken by him, or entrusted to him as aforesaid, or if he communicates the same to any agent of a foreign State, be guilty of felony, and on conviction be liable at the discretion of the court to penal servitude for life, or for any term not less than five years, or to imprisonment for any term not exceeding two years with or without hard labour.

Breach of official trust.

2.—(1.) Where a person, by means of his holding or having held an office under Her Majesty the Queen, has lawfully or unlawfully either obtained possession of or control over any document, sketch, plan, or model, or acquired any information, and at any time corruptly or contrary to his official duty communicates or attempts to communicate that document, sketch, plan, model, or information to any person to whom the same ought not, in the interest of the State, or otherwise in the public interest, to be communicated at that time, he shall be guilty of a breach of official trust.

(2.) A person guilty of a breach of official trust shall—

- (a.) if the communication was made or attempted to be made to a foreign State, be guilty of felony, and on conviction be liable at the discretion of the court to penal servitude for life, or for any term not less than five years, or to imprisonment for any term not exceeding two years, with or without hard labour; and
- (b.) in any other case be guilty of a misdemeanor, and on conviction be liable to imprisonment, with or without hard labour, for a term not exceeding one year, or to a fine, or to both imprisonment and a fine.
- (3.) This section shall apply to a person holding a contract with any department of the Government of the United Kingdom, or with the holder of any office under Her Majesty the Queen as such holder, where such contract involves an obligation of secrecy, and to any person employed by any person or body of persons holding such a contract, who is under a like obligation of secrecy, as if the person holding the contract and the person so employed were respectively holders of an office under Her Majesty the Queen.

Punishment for incitement or counselling to commit offence.

3. Any person who incites or counsels, or attempts to procure, another person to commit an offence under this Act, shall be guilty of a misdemeanor, and on conviction be liable to the same punishment as if he had committed the offence.

Expenses of prosecution.

4. The expenses of the prosecution of a misdemeanor under this Act shall be defrayed in like manner as in the case of a felony.

Saving for laws of British possessions. 5. If by any law made before or after the passing of this Act by the legislature of any British possession provisions are made which appear to Her Majesty the Queen to be of the like effect as those contained in this Act, Her Majesty may, by Order in Council, suspend the operation within such British possession of this Act

of any part thereof, so long as such law continues in force there, no longer, and such order shall have effect as if it were enacted this Act:

Provided that the suspension of this Act, or of any part thereof, any British possession shall not extend to the holder of an office. Her Majesty the Queen who is not appointed to that office the Government of that possession.

he expression "British possession" means any part of Heresty's dominions not within the United Kingdom.

6.—(1.) This Act shall apply to all acts made offences by this Extent of Act et when committed in any part of Her Majesty's dominions, or and place of trial of offence. hen committed by British officers or subjects elsewhere.

(2) An offence under this Act, if alleged to have been committed tof the United Kingdom, may be inquired of, heard, and detered, in any competent British court in the place where the new was committed, or in Her Majesty's High Court of Justice England or the Central Criminal Court, and the Act of the orty-second year of the reign of King George the Third, chapter ghty-five, shall apply in like manner as if the offence were mentioned in that Act, and the Central Criminal Court as well as the High Court possessed the jurisdiction given by that Act to the Court of King's Bench.

(3.) An offence under this Act shall not be tried by any court of general or quarter sessions, nor by the sheriff court in Scotland, nor by any court out of the United Kingdom which has not jurisdiction to try crimes which involve the greatest punishment allowed by

- (4.) The provisions of the Criminal Law and Procedure (Ireland) 50 & 51 Vict. Act, 1887, shall not apply to any trial under the provisions of this c. 20. Act.
- 7.—(1.) A prosecution for an offence against this Act shall not Restriction on be instituted except by or with the consent of the Attorney-prosecution. General.
- (2.) In this section the expression "Attorney-General" means the Attorney or Solicitor General for England; and as respects Scotland, means the Lord Advocate; and as respects Ireland, means the Attorney or Solicitor General for Ireland; and if the prosecution is instituted in any court out of the United Kingdom, means the person who in that court is Attorney-General, or exercises the like functions as the Attorney-General in England.

8. In this Act, unless the context otherwise requires—

Interpretations.

Any reference to a place belonging to Her Majesty the Queen includes a place belonging to any department of the Government of the United Kingdom or of any of Her Majesty's possessions, whether the place is or is not actually vested in Her Majesty;

Expressions referring to communications include any communication, whether in whole or in part, and whether the document, sketch, plan, model, or information itself or the substance

or effect thereof only be communicated;

The expression "document" includes part of a document;

The expression "model" includes design, pattern, and specimen: The expression "sketch" includes any photograph or other mode

of representation of any place or thing;

The expression "office under Her Majesty the Queen," includes any office or employment in or under any department of the Government of the United Kingdom, and so far as regards any document, sketch, plan, model, or information relating to the naval or military affairs of Her Majesty, includes any office or employment in or under any department of the Government of any of Her Majesty's possessions.

Saving.

9. This Act shall not exempt any person from any proceeding for an offence which is punishable at common law, or by military or naval law, or under any Act of Parliament other than this Act, so, however, that no person be punished twice for the same offence.

Short title.

10. This Act may be cited as the Official Secrets Act, 1889.

CHAPTER 53.

An Act to amend the Acts relating to the Office of Paymaster General, and to make better Provision for the Discharge of the Duties of that Office.

[30th August 1889.]

BE it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:

Power for Treasury to make regulations.

- 1.—(1.) The Commissioners of Her Majesty's Treasury (in this Act referred to as the Treasury) may from time to time make regulations—
 - (a.) For transferring to the Bank of England or the Bank of Ireland any of the duties performed at the passing of this Act in the office of Her Majesty's Paymaster General; and
 - (b.) For otherwise altering or rescinding the regulations in force at the passing of this Act for the conduct of business in the said office; and
 - (c.) In the case of any funds or securities required by any enactment in force at the passing of this Act to stand in the name of or be held by the Paymaster General or Assistant Paymaster General jointly with any other person, for substituting for the Paymaster General or Assistant Paymaster General any officer of the Bank of England appointed in that behalf by the Treasury, with the concurrence of the Governor and Company of the Bank of England, or any officer of any public department.
- (2.) All regulations made in pursuance of this section shall be laid before Parliament within three weeks after they are made if Parliament is then sitting, and if Parliament is not then sitting, within three weeks after the then next meeting of Parliament.

THE

QUEENSLAND STATUTES.

VOL. VI.

SESSIONAL ACTS, 1889-93,

BEING A CONTINUATION OF THE STATUTES OF QUEENSLAND;

TOGETHER WITH

THE ACTS OF THE FEDERAL COUNCIL; AND THE IMPERIAL ACTS APPLICABLE TO QUEENSLAND, PASSED 1889-93.

WITH INDEXES AND TABLES.



BRISBANE: EDMUND GREGORY, GOVERNMENT PRINTER, WILLIAM STREET. 1894. Safety of Defences Act.

54 Vic. No. 11,

Protection of contracts made before commencement of Act.

3. Any person who before the commencement of this Act had made or entered into any contract or agreement for the sale or delivery in Queensland, on or at any time after the nineteenth day of September, one thousand eight hundred and ninety, of any spirits whereon additional duty is payable under the provisions of this Act, shall be at liberty to add to the contract price so much money as will be equivalent to the additional duty which by reason of such provisions has been paid or made payable on such spirits, and shall be entitled, by virtue of this Act, to be paid the same accordingly by the purchaser of such spirits, and to sue for and recover the same from such purchaser:

Provided that the purchaser may at his option, by notice in writing under his hand served on the other party to the contract within fourteen days after the passing of this Act, declare the contract null and void, and the same shall be null and void accordingly.

Commencement and short title. 4. This Act shall be deemed and taken to have come into operation and to have been in force on and from the nineteenth day of September, one thousand eight hundred and ninety, and may be cited as "The Customs Duties Act of 1890."

[See section 1.]

THE SCHEDULE.

ARTICLES.

QUANTITIES, BATE.

Spirits or strong waters, excepting perfumed spirits, of any strength not exceeding the strength of proof by Sykes's hydrometer, and so in proportion for any greater strength than the strength of proof

Spirits, cordials, or strong waters sweetened or mixed with any article so that the strength thereof cannot be exactly ascertained by Sykes's hydrometer

14 shillings

per gallon per gallon per gallon thereof cannot be exactly ascertained by Sykes's hydrometer

DEFENCE.

54 Vic. No. 11. An Act to prevent the Unauthorised Disclosure of Informa-THE SAFETY OF DEFENCES tion relating to the Defences of Queensland.*

ACT OF 1890.

[Assented to 11th November, 1890.]

E it enacted by the Queen's Most Excellent Majesty,
by and with the advice and consent of the Legislative Council and Legislative Assembly of Queensland in

* Compare generally with this Act the Official Secrets Act, 1889 (52 & 53 Vic. c. 52), supra, page 3956.

1890.

Safety of Defences Act.

Parliament assembled, and by the authority of the same, as follows:

- 1. This Act may be cited as "The Sayety of Defences short title. 1ct of 1890."
- 2. It shall not be lawful for any person, whether a Sketching, etc., on British subject or an alien, to make any sketch, drawing, etc., on fortifications photograph, picture, or painting, of any battery, field-work, prohibited, or fortification in Queensland, or of any portion thereof, save by without the previous permission in writing of the Chief Secretary or other Minister charged with the administration of the Defences of the Colony. Any such permission shall clearly and expressly state the nature of the sketches, drawings, photographs, pictures, or paintings, which may be made by the person to whom such permission is given, and the place or places of which such sketches, drawings, photographs, pictures, or paintings, may be made.
- 3. Any person who offends against the provisions of Penalty. the last preceding section shall be liable to a penalty not exceeding one hundred pounds, or, at the discretion of the justices, to be imprisoned with or without hard labour for any period not exceeding three months; and all sketches, drawings, photographs, pictures, and paintings, and all tools, and all materials or apparatus for sketching, drawing, photographing, or painting, found in his possession shall be liable to be forfeited.
- 4. Any person who enters or approaches any battery, Penalty on field-work, or fortification with materials or apparatus for persons found on sketching, drawing, photographing, or painting in his postfortifications session, with the intention of committing any breach of with sketching the provisions of this Act, shall be liable to a penalty not exceeding twenty pounds, and all tools, and all materials or apparatus for sketching, drawing, photographing, or painting, found in his possession shall be liable to be forfeited.
- 5. Any person found trespassing on any enclosed Penalty on battery, field-work, or fortification, may be summarily persons removed therefrom by any officer or member of the Defence Force or any officer of police, and shall be liable to a penalty not exceeding twenty pounds.
- 6. Any officer or member of the Defence Force, or Penalty on officer of the Civil Service, who communicates to any communicate person, otherwise than in the course of his official duty, tionrespecting any plans, documents, or other information relating to any defences.

Diseases in Sheep Act Amendment Act. 54 Vic. No. 21.

battery, field-work, or fortification in Queensland, or toany other defences of the Colony, shall be guilty of a misdemeanour, and shall on conviction be liable to imprisonment for any term not exceeding three years, and not less than one year, and to a fine not exceeding two hundred pounds, and not less than fifty pounds.

DESIGNS AND TRADE MARKS.

See PATENTS, ETC.

DISEASES IN ANIMALS.

DISEASES IN SHEEP ACT AMENDMENT ACT OF 1890.

54 Vic. No. 21. An Act to further Amend "The Diseases in Sheep Act of 1867," and to provide for the Registration of Brands and Marks on Sheep.

ASSENTED TO 1ST DECEMBER, 1890.

E it enacted by the Queen's Most Excellent Majesty, by and with the advice and constant of the second secon by and with the advice and consent of the Legislative Council and Legislative Assembly of Queensland in Parliament assembled, and by the authority of the same, as follows:—

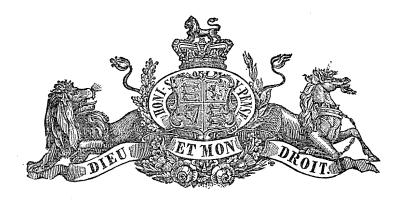
This Act to be construed with Diseases

1. This Act shall be read and construed with the "Diseases in Sheep Act of 1867" (hereinafter called the in Sheep Act. Principal Act), "The Diseases in Sheep Act of 1867 Amendment Act," "The Diseases in Sheep Act of 1867 Further Amendment Act," and "The Diseases in Sheep Act Amendment Act of 1877," and may be cited as "The Diseases in Sheep Act Amendment Act of 1890." The said Acts and this Act, and any Act amending them, may together be cited as "The Diseases in Sheep Acts."

Repeal of 40 Vic. No. 9 of 31 Vic. No. 35.¶

2. The thirty-ninth section of the Principal Act, "The 40 Vic. No. 9 Sheep Brands Act of 1876," and the fifth section of. "The Diseases in Sheep Act Amendment Act of 1877," \\$ are hereby repealed. But nothing in this Act contained shall invalidate any action done or commenced under the provisions hereby repealed.

^{* 31} Vic. No. 35, supra, page 522. † 31 Vic. No. 42, supra, page 546. ‡ 34 Vic. No. 26, supra, page 547. § 41 Vic. No. 14, supra, page 548. || 40 Vic. No. 9, supra, page 72. ¶ Marginal note misleading. Read the text.



ANNO QUINQUAGESIMO TERTIO ET QUINQUA-GESIMO QUARTO

VICTORIÆ REGINÆ.

A.D. 1890.

No. 488.

An Act to prevent the Unauthorised Disclosure of Information relating to the Defences of South Australia.

[Assented to, December 23rd, 1890.]

E it Enacted by the Governor of the Province of South Australia, with the advice and consent of the Legislative Council and House of Assembly of the said province, in this present Parliament assembled, as follows:

1. It shall not be lawful for any person to make any sketch, Sketching, &c., of converge the protections of converge the protections of converge the protections of converge the protections. drawing, photograph, picture, or painting of any fort, battery, prohibited, save by fieldwork, fortification, or other military work of defence in permission. South Australia, or of any portion thereof, without having previously obtained the permission, in writing, of the Chief Secretary on the recommendation of the Commandant of the South Australian Military Forces. Such permission shall clearly and expressly state the nature of the sketches, drawings, photographs, pictures, or paintings which may be made by the person to whom such permission is given, and the place or places of which such sketches, drawings, photographs, pictures, or paintings may be made.

2. Any person offending against the provisions of the above Penalty for offending section shall be liable to a penalty not exceeding One Hundred against provisions of Pounds, or, at the discretion of the Court, to be imprisoned, with or without hard labor, for any period not exceeding two years, and all such sketches, drawings, photographs, pictures, or paintings, and all tools and all materials or apparatus for sketching, drawing, photographing, or painting found in his possession shall be forfeited to the Crown.

The Safety of Defences Act.—1890.

Penalty on persons found in or near forts with drawing materials, &c.

Penalty—Fine, or imprisonment.

3. Any person who enters or approaches any fort, battery, fieldwork, fortification, or other military work of defence in the said province, with sketching, drawing, photographing, or painting materials or apparatus in his possession, with the intention of evading the provisions of this Act, shall be liable, upon conviction, to a penalty not exceeding Twenty-five Pounds, and in default to imprisonment, with or without hard labor, for any period not exceeding three calendar months, with or without hard labor, and all materials or apparatus for sketching, drawing, photographing, or painting found in his possession shall be forfeited to the Crown.

Penalty on persons trespassing.

4. Any person found trespassing on any enclosed fort, battery, fieldwork, fortification, or other work of military defence, may be summarily removed therefrom by any officer or member of the Defence Forces, or any officer of police, and shall be liable to a penalty of not exceeding Twenty Pounds, and in default to imprisonment not exceeding one month, with or without hard labor.

Penalty on communicating information respecting defences.

5. Any officer or member of the Defence Forces or officer of the Civil Service who communicates to any person, otherwise than in the course of his official duty, any plans, documents, or other information relating to any fort, battery, fieldwork, fortification, or other work of military defence, or to any other defences of the province, shall be guilty of a misdemeanor, and shall, on conviction, be liable to imprisonment for any term not exceeding three years, with or without hard labor.

Proceedings before Justices.

6. All proceedings for offences against this Act, except the misdemeanor mentioned in section 5, or for the recovery of penalties, shall be heard and determined in a summary way by any Special Magistrate or two Justices of the Peace, under the provisions of an Ordinance of the Governor and Legislative Council, No. 6 of 1850, intituled, "To facilitate the performance of the Duties of Justices of the Peace out of Sessions, with respect to summary convictions and orders," or of any Act now in force, or hereafter to be in force, relating to the duties of Justices of the Peace with respect to summary convictions and orders.

Short title.

7. This Act may be cited as "The Safety of Defences Act, 1890."

In the name and on behalf of Her Majesty, I hereby assent to this Bill.

KINTORE, Governor.



INDEX

TO THE

ACTS OF PARLIAMENT

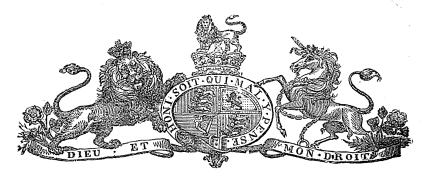
PASSED

SESSION 55° VICTORIÆ. (1891.)

VOL. X. PART II.

		•
Annual Control of the	/ ~ ~ **	PAGE
Appropriation, Consolidated Revenue Fund		381
Treasury Bills, £250,000	(No. 2.)	383
Partnership	(No. 3.)	385
Factors	(No. 4.)	3 9 7
Custody of Children	(No. 5.)	401
Directors' Liability	(No. 6.)	403
Safety of Defences	(No. 7.)	407
Companies (Memorandum of Association)	(No. 8.)	409
Leven Marine Board	(No. 9.)	413
Bank of Van Diemen's Land	(No. 10.)	415
Treasury Bills, £200,000	(No. 11.)	419
Bank of Van Diemen's Land	(No. 12.)	421
Supplementary Appropriation, 1890 and 1891	(No. 13.)	423
Collection and Recovery of Rates	(No. 14.)	447
Waratah and Zeehan Railway	(No. 15.)	· 449
Derwent Valley and Zeehan Railway	(No. 16.)	473
Bank of Van Diemen's Land	(No. 17.)	497
Appropriation, Consolidated Revenue Fund	(No. 18.)	501
Post Othce Act Amendment	(No. 19.)	503
Games and Wagers	(No. 20.)	507
Sale of Liquors at Tasmanian Exhibition	(No. 21.)	515
Dundas and Zeehan Railway Act Amendment	(No. 22.)	517

TASMANIA.



1891.

ANNO QUINQUAGESIMO-QUINTO

VICTORIÆ REGINÆ,

No. 7.

AN ACT to prevent unauthorised Disclosure A.D. 1891. of Information relating to the Defences of Tasmania. [19 August, 1891.]

DE it enacted by His Excellency the Governor of *Tasmania*, by and with the advice and consent of the Legislative Council and House of Assembly, in Parliament assembled, as follows:—

1 This Act may be cited as "The Safety of Defences Act, 1891."

Short title.

2 It shall not be lawful for any person, whether a British subject or Sketching, &c. on an alien, to make, for the purpose of wrongfully obtaining information, fortifications any sketch, drawing, photograph, picture, or painting of any battery, prohibited, save by permission, field-work, or fortification in *Tasmania*, or of any portion thereof.

3 Any person who offends against the provisions of the last Penalty. preceding section shall be liable to a penalty not exceeding One hundred Pounds, or, at the discretion of the Justices, to be imprisoned, with or without hard labour, for any period not exceeding Three months; and all sketches, drawings, photographs, pictures, and paintings, and all tools, and all materials or apparatus for sketching, drawing, photographing, or painting, found in his possession shall be liable to be forfeited.

Safety of Defences.

A.D. 1891.

Penalty on persons found on fortifications with sketch-

4 Any person who enters or approaches any battery, field-work, or fortification with materials or apparatus for sketching, drawing, photographing, or painting in his possession, with the intention of committing any breach of the provisions of this Act, shall be liable to a ing materials, &c. penalty not exceeding Twenty pounds, and all tools, and all materials or apparatus for sketching, drawing, photographing, or painting, found in his possession shall be liable to be forfeited.

Penalty on persons trespassing.

5 Any person found trespassing on any enclosed battery, field-work, or fortification may be summarily removed therefrom by any officer or member of the Defence Force or any officer of police, and shall be liable to a penalty not exceeding Twenty Pounds.

Penalty on communicating information respecting defences.

6 Any officer or member of the Defence Force or officer of the Civil Service who communicates to any person, otherwise than in the course of his official duty, any plans, documents, or other information relating to any battery, field-work, or fortification in Tasmania, or to any other defences of the Colony, shall be guilty of a misdemeanor, and shall on conviction be liable to imprisonment for any term not exceeding Two years, and to a fine not exceeding One hundred Pounds.

Offences dealt with summarily.

19 Vict. No. 8.

7 All offences against this Act, and all penalties imposed by this Act, shall be heard and determined and recovered in a summary way by and before any Two or more Justices of the Peace in the mode prescribed by The Magistrates Summary Procedure Act: Provided, that no such offence shall be heard or determined except by or with the consent of the Attorney-General or Solicitor-General.



Australia. Western

ANNO QUINQUAGESIMO SEXTO

VICTORIÆ REGINÆ.

No. IV.

AN ACT to prevent the Unauthorised Disof Information relating Defences of Western Australia.

[Assented to, 13th January, 1893.]

E it enacted by the Queen's Most Excellent Majesty, by and Preamble. with the advice and consent of the Legislative Council and Legislative Assembly of Western Australia, in this present Parliament assembled, and by the authority of the same, as follows:—

1. IT shall not be lawful for any person, whether a British subject or an alien, to make any sketch, drawing, photograph, pic- sketching, ac., or fortifications proture, or painting of any fort, battery, fieldwork, fortification, or other hibited, save by military work of defence in Western Australia, or of any portion thereof, without having previously obtained the permission, in writing, of the Minister for the time being charged with the administration of the defences of the Colony on the recommendation of the Commandant of the Western Australian Military Forces, but such permission may be revoked by the Minister at any time. Such permission shall clearly and expressly state the nature of the sketches,

Sketching, &c., of

56° VICTORIÆ, No. 4.

Safety of Defences.

drawings, photographs, pictures, or paintings which may be made by the person to whom such permission is given, and the place or places of which such sketches, drawings, photographs, pictures, or paintings may be made.

Penalty for offending against provisions of Section 1.

2. ANY person offending against the provisions of the last preceding section shall be liable to a penalty not exceeding One hundred pounds, or, at the discretion of the Justices, to be imprisoned, with or without hard labor, for any period not exceeding six months; and all sketches, drawings, photographs, pictures, and paintings, and all tools and all materials or apparatus for sketching, drawing, photographing, or painting found in his possession shall be forfeited to the Crown, and may be destroyed, sold, or otherwise disposed of as the Governor shall direct.

Penalty on persons found in or near forts with drawing materials, &c.

Penalty—Fine, or imprisonment.

3. ANY person who enters or approaches any fort, battery, fieldwork, fortification, or other military work of defence in the said Colony, with sketching, drawing, photographing, or painting materials or apparatus in his possession, with the intention or apparent intention of committing any breach of the provisions of this Act, shall be liable, upon conviction, to a penalty not exceeding Fifty pounds, and all tools and all materials or apparatus for sketching, drawing, photographing, or painting found in his possession shall be forfeited to the Crown, and may be destroyed, sold, or otherwise disposed of as the Governor shall direct.

Penalty on persons trespassing.

4. ANY person found trespassing on any fort, battery, fieldwork, fortification, or other work of military defence, or on any land reserved for or forming part of such defences, and whether any erection, fort, fortification, or work of any kind may be standing thereon or not, may be summarily arrested without warrant and removed therefrom by any officer or member of the Defence Forces, or any officer or member of the police force, and shall be liable to a penalty not exceeding Twenty pounds.

Penalty on communicating information respecting defences.

5. ANY officer or member of the Defence Forces or officer of the Civil Service who communicates to any person, otherwise than in the course of his official duty, any plans, documents, or other information relating to any fort, battery, fieldwork, fortification, or other work of military defence in Western Australia, or to any other defences of the Colony, shall be guilty of a misdemeanor, and shall, on conviction, be liable to imprisonment for any term not exceeding three years, and not less than one year, and to a fine not exceeding Two hundred pounds, and not less than Fifty pounds.

Proceedings before Justices. 6. ALL proceedings for offences against this Act, except the misdemeanor mentioned in section five, or for the recovery of penalties,

56° VICTORIÆ, No. 4.

Safety of Defences.

shall be heard and determined in a summary way by any Resident Magistrate or two or more Justices of the Peace, under the provisions of an Ordinance of the Governor and Legislative Council, No. 5 of 1850, intituled "An Ordinance to facilitate the performance of the Duties of Justices of the Peace out of Sessions within the Colony of Western Australia, with respect to summary convictions and orders," or of any Act now in force, or hereafter to be in force, relating to the duties of Justices of the Peace with respect to summary convictions and orders.

- 7. THIS Act shall not exempt any person from any proceeding for an offence which is punishable at common law, or by military or naval law, or under any Act other than this Act, so, however, that no person be punished twice for the same offence.
- 8. THIS Act may be cited as "The Safety of Defences Act, short title. 1892."

In the name and on behalf of the Queen I hereby assent to this Act.

W. C. F. ROBINSON, Governor.

VIC. No. 9, 1899.

Criminal Code Act.

CRIMINAL LAW.

An Act to Establish a Code of Criminal Law.

63 Vic. No. 9. THE CRIMINAL CODE ACT, 1899.

[Assented to 28th November, 1899.]

HEREAS it is desirable to Declare, Consolidate, and Preamble.

Amend the Criminal Law: Be it enacted and declared by the Queen's Most Excellent Majesty, by and with the advice and consent of the Legislative Council and Legislative Assembly of Queensland in Parliament assembled, and by the authority of the same, as follows:—

- 1. This Act may be cited as "The Criminal Code short title. Act, 1899."
- 2. On and from the first day of January, one thousand Establishnine hundred and one, the provisions contained in the ment of Code. Code of Criminal Law set forth in the First Schedule to [Schedule I.] this Act, and hereinafter called "the Code," shall be the law of Queensland with respect to the several matters therein dealt with.

The said Code may be cited as "The Criminal Code."

- 3. On and from the coming into operation of the Repeal.
 - (1) The several Statutes of the Realm mentioned in the Second Schedule to this Act shall be [Schedule II.] repealed so far as they are in force in Queensland to the extent in the said Schedule indicated;
 - (2) The several Statutes of New South Wales and Queensland mentioned in the Third Schedule [Schedule to this Act shall be repealed to the extent in III.] the said Schedule indicated:
 - (3) The several Statutes of New South Wales and Queensland mentioned in the Fourth Schedule [Schodule to this Act shall be amended in the manner in the said Schedule indicated, and shall be read and construed as being so amended accordingly.

Provided as follows:—

(1) The repeal of any Statute or part of a Statute saving. set forth in the said Schedules shall not affect the construction of any other Statute, or of any other part of the same Statute, whether as regards the past or the future:

ss. 84-87.

Criminal Code.

63 Vic. No. 9,

PART III.—OFFENCES AGAINST THE ADMINISTRATION OF LAW AND JUSTICE AND AGAINST PUBLIC AUTHORITY.

CHAPTER XII.

DISCLOSING OFFICIAL SECRETS.

Disclosure of Secrets relating to Defences by Public Officers.

84. Any person who, being employed in the Public Service, communicates to any person otherwise than in the course of his official duty any plans, documents, or other information, relating to any battery, field work, or fortification, in Queensland, or relating to any other defence of Queensland, is guilty of a misdemeanour.

If he does so advisedly, he is liable to imprisonment for three

years.

If he does so by negligence, he is liable to imprisonment for one year, or to a fine of one hundred pounds.

Obtaining Disclosure of Secrets relating to Defences.

85. Any person who procures any person employed in the Public Service to make any such communication as is mentioned in the last preceding section, or without lawful authority obtains information as to any such matter as is therein mentioned, is guilty of a misdemeanour, and is liable to imprisonment for three years.

Disclosure of other Official Secrets.

86. Any person who, being employed in the Public Service, publishes or communicates any fact which comes to his knowledge by virtue of his office and which it is his duty to keep secret, or any document which comes to his possession by virtue of his office and which it is his duty to keep secret, except to some person to whom he is bound to publish or communicate it, is guilty of a misdemeanour, and is liable to imprisonment for two years.

CHAPTER XIII. CORRUPTION AND ABUSE OF OFFICE. Official Corruption.

87. Any person who—

(1) Being employed in the Public Service, or being the holder of any public office, and being charged with the performance of any duty by virtue of such employment or office, not being a duty touching the administration of justice, corruptly asks, receives, or obtains, or agrees or attempts to receive or obtain, any property or benefit of any kind for himself or any other person on account of any thing already done or omitted to be done, or to be afterwards done or omitted to be done, by him in the discharge of the duties of his office; or



Official Secrets Act 1911

1911 CHAPTER 28

An Act to re-enact the Official Secrets Act, 1889, with Amendments. [22nd August 1911]

BE IT ENACTED by the King's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:

1 Penalties for spying

- (1) If any person for any purpose prejudicial to the safety or interests of the State—
 - (a) approaches or is in the neighbourhood of, or enters any prohibited place within the meaning of this Act; or
 - (b) makes any sketch, plan, model, or note which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy; or
 - obtains or communicates to any other person any sketch, plan, model, article, or note, or other document or information which is calculated to be or might be or is intended to be directly or indirectly useful to an enemy;

he shall be guilty of felony, and shall be liable to penal servitude for any term not less than three years and not exceeding seven years.

(2) On a prosecution under this section, it shall not be necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State, and, notwithstanding that no such act is proved against him, he may be convicted if, from the circumstances of the case, or his conduct, or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State; and if any sketch, plan, model, article, note, document, or information relating to or used in any prohibited place within the meaning of this Act, or anything in such a place, is made, obtained, or communicated by any person other than a person acting under lawful authority, it shall be deemed to have been made, obtained, or communicated for a purpose prejudicial to the safety or interests of the State unless the contrary is proved.

2 Wrongful communication, &c. of information

- (1) If any person having in his possession or control any sketch, plan, model, article, note, document, or information which relates to or is used in a prohibited place or anything in such a place, or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by any person holding office under His Majesty or which he has obtained owing to his position as a person who holds or has held office under His Majesty, or as a person who holds or has held a contract made on behalf of his Majesty, or as a person who is or has been employed under a person who holds or has held such an office or contract,—
 - (a) communicates the sketch, plan, model, article, note, document, or information to any person, other than a person to whom he is authorised to communicate it, or a person to whom it is in the interest of the State his duty to communicate it, or
 - (b) retains the sketch, plan, model, article, note, or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it:

that person shall be guilty of a misdemeanour.

- (2) If any person receives any sketch, plan, model, article, note, document, or information, knowing, or having reasonable ground to believe, at the time when he receives it, that the sketch, plan, model, article, note, document, or information is communicated to him in contravention of this Act, he shall be guilty of a misdemeanour, unless he proves that the communication to him of the sketch, plan, model, article, note, document, or information was contrary to his desire.
- (3) A person guilty of a misdemeanour under this section shall be liable to imprisonment with or without hard labour for a term not exceeding two years, or to a fine, or to both imprisonment and a fine.

3 Definition of prohibited place

For the purposes of this Act, the expression "prohibited place "means—

- (a) any work of defence, arsenal, factory, dockyard, camp, ship, telegraph or signal station, or office belonging to His Majesty, and any other place belonging to His Majesty used for the purpose of building, repairing, making, or storing any ship, arms, or other materials or instruments of use in time of war, or any plans or documents relating thereto; and
- (b) any place not belonging to His Majesty where any ship, arms, or other materials or instruments of use in time of war, or any plans or documents relating thereto, , are being made, repaired, or stored under contract with, or with any person on behalf of, His Majesty, or otherwise on behalf of His Majesty; and
- (c) any place belonging to His Majesty which is for the time being declared by a Secretary of State to be a prohibited place for the purposes of this section on the ground that information with respect thereto, or damage thereto, would be useful to an enemy; and
- (d) any railway, road, way, or channel, or other means of communication by land or water (including any works or structures being part thereof or connected therewith), or any place used for gas, water, or electricity works or other works for purposes of a public character, or any place where any ship, arms, or other materials or instruments of use in time of war, or any plans or documents

relating thereto, are being made, repaired, or stored otherwise than on behalf of His Majesty, which is for the time being declared by a Secretary of State to be a prohibited place for the purposes of this section, on the ground that information with respect thereto, or the destruction or obstruction thereof, or interference therewith, would be useful to an enemy.

4 Attempts to commit offence, or- incitement to commit offence, under Act

Any person who attempts to commit any offence under this Act, or incites, or counsels, or attempts to procure another person to commit an offence under this Act, shall be guilty of felony or of a misdemeanour according as the offence in question is felony or misdemeanour, and on conviction shall be liable to the same punishment, and to be proceeded against in the same manner, as if he had committed the offence."

5 Person elmrged with felony under Act may be convicted of misdemeanour under Act

Any person charged with an offence which is a felony under this Act may, if the circumstances warrant such a finding, be found guilty of an offence which is a misdemeanour under this Act.

6 Power to arrest

Any person who is found committing an offence under this Act, whether that offence is a felony or not, or who is reasonably suspected of having committed, or having attempted to commit, or being about to commit, such an offence, may be apprehended and detained in the same manner as a person who is found committing a felony.

7 Penalty for harbouring spies

If any person knowingly harbours any person whom he knows, or has reasonable grounds for supposing, to be a person who is about to commit or who has committed an offence under this Act, or knowingly permits to meet or assemble in any premises in his occupation or under his control any such persons, or if any person having harboured any such person, or permitted to meet or assemble in any premises in his occupation or under his control any such persons, wilfully refuses to disclose to a superintendent of police any information which it is in his power to give in relation to any such person he shall be guilty of a misdemeanour and liable to imprisonment with or without hard labour for a term not exceeding one year, or to a fine, or to both imprisonment and a fine.

8 Restriction on prosecution

A prosecution for an offence under this Act shall not be instituted except by or with the consent of the Attorney-General :

Provided that a person charged with such an offence may be arrested, or a warrant for his arrest may be issued and executed, and any such person may be remanded in custody or on bail, notwithstanding that the consent of the Attorney-General to the institution of a prosecution for the offence has not been obtained, but no further or other proceedings shall be taken until that consent has been obtained.

9 Search warrants

- (1) If a justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorising any constable named therein to enter at any time any premises or place named in the warrant, if necessary, by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note, or document, or anything of a like nature or anything which is evidence of an offence under this Act having been or being about to be committed, which he may find on the premises or place or on any such person, and with regard to or in connexion with which he- has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.
- (2) Where it appears to a superintendent of police that the case is one of great emergency and that in the interest of the State immediate action is necessary, he may by a written order under his hand give to any constable the like authority as may be given by the warrant of a justice under this section.

10 Extent of Act and place of trial of offence

- (1) This Act shall apply to all acts which are offences-under this Act when committed in any part of His Majesty's dominions, or when committed by British officers or subjects elsewhere.
- (2) An offence under this Act, if alleged to have been committed out of the United Kingdom, may be inquired of, heard, and determined, in any competent British court in the place where the offence was committed, or in the High Court in England or the Central Criminal Court, and the Criminal Jurisdiction Act, 1802, shall apply in like manner as if the offence, were mentioned in that Act, and the Central Criminal Court as well as the High Court possessed the jurisdiction given by that Act to the Court of King's Bench.
- (3) An offence under this Act shall not be tried by any court of general or quarter sessions, nor by the sheriff court in Scotland, nor by any court out of the United Kingdom which has not jurisdiction to try crimes which involve the greatest, punishment allowed by law.
- (4) The provisions of the Criminal Law and Procedure (Ireland) Act, 1887, shall not apply to any trial under the provisions of this Act.

11 Saving for laws of British possessions

If by any law made before or after the passing of this Act by the legislature of any British possession provisions are made which appear to His Majesty to be of the like effect as those contained in this Act, His Majesty may, by Order in Council, suspend the operation within that British possession of this Act, or of any part thereof, so long as that law continues in force there, and no longer, and the Order shall have effect as if it were enacted in this Act:

Provided that the suspension of this Act, or of any part thereof, in any British possession shall not extend to the holder of an office under His Majesty who is not appointed to that office by the Government of that possession.

Status: This is the original version (as it was originally enacted).

12 Interpretation

In this Act, unless the context otherwise requires,—

Any reference to a place belonging to His Majesty includes a place belonging to any department of the Government of the United Kingdom or of any British possessions, whether the place is or is not actually vested in His Majesty;

The expression "Attorney-General" means the Attorney or Solicitor-General for England; and as "inspects Scotland, means the Lord Advocate; and as respects-Ireland, means the Attorney or Solicitor-General for Ireland and, if the prosecution is instituted in any court out of-the United Kingdom, means the person who in that court is Attorney-General, or exercises the like functions as the Attorney-General in England;

Expressions referring to communicating or receiving include any communicating or receiving, whether in whole or in part, and whether the sketch, plan, model, article, note, document, or information itself or the substance, effect, or description thereof only be communicated or received; expressions referring to obtaining or retaining any sketch, plan, model, article, note, or document, include the copying or causing to be copied the whole or any part of any sketch, plan, model, article, note, or document; and expressions referring to the communication of any sketch, plan, model, article, note or document include the transfer or transmission of the sketch, plan, model, article, note or document;

The expression "document" includes part of a document;

The expression "model" includes design, pattern, and specimen;

The expression "sketch" includes any photograph or other mode of representing any place or thing;

The expression " superintendent of police " includes any police officer of a like or superior rank;

The expression "office under His Majesty" includes. any office or employment in or under any department of the Government of the United Kingdom, or of any British possession; r

The expression "offence under this Act" includes, any act, omission, or other thing which is punishable under this Act.

13 Short title and repeal

- (1) This Act may be cited as the Official Secrets Act, 1911.
- (2) The Official Secrets Act, 1889, is hereby repealed.

DEFENCE.

No. 20 of 1903.

An Act to provide for the Naval and Military Defence and Protection of the Commonwealth and of the several States.

[Assented to 22nd October, 1903.]

BE it enacted by the King's Most Excellent Majesty, the Senate, and the House of Representatives of the Commonwealth of Australia, as follows:—

PART I.—INTRODUCTORY.

Short title.

1. This Act may be cited as the Defence Act 1903.

Parts.

2. This Act is divided into Parts as follows:—

Part I.—Introductory, ss 1-7.

Part II.—Administration.

Division 1.—Officers and Military Districts, ss 8–28.

Division 2.—Naval and Military College, s 29.

Part III.—The Defence Force.

Division 1.—Constitution of the Defence Force, ss 30-32.

Division 2.—The Raising of the Defence Force and the Enlistment and Discharge of Members thereof, ss 33-44.

Division 3.—The Service of the Forces, ss 45-51. Division 4.—General Provisions, ss 52-58.

Part IV.—Liability to serve in the Militia Forces in time of war, ss 59-61.

Part V.—Cadets, s 62.

Part VI.—Special Powers in relation to Defence, ss 63-72.

Part VII.—Offences, ss 73–85.

Part VIII.—Courts-Martial, ss 86–100.

Part IX.—Legal Procedure, ss 101-116.

Part X.—Miscellaneous, ss 117-123.

Part XI.—Regulations, s 124.

Commencement of Act.

3. This Act shall commence on a day to be fixed by proclamation.*

^{*} Proclaimed to commence 1st March, 1904. See Gazette, 20th February, 1904.

- (c) Any vehicle employed only in conveying members of the Defence Force on march or duty or any prisoner under their charge or conveying naval or military arms stores or baggage; or
- (d) Any animal drawing any such vehicle.

Stopping traffic.

71. The officer in charge of any artillery or rifle range may stop all traffic, during artillery or rifle practice, on any road or water-way crossing the line of fire or in dangerous proximity thereto.

Regulations as to traffic. 72. No ships boats or persons shall come or remain within the prescribed distance of any ship battery gun or person engaged in artillery or rifle practice, or shall remain in any position so as to obstruct such practice.

PART VII.—OFFENCES.

73.—(1.) Any officer who—

Claiming for drills not performed.

Returning men not enrolled.

- (a) knowingly and except as prescribed claims pay on account of any drill performed with his corps for any man belonging to any other corps; or knowingly claims pay for officers or men not present; or
- (b) knowingly includes in any parade state, or other return, the name of any person not duly enlisted and attached as a member of the Defence Force; and
- (2.) Any soldier or sailor who-

Claiming for drills performed with another corps.

- (c) knowingly and except as prescribed claims or receives pay on account of any drill performed in the ranks of any corps, other than his own proper corps; and
- (3.) Any member of the Defence Force who—

Obtaining pay by false pretences. (d) knowingly obtains by means of any false pretence any pay or money belonging or payable to any other member of the Defence Force; or

Fraudulently retaining pay.

- (e) knowingly retains or keeps in his possession with intent to apply it to his own use any pay or money belonging or payable to any other member of the Defence Force; and
- (4.) Any member of the Defence Force or officer in the Public Service of the Commonwealth who—

Unlawfully giving information as to defences.

- (f) communicates to any person otherwise than in the course of his official duty any plan document or information relating to any fort battery fieldwork fortification or defence work or to any of the defences of the Commonwealth; and
- (5.) Any person who—

Unlawfully obtaining information as to defences.

(g) unlawfully obtains any plan document or information relating to any fort battery fieldwork fortification or defence work or to any of the defences of the Commonwealth; or

1903.

- (h) knowingly signs a false parade state, roll, or pay list or False parade states, &c. return: or
- (i) forges or utters, knowing it to be forged, any warrant or Forgery. order under this Act; or
- (j) falsely personates any other person at any parade or on False any occasion when the latter is required by this Act to do any act or attend at any place; and

(6.) Any contractor purveyor or other person and any employé Penalty for of any such contractor purveyor or other person who fraudulently and supplying interior knowingly supplies to the Commonwealth or any officer of the provisions, material, Commonwealth for use by the Defence Force or any part thereof any equipment, &c. article of food which is inferior in quality or quantity to that specified in the contract agreement or order under which it is supplied, or any material, equipment, or beast of draught or burden, which is inferior to that specified in the contract agreement or order under which it is supplied, and any officer of the Commonwealth who fraudulently and knowingly receives for use by the Defence Force or any part thereof any article of food or any material, equipment, or beast of draught or burden supplied in contravention of this sub-section—

shall be guilty of an indictable offence, and shall be liable to imprisonment, with or without hard labour, for any period not exceeding three years.

74.—(1.) Any person, of whom information is required by any Refusing officer or person in order to enable him to comply with the provisions required information of this Act relating to enlistment or enrolment, who refuses or neglects or neglects or neglects or neglects or neglects or neglects or neglects. (without just cause, proof whereof shall lie upon him) to give such information, or gives false information, shall be liable to a penalty not exceeding Five pounds for each item of information demanded and refused or neglected to be given or falsely given.

(2.) Any person appointed in that behalf who (without just cause, Refusing proof whereof shall lie upon him) refuses or neglects to make any to make enrolment. enrolment, or to make or transmit, in the prescribed manner, any prescribed roll or return, or copy thereof, shall be liable to a penalty not exceeding Fifty pounds.

75. Any person who—

Resisting draft, &c.

- (1) fails to enlist when required by this Act so to do; or
- (2) counsels or aids any person, called upon by proclamation to enlist in the Militia Forces, to fail to enlist or to evade enlistment; or
- (3) counsels or aids any person who has enlisted or who is liable to enlist in any part of the Defence Force not to perform any duty he is required by this Act to perform,

shall be liable to imprisonment, with or without hard labour, for any period not exceeding six months.

DAYLIGHT SAVING REPEAL.

No. 35 of 1917.

An Act to repeal the Daylight Saving Act 1916.

[Assented to 25th September, 1917]

BE it enacted by the King's Most Excellent Majesty, the Senate, and the House of Representatives of the Commonwealth of Australia, as follows:—

- 1. This Act may be cited as the Daylight Saving Repeal Act short title. 1917.
 - 2. The Daylight Saving Act 1916 is hereby repealed.

Repeal of Daylight Saving Act.

DEFENCE.

No. 36 of 1917.

An Act to amend the Defence Act 1903-1915.

[Assented to 25th September, 1917.]

BE it enacted by the King's Most Excellent Majesty, the Senate, and the House of Representatives of the Commonwealth of Australia, as follows:—

1.—(1.) This Act may be cited as the Defence Act 1917.

Short title and citation.

- (2.) The Defence Act 1903-1915 is in this Act referred to as the Principal Act.
- (3.) The Principal Act, as amended by this Act, may be cited as the Defence Act 1903-1917.(a)
 - 2. Section four of the Principal Act is amended—

Amendment of

(a) by omitting the definition of "Active service" and inserting in its stead the following definition:—

"'Active service' has a meaning corresponding to that of the same words as used in sub-section (1.) of section one hundred and eighty-nine of the Army Act defining the expression 'on active service.'":

⁽a) For copy of Defence Act 1903-1917, see p. 127 infra.

shall be deemed to be on war service and shall be subject to the Army Act as if they were part of His Majesty's Regular Land Forces, with such modifications and adaptations as are prescribed.

"(2.) Subject to any Imperial Act, members of the Imperial Forces serving in Australia with the Defence Force shall be subject to this Act.

"(3.) This section shall be construed as amplifying and not as

restricting any of the other provisions of this Act.".

offence so that it exceeds Twenty pounds.".

15. Section fifty-five of the Principal Act is repealed and the following section inserted in its stead:

"55. The Military Forces shall at all times, whilst on war military Forces service, whether within or without the limits of the Commonwealth, on war service subject to be subject to the Army Act save so far as it is inconsistent with Army Act. this Act and subject to such modifications and adaptations as are prescribed, including the imposition of a fine not exceeding Twenty pounds for an offence either in addition to or in substitution for the punishment provided by the Army Act, and the increase or reduction of the amount of a fine provided by the Army Act:

Provided that the regulations shall not increase the fine for any

16. Section fifty-seven of the Principal Act is amended by Amendment of omitting the word "active" (wherever occurring) and inserting in 8.57. its stead the word "war".

17. Section sixty-three of the Principal Act is amended by Amendment of. inserting in sub-section (3.) thereof—

- (a) after the words "other than" the words "appointments of persons in a civil capacity in pursuance of this section and"; and
- (b) after the words "five years therein" the words "or have served on active service as prescribed".
- 18. Section seventy-three of the Principal Act is repealed and the following sections are inserted in its stead:—

"73.—(1.) Any member of the Defence Force who—

Falsifying pay

- (a) except as prescribed, knowingly claims pay on account of any drill with his corps for any man belonging to any corps: or
- (b) knowingly claims pay for any member of the Defence Force not present; or
- (c) knowingly includes in any parade state, or other return, the name of any person who is not a member of the Defence Force.

shall be guilty of an offence.

"(2.) Any member of the Defence Force who—

(a) except as prescribed, knowingly claims or receives pay on improperly. account of any drill performed in any corps, other than his own proper corps; or

(b) knowingly claims or receives pay on account of any drill or duty not performed,

shall be guilty of an offence.

Fraudulently obtaining or retaining pay,

- "(3.) Any member of the Defence Force who-
 - (a) knowingly obtains by means of any false pretence any pay or money belonging or payable to any other member of the Defence Force; or
- (b) knowingly retains or keeps in his possession with intent to apply it to his own use any pay or money belonging or payable to any other member of the Defence Force,

shall be guilty of an offence.

Unlawfully giving or obtaining information as to defences.

- "73a.—(1.) Any member of the Defence Force or officer in the Public Service of the Commonwealth who communicates to any person otherwise than in the course of his official duty any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or any other naval or military information, shall be guilty of an offence.
- "(2.) Any person who unlawfully obtains any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any of the defences of the Commonwealth or any other naval or military information, shall be guilty of an offence.

Falsifying and forging parade states, orders, &c.

- "73B. Any person who—
 - (a) knowingly signs a false parade state roll or pay list or return; or
- (b) forges or utters, knowing it to be forged, any warrant or order under this Act; or
- (c) falsely personates any other person at any parade or on any occasion when the latter is required by this Act to do any act or to attend at any place,

shall be guilty of an offence.

Supplying inferior provisions, material or equipment.

- "73c.—(1.) Any contractor, purveyor or other person, and any employee of a contractor, purveyor or other person, who fraudulently supplies to the Commonwealth or any officer of the Commonwealth for use by the Defence Force—
 - (a) any article of food which is inferior in quality to or less in quantity than that specified in the contract, agreement or order under which it is to be supplied; or
 - (b) any material, equipment, or beast of draught or burden which is inferior to that specified in the contract, agreement or order under which it is to be supplied,

shall be guilty of an offence.

"(2.) Any officer of the Commonwealth who fraudulently receives for use by the Defence Force any article of food, or any material, equipment, or beast of draught or burden supplied in contravention of this section, shall be guilty of an offence.

Penalty.

- "73D. The punishment for an offence against any of the four last preceding sections shall be as follows:—
 - (a) if the offence is prosecuted summarily—a fine not exceeding Twenty pounds or imprisonment for a term not exceeding six months;

- (b) if the offence is prosecuted upon indictment—imprisonment with or without hard labour for any term not exceeding three years.".
- 19. Section seventy-four of the Principal Act is amended—

Amendment of

(a) by omitting the words "liable to a penalty not exceeding Five pounds for each item of information demanded and refused or neglected to be given or falsely given" and inserting in their stead the words "guilty of an offence.

> Penalty: Imprisonment for twelve months or Twenty pounds for each item of information demanded and refused or neglected to be given or falsely given, or both"; and

- (b) by adding at the end thereof the following sub-section:—
- "(3.) Where an offence against this section is tried by courtmartial the court may, in lieu of sentencing the offender to imprisonment sentence him to detention for the same period as that for which he might have been sentenced to imprisonment or for any less period.".
- 20. Section seventy-eight of the Principal Act is repealed and the following section inserted in its stead:—
- "78. Any member of the Citizen Military Forces who, having been Absence for required to serve pursuant to a proclamation made under Part III. of this Act, and any person who, having been required to serve pursuant to Part IV. of this Act, absents himself without leave for a longer period than seven days from his corps or from the place at which he should be present, shall be deemed to be a deserter and shall be liable to the punishment provided for desertion, by the Army Act.".

- 21. After section eighty of the Principal Act the following sections are inserted:—
- "80A.— (1.) Any person who falsely represents himself to be a realist rend soldier or sailor shall be guilty of an offence.

 The Contradict rendered represents himself to be a required to be returned soldier or sailor. returned soldier or sailor shall be guilty of an offence.

Penalty: One hundred pounds or imprisonment for six months, or both.

"(2.) For the purposes of this section—

(a) 'returned soldier' means a person who has served abroad during any war as a member of any Military Force raised in Australia or in any other part of the British Empire, or, during the present war, as a member of the Military Forces of any Ally of Great Britain; and

(b) 'returned sailor' means a person who has served abroad during any war as a member of any Naval Force raised in Australia or in any other part of the British Empire, or, during the present war, as a member of the Naval

Forces of any Ally of Great Britain.

"(3.) In any proceedings for an offence against this section the averment of the prosecutor that the defendant is not a returned soldier or sailor shall be deemed to be proved in the absence of proof to the contrary.



Defence Legislation Amendment (Application of Criminal Code) Act 2001

Act No. 141 of 2001 as amended

This compilation was prepared on 3 June 2003

[This Act was amended by Act No. 63 of 2002 and Act No. 135 of 2003]

Amendments from Act No. 63 of 2002

[Schedule 2 (item 10) amended Item 41 of Schedule 1 Schedule 2 (item 10) commenced on 2 October 2001]

Amendments from Act No. 135 of 2003

[Schedule 2 (item 28) repealed and substituted subsection 2(2)] Schedule 2 (item 9) commenced on 1 October 2001]

Prepared by the Office of Legislative Drafting, Attorney-General's Department, Canberra

G:\Legislation\pasteact\DefLegAmAppCrimCode2001.doc 7/6/2004 8:40 AM

(c) knows that the evidence is false or misleading in the material particular.

Penalty: Imprisonment for 6 months.

8 Sections 73 to 73E

Repeal the sections, substitute:

73A Unlawfully giving or obtaining information as to defences

- (1) A person who is a member of the Defence Force or a person appointed or engaged under the *Public Service Act 1999* is guilty of an offence if:
 - (a) the person communicates to any other person any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air force aerodrome or establishment or any other naval, military or air force information; and
 - (b) the communication is not in the course of the first-mentioned person's official duty.
- (2) A person is guilty of an offence if:
 - (a) the person obtains any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or air force aerodrome or establishment, or to any of the defences of the Commonwealth or any other naval, military or air force information; and
 - (b) that conduct is unlawful.

9 Subsections 73F(1) and (2)

Omit ", 73C, 73D or 73E".

10 Paragraph 79(1)(c)

Omit "except for lawful cause (the proof of which shall lie upon him)".

11 After subsection 79(1)

Insert:

(1AA) An offence under subsection (1) is an offence of strict liability.



INSTRUCTIONS FOR THE SECURITY

OF OFFICIAL DOCUMENTS

AND INFORMATION

PRIME MINISTER'S DEPARTMENT 19th October, 1948.

354.07145 Photo-lithographed, by Authority: 94007145 GOURLEY, Government Printer, Welbourge.

FOREWORD

documents and information within Commonwealth Departments and Instru-This booklet contains instructions for the security of official mentalities.

the entire British Commonwealth. Apart from the requirements of defence. defence of the British Commonwealth. Thus we have undertaken important caution must be taken to prevent the leakage of information in relation to these matters, the security of which may be wital to the defence of it is essential to orderly administration that no official information Australia is being called upon to take an increasing share in the defence commitments of a highly secret nature, such as the Long Range Commonwealth Departments and Instrumentalities. Every possible pre-Guided Weapons Project, aspects of which will concern a number of of any kind should be disclosed except in the course of duty.

in the attainment of security of documents and information. I commend These instructions outline principles and methods to be applied them to the careful attention of all whose duties they may concern.

J. B. CHIFLEY

PRIME MINISTER.

1		
1		
,		

(Ŧ)

02 CONTENT

Page	1 - 2	1 5	0	2	2 - 3	M	М	3 - 4	77	1 60	2	9 - 9	9	9	9	7	7	7 - 8	8 - 10	α) 0	1	9 - 10	10	2	0	10 - 11	10	10	10 - 11
Paragraph	1 - 5	6 : 9	9	7	7(a)	7(b)	7(c)	7(a)	8 - 8	10 - 18	10 - 11	12	13	14 - 18	15	16	17	18	19 - 23	0	000	3	21	22	0	,	24 - 28	24	25	26
	4	DOCUMENTS	:	3	1	*	5(9)2	***	ION OF	SSION	REGISTRIES	*	× *		:			2.6	MESSAGES			STAMPED WITH		1	ga.		:		200 Au	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
	:	OFFICIAL DO	CATION		*	* 0		* *	IN CLASSIFICATION	TRANSMISSION	SPECIAL	*		DOCUMENTS -	**	9.4	2	2	OF CYPHER			TEXTS STAME			CLEAR TEXTS	6	3	*	140	NOT T
	ä	Ä4 O	CLASSIFICATION	. SN			100	8.8		ATION AND	DOCUMENTS:	DOCUMENTS	344	TED DOCE	DESPATCH	ř	20	1	TEXT	7	PRECAUTIONS	EAR	 G	TORS	OF		3	BUSINESS	[E2]	P.
	3	CLASSIFICATION	PURPOSE OF	CLASSIFICATIONS	*	2	34.6		SE APPLIED	USTODY, CIRCULATION OF CLASSIFIED DOCUM	CLASSIFIED DO	FIED	TS	급	AND DESF	ŧ	í		Y OF CLEAR	:	SPECIAL PRE	ENT OF	E WARNING"	ORIGINATORS	TELEPHONING 25)		TEOUS	ы	CLASSI	1
	INTRODUCTION	PART I - THE CLASS	£	7	Top Secret	Secret	Confidential	ted	PRINCIPLES TO E	PART II - CUSTODY, OF CLAS	D OI	DY OF		TRANSMISSION CF	ION	CARRIAGE		SAFE HAND	PART III - SECURITY	GENERAL	REASONS FOR SPE	70	THE "PARAPHRASE	N DY	RESTRICTION ON 1		PART IV - MISCELLANEOUS	NO NC	SECURITY OF TELE TRANSMISSION OF	_

CONTENTS - continued.

Faragraph Page

		12
	2 2 2 8	
PART IV - continued.	TRANSMISSION BY TELEGRAM, CABLE OR WIRELESS DESTRUCTION OF OFFICE WASTE	APPENDIX "A" - METHOD OF SEALING ENVELOPES

RESTRICTED

INSTRUCTIONS FOR THE SECURITY OF OFFICIAL DOCUMENTS AND INFORMATION

INTRODUCTION

1. The purpose of this booklet is to outline the principles to be followed by Commonwealth Departments and offices concerning the safe-guarding of official documents and information. It replaces the instructions issued by the Prime Minister's Department on 1st July, 1944.

2. The irregular disclosure of official information may be attended with serious consequences ranging from administrative embarrassment to the Government to jeopardising the security of the nation. It is imperative that all Commonwealth officers should be fully seized of their responsibilities in this matter, and that each Department should give careful attention to the security of official information which it handles.

discretion, and care of officers to whose knowledge it comes, and secondly upon an effectively supervised system within each Department, Branch, and Section. Such a system should ensure that access to documents and information of a confidential nature is limited to those officers who require it in the course of their duties, and that adequate measures are taken at all times for the physical security of such documents. Officers are not entitled to see documents of this nature solely by wirtue of their status or office. Effective office security measures may often result in some additional work and administrative inconvenience. This must be accepted in the interests of national security.

4. Attention is directed to the following provisions of the Public Service Regulations and of the Crimes Act :-

"Except in the course of official duty, no information concerning public business or any matter of which an officer has knowledge officially shall be given, directly or indirectly, nor shall the contents of official papers be disclosed by an officer without the express authority of the Chief Officer." (Regulation 35 - Public Bervice Regulations.)

Any person who, being a Commonwealth officer, publishes or cummunicates any fact which comes to his knowledge by virtue of his comes to his possession by virtue of his office, and which it is his duty to keep secret, except to some person to whom he is suthor! a to publish or communicate it, shall be guilty of an offence."

Imprisonment for two years. (Section 70 of the Crimes Act.)

5. For the purpose of these instructions the term "document" includes any form of recorded information. Cables, signals, or other material which has been transmitted in appher are, however, subject to certain additional safeguards to preserve the security of the appher amployed. Cypher Security is dealt with through the Cypher Security Committee, which is part or the Higher Defence Machinery. Certain instructions of general application on this subject are included as Part III of this booklet. The Cypher Security Committee is responsible for recommending further special instructions which will be brought to the notice of those concerned.

PART 1 - THE CLASSIFICATION OF OFFICIAL DOCUMENTS

- according to the relative importance of the security of their contents. Each of these ontegories or "classifications" is the subject of special throughout the British Commonwealth. The process of allocating a docurules design of to restrict the circulation of, and otherwise safeguard Documents so treated are referred to as "classified" docuof their contents, will require special measures for their protection. A system has accordingly been evolved whereby documents which contain Whilst it is most imporcontained in any official document, certain documents, by the nature tant that there should be no unauthorised disclosure of information information of this nature are allocated to one of four categories ment to a security category is referred to as "classification" or the information contained in the document. This system is common ments; otherwise they are referred to as "unclassified". NATURE AND PURPOSE OF CLASSIFICATION. -"grading". 9
 - 7. SECURITY CLASSIFICATIONS. The four security "classifications" or "gradings" are -

TOP SECRET SECRET CONFIDENTIAL RESTRICTED.

These "classifications" are defined hereunder, and a few illustrations are given of their application. The illustrations are not intended to be exhaustive, and each document must be classified on its merits in the light of the definitions.

(a) Top Secret:

Documents, information, and material, the uneuthorised in closure of which would cause exceptionally grave damage to the

nation.

This category is reserved for the nation's closest secrets and is to be used with great reserve.

М

The following illustrations may provide some guidance :

- (1) Political preliminaries to major pacts and alliances.
- (11) Information relating to new and far reaching experimental, technical and scientific developments in methods of warfare.
- (111) Major governmental projects such as drastic proposals to adjust the nation's economy (before official publication).
 - (1v) Critical information relating to vital strategic areas.

(b) Secret:

Documents, information, and material, the unauthorised diselegance of which would endanger national security, cause serious injury to the interest or prestige of the nation or of any governmental activity thereof, or would be of great advantage to a foreign nation.

Illustrations. -

- Proposals for new schemes of governmental or other controls, foreknowledge of which would seriously prejudice their operation.
- (11) High level directives desling with important negotiations (as distinct from major negotiations which would be in the Top Secret category) with other countries.
- (iii) Decuments containing wer plans or details of schemes for the defence of areas other than vital strategic areas, including plans or particulars of operations connected with them.
- v) Vital military information including photographs relating to important defences, establishments and installations.
- (v) Information concerning foreign countries, the value of which depends upon the country concerned not knowing we possess it.
- (v1) Information on the supply of vital strategic materials.

(c) Confidential:

Documents, information, and material, the unauthorised discolorure of which, while not endangering the national security.

Would be prejudicial to the interests or prestige of the nation, any governmental activity, or would cause administrative embarrassment or difficulty or be of advantage to a foreign power.

Illustrations.

- (1) Departmental reports which, while not Secret, would be of adventage to a foreign power.
- (ii) Plane of Government projects such as land development, hydro-electric schemes, road development, or development of areas.
 - (111) Routine Service reports for example on operations or exercises which contain information of advantage to a foreign power.
 - (1v) Cartain personnel records and staff matters.

(d) Restricted.

Documents or information (other than Top Secret. Secret or anyone except for a new our our or be bublished or communicated to

- (1) Departmental books of instruction and training and technicel documents intended for official use only or not intended for release to the public.
- (11) Routing documents relating to the supply and procurement of military stores.

PRINCIPLES TO BE APPLIED IN CLASSIFICATION OF DOCUMENTS.

- followed in 8. The following are the more important principles to be classifying documents
- documents in the same series, or the grading of a classified file of which a document happens to be part, should not influence the grading of a document. A document must not, however, bear a lower classification than the highest classification of any of its appendices or attachments. Each strachment, etc., must be graded on its own individual merits. (a) A <u>document</u> is graded on its merits, that is to say it is graded according to the nature, source, and implications of the information contained therein. Factors such as the grading of other
- file containing classified documents is graded according to the highest classification of any documents contained therein. For this reason, it may sometimes be found desirable to break a file into two or more parts, one part to contain the higher category pepere. 9
 - The security classification of a document is not necessarily a permanent quality attaching to it. Classified matter should be kept under constant revision and "downgraded" to a lower category as the need for protection diminishes, or made unclassified when classification is no longer necessary. 0
 - Documents must be downgraded only on the instructions of, or with the permission of the originating authority, who will inform sil recipients or holders of the particular documents of the new The authority to downgrade documents is to be confined to senior officers. classification. 9
- Some departments Experience has shown that it is desirable to have distinctive file covers for Top Secret and Secret files. Some department have distinctive covers for all four classifications. 9
- Top Secret documents and all documents for which recipients have to account periodically are not to be reproduced in whole or part, except with the approval of the originating authority. This permission will not extend beyond a specified number of copies which are to be accorded the same treatment as the original. (F)
- ment than its contents warrant ("overgrading") must be carefully guard-The tendency to allot a higher security classification to a docued against. Overgrading encourages neglect of the rules for the protection of classified documents and thus endangers the whole system.

- CUSTODY, CIRCULATION AND TRANSMISSION OF CLASSIFIED DOCUMENTS

PART II

ACCESS TO CLASSIFIED DOCUMENTS: SPECIAL REGISTRIES.

of co-ordination and co-operation. On the other hand, too is not necessary for the entire contents of a classified document to be should be passed only to those officers to whom it is necessary for the wide a circulation will tend to prejudice the security of the informa-The guiding principle is that information fulfillment of their duties. Officers are not entitled to see classmade available to a particular officer, he should be acquainted only A balanced assessment of these conflicting claims is often a 10. Failure to impart information on a sufficiently wide basis may ified documents solely by wirtue of their status or office. with those facts relevant to his duties, matter of some difficulty. lead to lack

these docu-11. In addition to those officers who require to study classified doc-Special arrangements are necessary to ensure that this work is entrusted to selected members of under conditions which do not permit others to view or have matter must be maintained in separate sections of central registries, It is for the consideration of Departments whether Top Secret matter should not be ex-For these reasons, Top Secret and Secret uments in the course of their duties, certain other members such as registry clerks and typists, will necessarily handle the staffs of which have been carefully selected. cluded entirely from the Central Registry system. ments in the normal course of administration. access to the documents. the staff

GUSTODY OF CLASSIFIED DOCUMENTS. - Whilst it is not practicable to lay down detailed rules for the custody of classified documents, there are certain safeguards which are fundamental; these are as follows :-(a) When hot actually in use, Top Secret and Secret documents must

always be kept in a fireproof safe or want which should not be accessible to unauthorised persons.

After office hours, keys, if not retained by the After office, in a locked safe or left in charge of officer. Locks should be changed if a key is of the branch or section. (b) Keys to these safes or vaults must be held by a responsible

Ø A eglater of Top Secret documents held must be maintained and cheek should be carried out frequently, in order to bring to light an deficiencies at an early date.

which the instructions of the originator, must be accounted for periodically to the originator.

must be made for the safe custody of Confidenwestricted documents when not in use.

- Officers must ensure that classified documents are not left lying open or unguarded on deaks where they can be read by visitors or other unauthorised persons. (F)
- Doors of rooms in which classified documents are kept must be locked when rooms are vacant. (8)

the compromise, and that such action as is considered necessary towards notified in order that any steps may be taken to limit the extent of document, the officer reaponaible for the security of documents must The originating authority will at once be In the event of the loss of a classified recovery of the document is initiated. LOSS OF DOCUMENTS. be informed immediately.

PRANSWISSION OF CLASSIFIED DOCUMENTS.

only be formulated in the light of the special circumstances pertaining 14. Every Department must adopt a systematic procedure for the trans-Whilst the detailed procedure can in each Deportment, there are fundamental safeguards which must be G There are three general stages in the transmission mission of classified documents. material, namely :adhered to.

Origination and despatch Delivery and receipt Carriage

- The following security safeguards are applicable to the origination and despatch of material :-DESPATCH. -ORIGINATION
- other places in the document as the originating authority deems advisable. In the case of Top Secret and Secret documents, the classification must appear on each sheet of the document. The classification of appendices or attachments is dealt with in paragraph 8(a) above. (a) The security classification must be indicated in bold letters at the top centre of the front sheet of the document and at such
- ification of the material and being wax sealed, the outer envelope bearing only the address. The wax seal renders it difficult to tamper with the contents in transit, whilst the plain outer envelope does not attract attention to the classification of matter contained therein. The security classification must not be shown on the outer envelope. Confidential and Restricted enclosed in two envelopes, the inner envelope showing the class-The correct method of sealing If the material is classified Top Secret or Secret, it must be matter is not usually wax sealed, and may be enclosed in one envelope; however, the outer envelope must not disclose the classification of the contents. The correct method of sealin envelopes is shown in Appendix "A". 9
 - A register of all recipients of each Top Secret document originated in the Department must be maintained. 9
- Top Secret documents are to be covered by a receipt system. It is left to the discretion of Departments whether receipts are to be obtained from recipients of all or any Secret or other lified documents. The receipt form may conveniently be included with the documents. (P)
- Where material is for delivery by "Safe Hand", the outer envelope should be inscribed accordingly in bold lettera. (See paragraph 18 "Safe Hand".) (e)

CARRIAGE. -16.

- appliances must never be despatched by civil post, but by "Safe Hand" (See paragraph 18 - "Safe Hand".). Other Secret matter should not be mission within Australia is left to the discretion of the originating (a) Top Secret matter, also classified code and cypher books and sent by civil post if a more secure means is available, and then only Australia. Postal registration of Confidential documenta for transauthority. All classified matter for transmission to destinations outside Australia should be forwarded as described in paragraph 18 provided it is sent by registered post within the Commonwealth of
- (b) For internal circulation within a Department, Top Secret papers practicable, Top Secret documents may be delivered personally to the recipient in locked boxes or bags, or enclosed in two envelopes, the abould be passed by hand of responsible officers. If this is not inner one as outlined in paragraph 15(a).
- 17. DELIVERY. Top Secret documents should be addressed to and opened only by the person for whom the information is intended, or by a representative authorised for that purpose. Secret matter addressed to a Registry, or an officer apecially appointed for that purpose. general address should be opened by the Officer-in-Charge
- patched to the addressee in the personal care of an authorised officer The following rules 18. "SAFE HAND" TRANSMISSION WITHIN AUSTRALIA AND TRANSMISSION OVERor a succession of authorised officers who are personally responsible Transmission of material by "Safe Hand" means that it is desfor the carriage and safekeeping of the material. apply to "Safe Hand" transmission :-

(A) Carriage entirely within Australia:

- (a) Classification of material requiring "Safe Hand" transmission :-
- (1) All Top Secret meterial;
- classified contente (11) On occasions, depending on the nature and certain other classified material, e.g., code and cypher books and appliances.
- (h) Methods:
- (1) By hand of a responsible officer(s) appointed to liver the material to the addressee;

de

- Care of the Captain of an aircraft of an Australian Airline Company which has been authorised to carry 'Safe Hand" material.
- Despatch overseas to a destination within British territory and if carried by air on a route which does not traverse or touch non-British territory: (11)
- (a) Classification of material requiring "Safe Hand" trans--: moissim

- (1) All Top Secret and Secret material;
- On occeasions, depending on the nature and contents, certain other classified material, e.g., classified code and cypher books and appliances.
- (b) Methoda:
- (1) By hand of a responsible officer(s) appointed to de-liver the material to the addresses;
- (11) By diplomatic bag through the Department of External Affairs;
- (111) Care of the captain of an aircraft of a British Air-line Company which has been authorised to carry "Safe Hand" material. Departments should refer, in the first instance, to the Department of External Affairs in connection with arrangements for the use
- Care of the Master of a British vessel; the material is placed in the personal care of the Master. Departments should make arrangements for transmission by this method through the Department of the Navy which has facilities for the despatch of all classified material and equipment by sea route. (iv)
- Despatch to a destination in a foreign country or despatch to any destination on an air route which traverses or touches non-British territory: 9
- Classification of material requiring "Safe Hand" transmission: (8)
- All classified material.
- (b) Methods:
- (1) By hand of a responsible officer who is in possession of a diplomatic passport;
- Department of External (11) By diplomatic bag through the Affelra;
- the meterial partments should make arrangements for transmission by this method through the Department of the Navy. is placed in the personal care of the Master. (111) Care of the Master of a British vessel;
- (D) All material lodged with the appropriate authority, for transmission by "Safe Hand", should be clearly marked "BY SAFE HAND".

PART III - SECURITY OF CLEAR TEXT OF CYPHER MESSAGES

The clear texts which have to be protected in this way will 19. GENERAL. - When a message is sent or received in certain kinds of cypher, it is of vital importance that the exact "clear texts" (plain language versions) of that measage are safeguarded until ultimately She stamped with the following warning :destroyed.

"This is an unparaphresed version of a cypher message, It is not to be distributed outside a Britlah Commonwealth Government Department or instrumentality without paraphrasing. It is never to be downgreaded below "Restricted".

Rules for the handling of messages bearing this warning are set out in paragraph 21 below.

- future and past traffic and even affecting the security of other cypher of such a message (which may have been obtained unknown to the origin-The reasons for this procedure is that possession by unauthorised persons of the encyphered version ayatem concerned. The effects could be far reaching, affecting both same message would constitute a grave danger to the security of the ator by wireless interception) together with the clear text of PARTICIPATIONS -вувтетв
- RILES FOR TREATMENT OF CLEAR TEXTS STAMPED AITH THE "PARAPHRASE WARNING
- distributed outside British Commonwealth Governclear (a) To svoid the possibility of unsuthorised possession, ment Departments or instrumentalities. texts are never to be
- below the security classification "Restricted". It is emphasised that this rule is necessary to avoid a compromise of the cypher system used downgrade e file to "unclassified", any clear texts must first be removed or and has no connection with the nature of the subject matter. necessary in reclassifying files. Should it be necessary to (b) As a further safeguerd, clear texts must never be paraphrased.
- Originators of classified messages who may retain copies of messages which they send to a signal office for despatch must ensure that every such cony is marked with the "para-(c) Originator's copies: phrase werning".
- must be pulped or burnt under the supervision of a responsible officer Since they never became unclassified, clear texts when no longer required. (d) Disposal:
- (e) Publication: Although it is essential to avoid the clear text of such a message being linked with the encyphered version, occasions will arise when it is necessary to divulge publicly the contents (or of a Government cypher message, such as by part of the contents)
- Publishing it in the press.
- (11) Quoting 1t during speeches or lectures.
- (iii) Conveying it to a person who is not a British Government official, e.g., a contractor.
- (iv) Publishing it in a non-restricted order
- Posting it on notice boards. E
- Conveying it to a foreign or allied authority. (vi)

instructions) must be removed before it is released from government condetails (cate time groups, times of receipt, serial number and delivery On such occasions the text must be "paraphrased" and the technical trol.

ruction of sentences, at the same time retaining the sense of "Paraphrasing" entails re-arranging the order and con-

- CO-OPERATION BY URIGINATORS. Originators of messeges which may be sent in cypher (i.e., all messages graded "Restricted" or above) should chosen by the cypher office. The need for paraphrasing before publicabear in mind the possibility of publication. In such cases, the draft message should be marked accordingly so that a suitable system can be tion can then, in nearly all cases, be eliminated.
- 23. RESTRICTION ON TELEPHONING OF CLEAR TEXTS. Under no circumstances messages over the telephone, including speech privacy equipment (Secraphone), nor may messages which have been sent, and which bear the paraphrase warning (paragraph 19) on the distribution copy, be confirmed by may originators dictate the text or portions of the text of classified telephone.

PART IV - MISCELLANEOUS

- discussing metters of a classified nature, and indeed official business heard by unauthorised persons. Wartime experience proved that neglect of this precaution resulted in the leskage of much important informsof any kind, in places where there is any possibility of being over-DISCUSSION OF OFFICIAL BUSINESS. - Officers must guard against
- expert with suitable equipment, and it may be possible for a trained ear arise from casual interception by cross-connection, etc., the possibilsome Government Departments, does not afford a high degree of security. 25. SECURITY OF TELEPHONE CONVERSATIONS. - Officers must bear in mind that telephone conversations are not secure. The risk of leskage may ity of telephone operators and engineers overhearing conversations in progress is possible. Deliberate interception is also possible to an privacy equipment ("Secraphone" or "Scrambler") at present in use in Cross-connection of lines over which secraphone conversations are in to "translate" anatches of "scrambled" conversation. The secraphone should, therefore, be regarded only as a device that will, in most the performance of their duty, or by deliberate interception. instances, defeat casual eavesdropping.
- (MELEPRINTER). Printing telegraphy (e.g., teleprinter) circuits cannot Ar regarded as a secure means of transmission. All messages classified confidential" or above should be encrypted for transmission by these means. TRANSMISSION OF CLASSIFIED INFORMATION BY FRINTING TELEGRAPHY

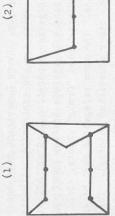
1,

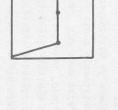
cypher, and irrespective of its method of transmission, it must be re-In this connection, if a message has previously been handled in layed in cypher in subsequent transmission(s). (See Part III, parsgraph 21.)

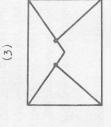
- formation must, of course, not be despatched by telegram, cable or 27. TRANSMISSION BY TELEGRAM, CABLE OR WIRELESS. - Classified inwireless in plain language
- tents of waste paper receptacles may constitute a most dangerous source factory arrangements exist for the systematic collection, custody and This will include drafts, proof copies, used car-The same safeguards must be applied to waste 28. DESTRUCTION OF OFFICE WASTE. - The careless disposal of the conof leakage of information. Every Department must ensure that satisfactory methods of destruction of classified documents are by fire, destruction, under effective aupervision, of all office waste of a bon papers, shorthand notebooks, "Ormig" sheets, etc., relating to The only satisor pulping, under supervision of a responsible officer. of this kind as to any other classified material. classified information. classified nature.

SEALING ENVELOPES

inner envelope should be sealed with wax in whichever of the three ways When Top Secret or Secret matter is prepared for despatch, the shown below is appropriate to the form of the envelope.







The sealing wax should be apresd as thinly as possible, and the die of the seal pressed firmly into the wax to ensure that the seal cannot be removed intact.

Printed & Written Records Australian War Memorial

354. Australia. Prime 94007145Minister's Dept Instructions for A9531 the security of official documents and information



AUSTRALIAN WAR MEMORIAL PRINTED RECODE



COMMONWEALTH OF AUSTRALIA

SECURITY

OF

CLASSIFIED MATTER

IN

GOVERNMENT DEPARTMENTS

AND

INSTRUMENTALITIES

Issued by the ATTORNEY-GENERAL'S DEPARTMENT

MAY, 1954

RESTRICTED



COMMONWEALTH OF AUSTRALIA

SECURITY

OF

CLASSIFIED MATTER

IN

GOVERNMENT DEPARTMENTS

AND

INSTRUMENTALITIES

Issued by the ATTORNEY-GENERAL'S DEPARTMENT

MAY, 1954

RESTRICTED

FOREWORD

I commend this booklet to the attention of all members of the Commonwealth Government Service of Australia.

It is the duty of each one of you to safeguard the official information which is entrusted to you. It may be information affecting national or even international security or it may be a routine matter of administration, but whether or not it is improperly used depends upon your integrity and your care,

The rules laid down in this booklet are designed to help you fulfil this duty, and it is essential that they should be faithfully observed.

R. G. MENZIES
PRIME MINISTER

CONTENTS

Chapter								Page
1	INTROI	DUCTION	3.8	* *	* *			9
	Para. 1	General		***			0.0	,,
	8	Definitions	600	66.00	11	u u	* *	1()
	9	Departmental	Secur	rity Of	ficers	N N	* *	,,
	10	Enquiries on	Securi	ity		1000 W		11
11	CLASSI	FICATION OF	OFFI	CLAL :	MATT	ER	5.024	1.3
	Para. 1	Security Class	sificati	ons	200		STATES	,,
	2	Unclassified M	atter		2 2		• •	17
	3	Principles to	be .\	applied	in (lassify	ing	
		Matter		(* ix	* *	8.8	• •	**
	6	Responsibility classification	for (lassific	ration	and I	ζ(,-	19
	7	Overclassificat	1011	14.54		9 N		٠,
	9	Classification			N#83#1			20
	12	Numbering	8.8		(454)			,,
111	DISSEM	INATION OF	CLAS	SIFIEI) MA'	TTER	19.00	21
	Para. 1	General — The	e "Nee	ed to K	now"	Princi	ple	
	3	TOP SECRET						,,
	4	Distribution of			1876			,,
	7	Reproduction of	of Clas	sified I	Latter		E 16	22
	11	Discussion of					¥ ¥	500
	12	Telephone Con					* *	
1V	CUSTOL	Y OF CLASSI	FIED	MATT	ER			23
	Para. 1	Storage of Cla	assified	Matte	.1.			**
	7	Access to Sto					10000	25
		Combinations						,,
	9	Keys			8 8			26
	200			ac 5			50000	0.290.00

May, 1954

Chapter			Page
	10	Protection of Classified Matter in Actual	
		Use	26
	11	Office and Area Inspection	**
	12	Receipts for Custody	
	13	Accounting for Classified Matter Held	
	14	Removal of Classified Matter from a Department	.,
	17	Destruction of Classified Documents and	
		Equipment	27
	20	Destruction of Office Waste	,,
V	TRANSI	MISSION OF CLASSIFIED MATTER	29
	Para. 1	Envelopes	
	5	Carriage Within a Department	30
	6	Carriage Outside a Department or Area	1212
	8	"Safe Hand" Transmission	31
	9	Carriage by Officers Travelling Overseas .	32
	10	Receipts for Transmission	,,
	12	Transmission by Telephone	,,
	15	Printing Telegraphy (Teleprinter)	33
	16	Telegram, Cable or Wireless	"
	17	Transmission of Classified Equipment	"
VI	CODEW	ORDS AND NICKNAMES	35
		Codewords	W.
		Department of Supply	**
	6	Nicknames	
VII	СУРНЕ	R SECURITY	37
	Para. 1	Cypher Categories	303
	2	Telegrams Requiring Safeguarding of the	
	ges)	Verbatim Text	133
	3	Publication of Texts of Cypher Telegrams	••

Chapter			Page
	4	Reason for Special Precautions	38
	5	Co-operation by Originators	,,
	7	Cypher Security Committee	39
VIII	SECURI	TY OF BUILDINGS AND AREAS CON-	
	TAININ	G CLASSIFIED MATTER	41
	Para. 1	Responsibility for Building and Area Security	,,
	2	Access to Buildings and Areas	,,
	4	Passes	"
	9	Visitors	42
	10	Visits by Press, Radio and Other Accredited Representatives	43
	11	Control of Photography	
	12	Custody of Keys	22
	14	Instructions to Guards, Sentries, etc	,. 44
	1,	instructions to eather the foreign etc.	
IX	ACTION	IN CASES OF BREACH OF SECURITY	47
	Para. 1	General	"
	4	Responsibility for Action	,,
	6	Losses and Leakages	48
	7	Losses	,,
	9	Leakages	,,
	13	Minimising Damage	49
	14	Preventing Recurrence	,,
	15	Possibility of Prosecution	,,
X	STAFF	ENGAGED ON CLASSIFIED WORK	51
	Para. 1	Responsibility of Departments	,,
	2	Security Clearance	22
	5	Supervision of Staff	,,
	6	Application of Acts and Regulations Dealing with Official Secrecy	52
	7	Persons Outside the Government Service	,.

Chapter		¥	Page
XI	CLASS1	FIED MATTER ENTRUSTED TO PER-	
	SONS O	UTSIDE THE GOVERNMENT SERVICE	53
	Para. 1	Approval by Permanent Head	20
	2	Security Clearance	
	3	Application of Acts dealing with Official Secrecy	54
	4	General Security Arrangements	,.
	5	Government Contracts	••
XII	ACTS :	AND REGULATIONS DEALING WITH	
2111		AL CECDECY	55
		Introduction	.,
		The Commonwealth Public Service Act and	٠,
	-	Regulations	**
	+	The Crimes Act. L'art VI — Offences by and against Public Officers	56
	6	The Crimes Act. Part VII - Breach of	
		Official Security	••
	9	Other Provisions of the Crimes Act	59
	11	The Defence Act 1903-1949	60
	13	The Supply and Development Act 1939-1948	61
	14	The Defence (Special Undertakings) Act 1952	62
	16	Various Other Commonwealth Acts	.,,
15	17	The Application of the Provisions to Public Servants and Others Employed by the Government and to Persons not in the	
		Employ of the Government	63
1ppendi	l.		
:\		G ENVELOPES	65
В		TED EQUIPMENT IN TRANSIT	67
		55/407	

Page 8

CHAPTER 1

INTRODUCTION

General

- 1. This booklet outlines the principles to be followed I Commonwealth Departments and Statutory Authorities in saf guarding official matter. It supersedes the Instructions for the Security of Official Documents and Information issued by the Prime Minister's Department on the 19th October, 1948, and we be revised as necessary.
- 2. The unauthorised disclosure of official information mathematical have serious consequences, ranging from administrative embarrasment to the Government to jeopardising the security not only Australia, but of other countries in the British Commonwealth, an our Allies with whom information is shared.
- 3. The security of official information is the personal conce of everyone in the Government Service, and all public servan should be aware of their responsibility in this regard.
- 4. In the first place, it must be emphasized that it is primary duty of every public servant to be discreet in the use any information obtained in an official capacity. The provisio of the Commonwealth Public Service Act and Regulations and the Crimes, Defence and other Acts, in this regard, are set out Chapter XII.
- 5. Certain official matter requires to be specially protecte Such matter is allocated a security classification and is known "classified matter".
- 6. The security of classified matter depends primarily on t integrity, discretion, and vigilance of officers who deal with it, a secondly, on an effective system within each Department, Bran and Section which is enforced constantly so that observar becomes a habit. Such a system should ensure that access classified matter is limited to those who require it in the course their duties, and that adequate measures are taken at all times this physical security. Effective office security measures may off result in some additional work and administrative inconvenien but this must be accepted in the interests of national security.

To ensure that classified matter is treated with equal care all concerned, it is essential that a common standard of classifion and safeguarding should be observed by all Departments, amount of classified matter handled will vary greatly between partments, according to their functions, and their security uirements may differ. However, the principles set out in this klet should be adhered to by all, and security instructions ned by Departments to suit their individual needs should be in ordance with these principles.

initions

For the purposes of this booklet the following definitions ly:—

- (a) The term "Department" is used to cover any Australian Commonwealth Government Department, Service or Statutory Authority.
- (b) The term "officer" includes any person permanently or temporarily employed in a Department as defined in (a).
- (c) The term "matter" includes everything, regardless of its physical character, on or in which information is recorded or embodied. Books, reports, articles, notes, letters, drawings, sketches, plans, photographs, recordings, machinery, models, apparatus, devices, and all other products or substances fall within the general term "matter". Information which is transmitted orally is considered as "matter" for purposes of security.
- (d) The term "document" covers any form of recorded information, including printed, written, drawn or painted matter, sound recordings, photographs, films, etc. "Documents" are included in "matter".
- (e) "Equipment" includes machinery, apparatus, devices, supplies, ammunition, etc. "Equipment" is included in "matter".

partmental Security Officers

The responsibility for security within each Department is with the Permanent Head. For administration purposes a for officer should be appointed Departmental Security Officer a full or part time basis, according to the varying requirements

of Departments. This officer will be concerned with the issuing of instructions on all aspects of security, with their observance, and with action in case of breaches of security.

Enquiries on Security

10. Any enquiries on security matters should be addressed by Departments to the Director-General, Attorney-General's Department, "D" Branch, Box 5105 BB, G.P.O., Melbourne.

May, 1954

CHAPTER II

CLASSIFICATION OF OFFICIAL MATTER

Security Classifications

1. Matter requiring special protection is, according to the degree of protection required, allocated to one of four security classifications or gradings, each with its own rules. This system is used in common by British and United States authorities. The four security classifications or gradings are:—

TOP SECRET
SECRET
CONFIDENTIAL
RESTRICTED

These classifications are defined hereunder and some illustrations are given of their application to both civil and defence matters. The illustrations are not intended to be exhaustive but to provide a general guide for the preparation of departmental instructions. Each Department should carefully consider the four definitions and formulate examples suited to its individual needs.

A. TOP SECRET

Information and material (matter), the unauthorised disclosure of which would cause exceptionally grave damage to the nation, politically, economically, or from a security aspect. This category is reserved for the nation's closest secrets and is to be used with great reserve. Very little matter belongs in the TOP SECRET category.

Illustrations

- (a) Very important political documents dealing with such matters as negotiations for major alliances, etc.
- (b) Major governmental projects such as drastic proposals to adjust the nation's economy (before official publication).
- (c) Matter relating to new and far reaching experimental, technical and scientific developments in methods of warfare or defence, e.g., vital matter relating to

atomic warfare, defence against biological warfare, or matter affecting future operational strategy. A TOP SECRET grading is justified if:

- (i) a project is likely to influence military strategy materially;
- (ii) it gives us a prolonged military advantage over other nations;
- (iii) it is liable to compromise some other project similarly graded.
- (d) Critical information relating to vital strategic areas and the supply of vital strategic materials.
- (e) Information which would indicate the capabilities or major successes of our intelligence services or which would imperil secret sources.
- (f) Critical information about cryptography so far as it relates to devices and equipment under development.
- (g) Certain compilations of data or items which individually may be classified SECRET or lower, but which collectively should be put in a higher grade.

B. SECRET

Information and material (matter), the unauthorised disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation or of any governmental activity thereof, or would be of great advantage to a foreign nation.

This classification should be used only for highly important matter and is the highest classification ordinarily used.

Illustrations

- (a) High level directives dealing with important negotiations (as distinct from major negotiations which would be in the TOP SECRET category) with other countries.
- (b) Proposals for new schemes of governmental or other controls, foreknowledge of which would seriously prejudice their operation.
- (c) Matter relating to certain new methods of warfare or defence, including scientific and technical developments, not classified as TOP SECRET, e.g., new

designs of Service aircraft, guided projectiles, tanks, radar and anti-submarine devices. A SECRET grading is justified if:

(i) a project materially influences a major aspect of

military tactics;

(ii) a novel principle applicable to existing important

projects is involved;

- (iii) the project is sufficiently revolutionary to result in a major advance in existing techniques or in the performance of existing secret weapons;
- (iv) it is liable to compromise some other projects already so graded.
- (d) War plans or details of schemes for the defence of areas other than vital strategic areas, including plans or particulars of operations connected with them.
- (e) Vital military information, including photographs, maps, etc., relating to important defences, establishments, and installations.
- (f) Intelligence which is not in the TOP SECRET category but which would reveal a secret source, or the value of which depends upon concealing the fact that we possess it.
- (g) Cryptographic devices and equipment unless specifically assigned to a lower classification.
- (h) Certain compilations of data or items which individually may be classified CONFIDENTIAL or lower, but which collectively should be put in a higher grade.

C. CONFIDENTIAL

Information and material (matter), the unauthorised disclosure of which, while not endangering the national security, would be prejudicial to the interests or prestige of the nation, would cause administrative embarrassment, or unwarranted injury to an individual, or would be of advantage to a foreign power.

Most matter will, on proper analysis, be classified no higher than CONFIDENTIAL.

Illustrations

(a) Plans of Government projects such as land development, hydro-electric schemes, road development, or development of areas.

- (b) Routine Service reports, e.g., on operations and exercises, which contain information of value but not of vital interest to a foreign power.
- (c) Routine Intelligence reports.
- (d) Technical matter not of major importance but which has a distinct military value or requires protection otherwise, e.g., new weapons calculated to influence minor tactics or Service tests of war equipment of a standard pattern. A CONFIDENTIAL grading is justified if:
 - (i) the project is more than a routine modification or logical improvement of existing materials and is sufficiently advanced to result in substantial improvement in the performance of existing CONFIDENTIAL weapons;
 - (ii) the project is sufficiently important potentially to make it desirable to postpone knowledge of its value reaching a foreign nation;
 - (iii) it is liable to compromise some other project already so graded.
- (e) Certain personnel records and staff matters.
- (f) Certain compilations of data or items which individually may be classified RESTRICTED, or which may be unclassified, but the aggregation of which enhances their security value.

D. RESTRICTED

Information and material (matter), which requires special protection other than that determined to be TOP SECRET, SECRET or CONFIDENTIAL.

Illustrations

- (a) Departmental books of instruction and training and technical documents intended for official use only or not intended for release to the public.
- (b) Routine information relating to the supply and procurement of military stores.
- (c) Minor modifications and routine tests of equipment.
- (d) Certain compilations of data or items which individually may be unclassified but which in the aggregate warrant a classification.

Note.—Documents, while not containing more actual information than has been published in the Press or otherwise issued by unofficial agencies, may confirm the accuracy or otherwise of such published material and/or give official views thereon. Where it is necessary to protect official confirmation or comment from unauthorised disclosure, such documents should be appropriately classified.

Unclassified Matter

2. Matter may be marked "Unclassified" if it is necessary to indicate that no security classification is required. However, all official information must be protected. The fact that information is not classified or is marked "Unclassified" does not eliminate the necessity for preventing its unauthorised disclosure. (The provisions of the Public Service Act and Regulations and of the Crimes Act and other Statutes mentioned in Chapter XII apply equally to all official information, whether classified or unclassified.)

Principles to be Applied in Classifying Matter

- 3. Classification of Documents. The following are the more important principles to be followed in classifying documents:—
 - (a) A document is to be classified as soon as possible during its preparation.
 - (b) Each document is graded on its merits, that is to say it is graded according to the nature, source, and implications of the information contained therein. Factors such as the grading of other documents in the same series, or the grading of a classified file of which a document happens to be part, should not influence the grading of a document.
 - (c) If it is practicable to indicate pages or passages within a document which merit varying classifications, this should be done. In such cases the overall classification of the document must be clearly shown at the beginning and must, of course, not be lower than the highest classified portion.
 - (d) A document must not bear a lower classification than the highest classification of any of its appendices or attachments. Each attachment, etc., must be graded on its own individual merits.

- (e) There is no need to allot to a subsequent document a classification as high as that of an earlier one which it quotes or refers to, provided the quotation is limited to the reference number, the date, and matter not in itself justifying a classification higher than that of the subsequent document.
- (f) A file containing classified documents is graded according to the highest classification of any documents contained therein. For this reason, it may sometimes be found desirable to break a file into two or more parts, one part to contain the higher category papers.

 Note.—Distinctive file covers should be provided for TOP SECRET (bright red), SECRET (salmon pink), and CONFIDENTIAL (green).

4. Re-classification of Documents

- (a) Classified documents should be kept under constant revision and "downgraded" to a lower category as the need for protection diminishes, or made unclassified when classification is no longer necessary.
- (b) Documents must be re-classified only on the instructions or with the permission of the originating authority, who should inform all recipients or holders of the particular documents of the new classification. In some cases it may be possible for the originating authority to indicate at the time of issue that a document may be downgraded after a given date.
- (c) When a document is re-classified the old security classification should be deleted in ink and the new one substituted. The deletion should be signed and dated by the officer responsible and a note made of any documentary authority for it.
- (d) Cypher telegrams bearing the paraphrase warning (see Chapter VII, paragraph 2) should never be downgraded below RESTRICTED.
- 5. Equipment. The same general principles as apply to documents are to be followed in classifying equipment.
 - (a) Equipment is to be graded in the same category as would be a document describing the equipment. However, the components of such equipment are to be classified on their merits.

- (b) The initial secrecy grading of equipment procured through the Departments of Supply and Defence Production is reviewed by a Technical Security Grading Committee. Unless it conflicts with other equipment gradings, the Committee normally adopts the classification placed upon the equipment by the sponsoring Department.
- (c) Departments are responsible for grading equipment not under contract for manufacture or supply with or through the Departments of Supply and Defence Production.
- (d) Equipment of any apparent importance in the very early stages of design and development, i.e., before its ultimate military value is clearly determined, is to be treated as at least SECRET.
- (e) Classified equipment must be kept constantly under review by Departments and downgraded as soon as circumstances permit. In certain circumstances, it may be necessary to upgrade equipment. Where applicable, Departments are to notify the Technical Security Grading Committee immediately of any changes in security classification.

Responsibility for Classification and Re-classification

6. In each Department, specified officers should be authorised to approve the classification of matter originating in the Department. Only a senior officer should be authorised to approve TOP SECRET and SECRET classifications. Officers should also be designated to approve the re-classification of matter originating in the Department.

Over-classification

7. Matter is to be assigned the lowest possible classification consistent with its being properly safeguarded. Over-classification must be avoided, since it depreciates the importance of classified matter in the minds of personnel, encourages neglect for the rules of protection, and thus endangers the whole system of security. In allotting a classification, the officer responsible should always consider whether compromise of the matter would in fact cause the damage envisaged in the relevant definition.

8. The use of codewords and nicknames (see Chapter VI) may enable documents to be given a lower classification than would otherwise be the case, or may eliminate the need for classification.

Classification Marking

- 2. Classified books, pamphlets, letters, memoranda, etc., and all copies thereof are to be plainly and conspicuously marked (preferably by rubber stamp) with the appropriate classification at the top and bottom of each page, including the front cover and the title page of books and pamphlets. The marking is to be placed so that it is clearly visible when pages are fastened together.
- 10. Other classified documents such as drawings, maps, photographs, films, etc., are to be marked in accordance with the above principles. Drawings, negatives, etc., should be marked in such a way that the classification is reproduced on any copies made therefrom. Negatives in roll form and films should be marked at the beginning and end and containers should also be marked.
- 11. Classified equipment is normally to be marked by stamping, etching, attaching a classification plate, or other appropriate means. In certain special cases where equipment cannot be kept from general observation, it may not be in the best interests of security to mark it.

Numbering

12. Any classified matter issued in a series should bear a serial number so that non-receipt of a particular item is noticed. TOP SECRET matter is to bear a copy number to facilitate recording of distribution and enquiry in case of a breach of security. In particular cases of importance, this procedure should be extended to SECRET matter.

CHAPTER III

DISSEMINATION OF CLASSIFIED MATTER

General — The "Need to Know" Principle

- I. Failure to impart information on a sufficiently wide basis may lead to lack of co-ordination and co-operation. On the other hand, too wide a circulation will tend to prejudice the security of the information. A balanced assessment of these conflicting claims is often a matter of some difficulty. The guiding principle is that information should be passed only to those officers to whom it is necessary for the fulfilment of their duties (that is those who "need to know"). Officers are not entitled to have access to classified matter solely by virtue of their status or office. Where it is not necessary for the entire contents of a classified document to be made available to an officer, he should be acquainted only with those facts relevant to his duties.
- In addition to those officers who require to study classified matter in the course of their duties, certain other members of the staff such as registry clerks and typists will necessarily handle this matter in the normal course of administration. Special arrangements are necessary to ensure that this work is entrusted to authorised persons under conditions which do not permit others to view or have access to the matter.

TOP SECRET and SECRET Registries

3. TOP SECRET and SECRET matter must be maintained in separate registries in segregated areas. TOP SECRET and SECRET registries are to be staffed by selected persons authorised to handle such matter, and are not to be accessible to others.

Distribution of Classified Matter

- 4. Each Department should authorise officers to be responsible for determining the distribution of classified matter.
- 5. TOP SECRET Distribution. TOP SECRET matter is to be made available only to persons specifically authorised to receive it and each TOP SECRET document or item is to be treated individually. A record is to be maintained of all persons within a Department having access to a TOP SECRET document or item.

all those outside a Department to whom a TOP SECRET document or item is transmitted, and all those to whom TOP SECRET information is disclosed.

6. Classified matter is to be made available to persons or bodies outside the Government Service only with the approval of the Permanent Head of the originating Department. The measures to be taken to safeguard such matter are outlined in Chapter XI below.

Reproduction of Classified Matter

- 7. Copies of classified matter are to be kept to a minimum, as the risk that the matter may fall into unauthorised hands increases in proportion to the number of copies in existence.
- 8. TOP SECRET matter is not to be reproduced in whole or in part except with the approval of the originating authority. This permission will not extend beyond a specified number of copies which are to be accorded the same treatment as the original.
- 9. The typing, roneoing, etc., of TOP SECRET and SECRET matter should be carried out under the supervision of an authorised officer in a segregated area. All materials and waste incidental to the reproduction of classified matter should be accounted for and safeguarded or destroyed in the manner prescribed in this booklet (see Chapter IV, paragraphs 5 and 20).
- 10. When TOP SECRET, SECRET and CONFIDENTIAL matter is reproduced by printing, the necessary safeguards must be provided at each stage.

Discussion of Official Business

11. Officers must guard against discussing matters of a classified nature, and indeed official business of any kind, in places where there is any possibility of being overheard by unauthorised persons.

Telephone Conversations

12. The insecurity of telephone conversations, and restrictions on the use of the telephone for transmitting classified information, are dealt with in Chapter V.

CHAPTER IV

CUSTODY OF CLASSIFIED MATTER

Storage of Classified Matter

- 1. Documents
 - (a) TOP SECRET and SECRET documents are to be stored, when not in actual use or under guard, in vaults, safes or other equivalent containers fitted with dial type combination locks. Key type safes should not be used.
 - (b) CONFIDENTIAL documents are to be stored, when not in actual use or under guard, in secure vaults, safes, safe-file cabinets or their equivalent, having secure locks (preferably dial type).
 - (c) RESTRICTED documents are to be stored in a locked room or container equipped with a reasonably secure locking device, or are to be given equivalent protection.
- 2. Containers. The quality of containers required to afford the necessary protection will depend on a number of other security factors and it is therefore not possible to define specifications to cover every case. When determining the suitability of containers Departments should bear in mind the following factors, examples of the application of which are mentioned below:—
 - (a) Location

If the container is located in AUSTRALIA a lower standard can be accepted than would be the case if the container were to be located in a foreign country, e.g., in an Australian Embassy abroad.

Containers located in isolated, easily entered buildings must be of higher quality than those located in, say, the upper stories of buildings, the entry to which is restricted.

Safes for use in foreign countries should not be locally purchased as such purchases may be subject to pre-delivery tampering. All these safes should be fitted with a 4-wheel indirect drive combination lock.

- (b) System of Guarding
 - Guarding can range from cases in which no guard is provided and the container is left unattended for periods of 48 hours or more (e.g., over the weekend) to conditions under which the container is subject to regular inspection by armed guards. (Important safes or strongrooms can have time clocks installed near them so that a check can be kept on guards inspections.)
- (c) Burglar Alarm Systems

Where these are installed in conjunction with armed guards lower standards of containers can be accepted. However, for the storage of TOP SECRET matter the principle should be accepted that the highest standard of container is necessary, since circumstances may arise in which the other protective systems become inoperative for a period.

- Particularly abroad or where a container is located in an isolated building, steps should be taken to ensure that the container cannot be easily removed from the building. This may sometimes be done by using a larger and heavier container than would normally be required, or by bricking and cementing a small container into position.
- 3. When in doubt as to the suitability of a container, Departments may refer to the Director-General of the Australian Security Intelligence Organisation for technical advice.
- 4. Equipment
 - (a) TOP SECRET and SECRET equipment is to be so stored and protected that unauthorised persons are denied access to or view of it at all times. Access to areas and buildings containing such equipment is to be controlled.

- (b) CONFIDENTIAL and RESTRICTED equipment is to be so stored and protected that access to it is denied to unauthorised persons.
- (c) Separate instructions for the storage of cryptographic equipment are issued to the Departments concerned.
- (d) The custody of classified equipment is to accord with the principles outlined above, but precautions will vary according to the nature of the equipment, the storage facilities available, and the position of the equipment during operational use. In establishments where classified equipment is stored or is in operational use a security officer should be designated to ensure that all necessary measures for safeguarding the equipment are taken.
- 5. Shorthand Notebooks, etc. Shorthand notebooks, carbon and blotting paper, stencils, newly used typewriter ribbons, waste sheets passed through duplicating machines, and all materials being used for preparing or reproducing classified matter, must be treated as classified matter themselves, until they are to be destroyed as classified waste (see paragraph 20 below).
- 6. Containers used to transmit Classified Matter. The security of containers used to transmit classified matter is to be regarded as compromised when a key is lost and also when an unauthorised person has had any opportunity of examining the lock, since an expert is able to produce a suitable key after such an examination. When not in actual use or under guard, containers should be stored in the same way as the matter they are used to transmit.

Access to Storage Containers

7. Only a minimum number of authorised persons should possess the combination or keys to storage space or have access to the material stored therein. Containers are to be kept locked when not under the direct supervision of a person officially entrusted with the combination, keys or the contents.

Combinations of Safes

8. Combinations of safes are to be classified as high as the highest security classification of the matter protected, and safeguarded accordingly. Combinations are to be changed at least

every three months and at other times as considered necessary (as when a person knowing the combination severs his connection with the office concerned).

Keys

9. The custody of keys is dealt with in Chapter VIII.

Protection of Classified Matter in Actual Use

10. Those using classified matter must take every precaution to prevent deliberate or casual inspection of it by unauthorised persons. Papers should never be left lying open when unauthorised persons are present. If a room containing classified matter has to be left unoccupied for a few minutes during working hours the door must be locked; at all other times classified matter must be stored as prescribed above.

Office and Area Inspection

11. Office or area inspection should be made daily after working hours to ensure that no classified matter is left unprotected, and that all safes, filing cabinets, windows, doors, gates, etc., are locked.

Receipts for Custody

12. The custody of TOP SECRET matter within Departments is to be covered by a receipt system. Departments are responsible for ensuring that a receipt system applies in special cases where receipts are required for the custody of classified matter other than TOP SECRET.

Accounting for Classified Matter Held

13. A record of TOP SECRET matter held must be maintained and a check should be carried out periodically in order to bring to light any deficiencies. A record must also be maintained of classified matter which, on the instructions of the originator, must be accounted for periodically to the originator.

Removal of Classified Matter from a Department

14. Classified matter should not normally be taken out of a Department unless it is required for official reference elsewhere, e.g., at a conference. TOP SECRET matter must never under any circumstances be taken home.

- 15. Before taking TOP SECKET, SECRET and CONFIDEN TIAL matter out of a Department, the approval of a responsible senior officer is to be obtained. A record of the removal and return of all classified matter taken away overnight is also to be kept by the appropriate registry.
- 16. The officers removing and approving the removal of classified matter from a Department, are responsible for ensuring that it is adequately protected at all stages. When not actually it use it should be kept in a locked container and guarded by the officer concerned, unless it can be kept in an approved safe.

Destruction of Classified Documents and Equipment

- 17. The only satisfactory methods of destruction of classific documents are by fire or pulping. When destruction is authorise documents are to be burnt or pulped under supervision of a authorised officer. This officer must ensure that no unburnt chalf-burnt fragments can be carried away by the draught of the fire and must see that the ashes are reduced to powder. Documents for pulping are to be torn in small pieces and the supervisit officer must watch the process of pulping until an advanced stag has been reached.
- 18. When it is necessary to dispose of classified equipment destruction is to be in such a manner as to make reconstructionand/or identification impossible, and is to be carried out und supervision of an authorised officer. The method of destruction will vary according to the nature of the equipment concerne Necessary destruction may be limited to those portions of the equipment which incorporate the classified features.
- 19. A record is to be retained and appropriately certified the destruction of classified documents and equipment.

Destruction of Office Waste

20. The careless disposal of waste matter constitutes one the most dangerous sources of leakage of information. Eve Department must ensure that satisfactory arrangements exist the systematic collection, custody, and destruction in accordawith the methods outlined above, of all office waste of a classificature.

CHAPTER V

TRANSMISSION OF CLASSIFIED MATTER

Envelopes

- 1. TOP SECRET, SECRET and CONFIDENTIAL matter is to be enclosed in two opaque envelopes. The inner envelope is to show the classification and full address and is to be wax sealed so as to prevent or reveal tampering (the correct method of sealing is shown in Appendix A). The outer envelope is to be fully addressed but must not show the security classification. The address of the sender should be shown on the outer envelope. RESTRICTED matter may be enclosed in one envelope provided this does not disclose the classification. Where matter is for delivery by "Safe Hand" (see paragraph 8 below) the outer envelope should be inscribed accordingly in bold letters, and bear a number for identification purposes.
- 2. Documents should be covered or folded so that the text does not come in direct contact with the inner cover. The size of the envelope should be approximate to the size of the contents so that the envelope and its fastenings do not suffer strain and to minimize the risk of any of its contents being extracted.
- 3. The outer envelope of TOP SECRET matter should be addressed to a Department in the normal manner. Opening instructions should be shown on the inner envelope which should, if necessary, be addressed to the individual for whom it is intended. TOP SECRET and SECRET matter is to be opened only by the addressee or a representative who is authorised to open such matter.
- 4. Where the originating Department cannot effect delivery to the office of the addressee, and use is made of another Department or Statutory Authority as the transmitting agent, an inner envelope and an outer envelope should be used for all classified matter, the inner envelope showing:—
 - (a) the full address of the addressee, together with name or appointment;
 - (b) the originating Department;

- (c) a reference number for identification purposes;
- (d) the appropriate security grading.

The outer envelope should bear no indication of the security classification and should be addressed to the appropriate authority at the transmitting Department, who will remove the outer envelope and forward the inner envelope in accordance with the practice of his Department to the addressee.

Carriage within a Department

5. For internal circulation within a Department located in one area, TOP SECRET matter should be passed by hand of responsible officers. If this is not practicable, TOP SECRET matter may be delivered by authorised messenger personally to the recipient or his authorised representative, in a locked container or enclosed in two envelopes as prescribed in paragraphs 1 to 3 above. SECRET matter may be enclosed in a single envelope marked "SECRET" provided this is sent direct by hand. CONFIDENTIAL matter may be sent in a single envelope marked "CONFIDENTIAL". RESTRICTED matter may be sent with or without a cover, as considered advisable.

Carriage Outside a Department or Area

- 6. Despatch and Carriage Within Australia
 - (a) TOP SECRET matter, also classified code and cypher books and appliances, must never be despatched by civil post, but by "Safe Hand" (see paragraph 8 below).
 - (b) SECRET matter should be despatched by "Safe Hand". If this service is not available the only alternative means of despatch to be used is registered mail.
 - (c) Postal registration of CONFIDENTIAL matter is discretionary for the originating Department. (However, CONFIDENTIAL equipment is to be sent by registered mail.) RESTRICTED matter may be sent by ordinary mail.

 (CONFIDENTIAL and RESTRICTED matter may be

CONFIDENTIAL and RESTRICTED matter may be carried by authorised messenger between buildings in the same town. Envelopes should not be carried loose but should be enclosed in securely fastened containers. If a van is used it must be locked whenever it is left unattended.

7. Carriage Outside instralia. All classified matter should be forwarded by "Safe Hand", with the following exception. CONFIDENTIAL matter may be sent by registered mail and RESTRICTED matter by ordinary mail to a destination within British territory, provided that, if carried by air, the route does not traverse or touch non-British territory.

"Safe Hand" Transmission

- 8. Transmission of matter by "Safe Hand" means that it is despatched to the addressee in the personal care of an authorised officer or succession of authorised officers who are personally responsible for its carriage and safekeeping. At each handover, a receipt must be obtained showing identification number of the package, time, date, etc. The following methods are used:—
 - (A) Carriage Entirely Within Australia:
 - (i) By hand of a responsible officer or succession of officers appointed to deliver the matter to the addressee.
 - (ii) Care of the Captain of an aircraft of an Australian Airline Company which has been authorised to carry "Safe Hand" matter.
 - (B) Carriage Outside Australia:
 - (a) Between points within British Territory (including Australia) and, if carried by air, on a route which does not traverse or touch non-British territory.
 - (i) By hand of a responsible officer or succession of officers appointed to deliver the matter to the addressee.
 - (ii) By diplomatic bag through the Department of External Affairs.
 - (iii) Care of the Captain of an Aircraft of a British Airline Company which has been authorised to carry "Safe Hand" matter. Departments should refer, in the first instance, to the Department of External Affairs in connection with arrangements for the use of this method.
 - (iv) Care of the Master of a British vessel; the matter is placed in the personal care of the Master. Departments should make arrangements for transmission by this method through the Department of the Navy which has facilities for the despatch of all classified matter by sea route.

- (b) To or from a point in a Foreign Country, or by an air route which traverses or touches non-British territory.
 - (i) By hand of a responsible officer who is in possession of a diplomatic passport.
 - (ii) By diplomatic bag through the Department of External Affairs.
 - (iii) Care of the Master of a British vessel; the matter is placed in the personal care of the Master. Departments should make arrangements for transmission by this method through the Department of the Navy.

Carriage by Officers Travelling Overseas

9. Classified matter required by an officer travelling overseas should be sent ahead by the means prescribed in paragraphs 8 (B) (a) and (b) above.

Receipts for Transmission

- 10. The transmission of TOP SECRET and SECRET matter is to be covered by a receipt system. The addressee or his authorised representative is to sign and check the accuracy of the receipt and the sender is to check its return.
- 11. Departments may decide whether in any instances receipts are to be obtained for other classified matter.

Transmission by Telephone

12. No form of telephone conversation — even on a direct line or between two extensions from the same switchboard—is secure. The risk of leakage may arise from casual interception by cross-connection, etc., the possibility of telephone operators and engineers overhearing conversations in the performance of their duty, or by deliberate interception. The privacy equipment (previously known as the "secraphone" or "scrambler") at present in use in some Government Departments, does not afford a high degree of security and is not a "secret" telephone system. Cross-connection of lines over which privacy telephone conversations are in progress is possible. Deliberate interception is also possible to an expert with suitable equipment, and it may be possible for a trained ear to "translate" snatches of "scrambled" conversation. Privacy equipment should therefore be regarded only as a device that will, in most instances, defeat casual eavesdropping.

- 13. TOP SECRET information must never be transmitted by open or privacy telephone. SECRET information must never be conveyed over the open telephone, and should be transmitted by privacy telephone only when the need for speed outweighs the need to guard against leakage. There is less objection to the transmission by telephone of CONFIDENTIAL and RESTRICTEL information, but, even so, every effort should be made to render the conversation as obscure as possible to eavesdroppers. As a general rule CONFIDENTIAL information should not be transmitted over open telephone lines.
- Note.—The foregoing is for guidance. Users of speech privacy equipment must in all cases observe current detailed instructions issued with or in connection with such equipment.
- 14. Care must be taken when referring to a cypher telegram not to give any indication which might lead to a compromise of the cypher used (see Chapter VII).

Printing Telegraphy (Teleprinter)

15. Printing telegraphy (e.g., teleprinter) circuits cannot be regarded as a secure means of transmission. All messages classified CONFIDENTIAL or above should be encrypted for transmission by these means. In this connection, a message bearing a paraphrase warning should be paraphrased before re-transmission even in cypher. If paraphrase is not possible the re-transmission must be in one time or Category A System and the cypher staff must be warned that the text is an unparaphrased version of a Category B message (see Chapter VII).

Telegram, Cable or Wireless

16. Classified information must not be despatched by telegram cable or wireless in plain language.

Transmission of Classified Equipment

17. The measures to be taken to safeguard classified equipment in transit are set out in Appendix B.

CHAPTER VI

CODEWORDS AND NICKNAMES

Codewords

- 1. A codeword is used to provide security cover in referring to some particular classified matter or project. Examples of the use of a codeword include:—
 - (a) providing a name for plans, projects and operations;
 - (b) concealing intentions in documents, communications and discussions pertaining to plans, projects and operations;
 - (c) designating geographical locations in conjunction with (a) and (b) above.
- 2. When taken into use, codewords are assigned meanings which are registered and accorded appropriate security classification. They are invariably to consist of one word only.
- 3. All codewords are to be taken from the Australian block Inter-Services Codeword Index maintained by the Joint Intelligence Committee, Department of Defence, Melbourne, and requests for codewords are to be made through Departments to the Joint Secretary of that Committee. Such requests should distinguish between words required for designating geographical locations (as above) and those required for other security purposes, since the former are drawn from a special index.
- 4. Advice on the allocation and use of codewords is given in directives issued by the Joint Intelligence Committee. The use of words as codewords, other than those obtained from the Committee, is not authorised.

Department of Supply

5. A special procedure applies to the Department of Supply which, in addition to codewords, uses two word codenames, the second word of which is a colour.

Nicknames

6. A nickname is a name used for administrative convenience in referring to some particular matter in which security cover is

not required. It may be used as and when convenient for unclassified and RESTRICTED matter only. Nicknames are not registered.

7. To avoid any confusion with a codeword or with Department of Supply codenames, nicknames must always consist of two separate words neither of which is to be a colour. Care should be taken that the two words are kept distinct and that they do not consist of pairs of words normally associated with each other (e.g., CROSS ROADS).

CHAPTER VII

CYPHER SECURITY

Cypher Categories

- 1. The cyphers used by the British Commonwealth fall into two categories:
 - Category A. Those for which it is unnecessary to paraphrase the verbatim text before publication or distribution to persons outside the Government Services of British Commonwealth countries. This category includes all one-time cyphers and some non-one-time cyphers.
 - Category B. Certain non-one-time cyphers for which the paraphrasing precaution is necessary in the event of publication or outside distribution, because the accurate fitting of the verbatim text to the cryptogram would endanger the cypher key.

The majority of cyphers now used are Category A systems.

Telegrams Requiring Safeguarding of the Verbatim Text

2. Occasionally the copy of a telegram will be round to be headed with a warning to the effect:

"This message must be paraphrased if it is to be communicated to persons outside British Government Departments."

This indicates that a Category B cypher has been used. It will be rare for such a telegram to be of current date but it is not infrequently to be found in the case of telegrams dated prior to September, 1950.

Publication of Texts of Cypher Telegrams

- 3. Whenever it is necessary for the text of a Category B cypher telegram (i.e., one bearing the paraphrase warning) to be published or communicated in any way to anyone not in the Government Service of a British Commonwealth country or the United States Government Service, the following rules must be observed unless the telegram is dated earlier than January, 1944:—
 - (i) The telegram must be thoroughly paraphrased; the entire make-up of the message must be

changed; the order of the paragraphs, sentences, clauses and sequences of words must be varied; synonyms must be substituted and the overall length of the message must be altered.

(ii) No mention must be made of the fact that the

telegram was a cypher telegram,

(iii) The Date-Time Group, the Time of Origin, the Time of Handing In, or any other identification transmitted en clair must not be quoted. Even the encrypted serial number should not be quoted if this is unnecessary.

(iv) Encrypted addresses and delivery instructions

must, wherever possible, be omitted.

(v) External addresses and signatures which were transmitted with, but not encrypted in the same system as, the text of the telegram must be expressed in normal plain language and not in the form as transmitted.

Reason for Special Precautions

4. The reason for the above rules is that possession by unauthorised persons of the encyphered version of a message transmitted in a Category B cypher (which may have been obtained by wireless interception) together with the clear text of the same message would constitute a grave danger to the security of the system concerned. The effects could be far-reaching, affecting both future and past traffic and even affecting the security of other Category B cypher systems.

Co-operation by Originators

- 5. Originators of classified messages should bear in mind the possibility of publication. Where publication is likely the message should be marked "FOR TRANSMISSION IN OTP" (One Time Process) or "CATEGORY A CYPHER" according to instructions issued in their Departments; the need for paraphrasing before publication could then, in nearly all cases, be eliminated.
- 6. In no circumstances may originators dictate the text or portions of the text of classified messages by telephone, even if the telephone is fitted with speech privacy equipment (Secraphone), nor may messages already transmitted in a Category B system (i.e., with the paraphrase warning on the distribution copy) be confirmed by telephone.

Cypher Security Committee

7. Cypher security is dealt with through the Cypher Security Committee which is part of the Higher Defence Machinery. The Committee is responsible for recommending further special instructions on the subject of cypher security which are brought to the notice of those concerned.

CHAPTER VIII

SECURITY OF BUILDINGS AND AREAS CONTAINING CLASSIFIED MATTER

Responsibility for Building and Area Security

1. Each Department is responsible for ensuring that the building(s) and area(s) or portion thereof which it occupies are adequately safeguarded both during and after office hours.

Access to Buildings and Areas

- 2. All possible means of access to buildings should be examined and, if necessary, locks should be strengthened, bars fitted to ground floor windows, etc.
- 3. Buildings and areas or portions thereof containing TOP SECRET and SECRET matter should, where practicable, have one entrance only, controlled during working hours by a Peace Officer or other authorised officer. Access can be further controlled by segregating sections within a security area. Precautions to be taken after working hours, e.g., installation of burglar alarms, provision of patrols or guards, etc., will vary according to the site and the nature of the matter to be protected.

Passes

- 4. In some cases a pass system is essential to security, but the fact that passes have been issued does not automatically ensure security. The issue of passes is advisable in a large Department or a large building housing several Departments, or in an area where access is granted only to certain officers of a Department.
- 5. Each officer receiving a pass should sign for it in a register in the presence of the Departmental Security Officer or the appropriate administrative officer. Passes should be serially numbered and to provide the ideal protection (which may not always be necessary or practicable) they should bear the following information:—
 - (a) photograph and description of holder;
 - (b) signature of holder and issuing officer;
 - (c) an embossed seal over the two signatures;

- (d) conditions of issue;
- (e) instructions to a finder.
 Passes need not necessarily indicate the issuing Department and must not state the buildings or areas to which they give access, except in code.
- 6. Passes should be checked periodically. The loss of a pass must be reported immediately.
- 7. All sets of passes are liable to become compromised in time and should either be replaced by a set in a different colour or revalidated by a stamp that cannot easily be forged. It is advisable for a new set of passes always to be held in reserve in case of emergency.
- 8. Whether or not a pass system operates, officers should be required to sign a register upon entering and leaving a building outside working hours. Where overtime is to be worked, prior written advice should be lodged with guard posts, and guards should be instructed not to admit employees during silent hours, unless the appropriate authority has been received.

Visitors

- 9. Where control of entry is necessary either by a pass system or by recognition, written instructions regarding visitors, workmen, etc., should be given to doorkeepers. To be effective, measures for the control of visitors should include the following:—
 - (a) A register should be signed by all visitors and should show times of arrival and departure, name, business, the Department or firm from which the visitor comes, and the officer to be visited. The Departmental Security Officer should peruse this register periodically.
 - (b) Visitors should be issued with a form or badge authorising entry and this should be collected by the doorkeeper at the exit. If a form is used it should be signed by the officer interviewed upon completion of the visit.
 - particularly, the doorkeeper should telephone the officer to be visited and should see that the visitor is escorted to his office. The officer interviewed is responsible for providing the visitor with escort out of the area.

- (d) It may not be necessary to observe all the above procedure in the case of designated senior official visitors, but a record of the visits should be kept.
- (e) Care should be taken to prevent visitors from seeing classified matter which does not concern them. Officers should see that papers are protected from view and that visitors are not left unattended in rooms containing classified matter.
- (f) Where necessary, bags, cases, parcels, etc., carried by visitors should be subject to control.

Visits by Press, Radio and Other Accredited Representatives

- 10. If permission is granted for visits by press, radio and other accredited representatives to factories or annexes where classified equipment is being produced, the following security principles are to be observed.
 - (a) Classified matter which is not to be viewed must be segregated and protected from observation.
 - (b) An undertaking of secrecy is to be signed.
 - (c) Script and photographs relating to classified equipment and projects are to be submitted for approval before release to press and radio representatives.
 - (d) A security officer should accompany representatives throughout the visit.

Control of Photography

11. Security regulations in regard to the use of cameras will vary with the security classification of a project or establishment or of certain sections of an establishment. Local security instructions should ensure that there is no danger of classified matter being unofficially photographed, and where necessary a register of cameras should be maintained and films submitted to the security officer for clearance before printing.

Custody of Keys

12. Measures for safeguarding keys require constant attention to prevent insecure practices from developing. Such measures are to include the following:—

(a) All keys are to be recorded in a central register which is to be periodically checked, at least quarterly. In addition, it is recommended that there should be an

- occasional check of all keys without warning, to ensure that the regulations for custody are being observed.
- (b) Only in exceptional circumstances should keys be removed from official premises. When it is necessary to remove a key, it should be securely attached by a chain to the clothing of the officer concerned and should never leave his person. (It must be remembered that to take an impression of a key is a very easy matter.) Such keys should not be marked or labelled.
- (c) Both during and after office hours, keys, including the keys of unlocked rooms, cupboards, drawers, etc., should either be in charge of a responsible officer or should be placed in a locked box which is stored in a safe place, preferably a combination safe. Where a building is under continuous armed guard the locked box should be placed in the care of the guard. Keys should not be left where they can be seen by anyone passing. (Highly skilled locksmiths can, after a glance at a key, often produce a duplicate that will, with very little adjustment, operate the lock.) The practice of keeping keys on nails in locked or unlocked drawers or other similar places must be prohibited.
- (d) Duplicate keys should be placed in a sealed container and kept in a combination safe.
- (e) It should be impressed upon all officers that duplicate keys may not be cut without permission of a responsible senior authority.
- 13. The loss of a key must be reported immediately. Action to be taken in the event of such a loss is outlined in Chapter IX. It should be noted, however, that even when a lost key is recovered the security of the lock may be compromised, depending on the circumstances surrounding the loss.

Instructions to Guards, Sentries, etc.

14. The duties of guards, sentries, watchmen, etc., should be clearly detailed in Departmental security regulations. A copy of the relevant parts of these regulations should be handed over by

guards, etc., to their reliefs, but should not be available for scrutiny by unauthorised persons. In addition, guards, sentries, etc., should be fully instructed in their powers of apprehension and detention of persons who attempt to gain unauthorised admission.

CHAPTER IX

ACTION IN CASES OF BREACH OF SECURITY

General

- 1. No practicable system of security can afford complete protection against the skilled agent and no system is proof against foolishness or negligence. However, an efficient system will, with the least possible delay, draw attention to any breach of security which may occur, and will narrow the field of enquiry.
- 2. The success of investigations depends primarily on the time factor, and every officer should instantly report to the Departmental Security Officer any loss or any other possible case in which security may have been compromised. Investigation should be commenced immediately and any assistance required should be sought as early as possible.
- 3. In dealing with a breach of security the main objectives are-
 - (a) to find out what happened;
 - (b) to minimise the damage done:
 - (c) to prevent a recurrence.

Responsibility for Action

- 4. The Department in which a breach of security occurs is responsible for undertaking the necessary investigation, if it originated the matter involved. If not, the breach is to be reported to the originating Department and the investigation will be undertaken either by the Department in which the breach occurred or the originating Department, as agreed upon.
- 5. While the primary responsibility for action rests with the Department or Departments concerned, the advice of the Australian Security Intelligence Organisation may, and in some cases should, be sought. In such cases the Australian Security Intelligence Organisation will indicate whether it wishes to take part in the investigation.

Losses and Leakages

- 6. For the purposes of this chapter breaches of security are divided into two classes—
 - (a) loss where classified matter is missing;
 - (b) leakage where classified matter has come to the knowledge of unauthorised persons.

Losses

- 7. The Departmental Security Officer should first ascertain the basic facts of the loss and, in consultation with the branch concerned, should assess its importance. If initial enquiries show that the loss is not simply due to carelessness or is not otherwise readily explicable, and that therefore there may be some improper motive behind it, the Australian Security Intelligence Organisation should at once be informed so that it may determine whether there is a case for suspecting espionage.
- 8. The loss of a key may have more widespread effects than the loss of a document. Even when a key is recovered, the lock must be regarded as compromised, unless it is established beyond reasonable doubt that there has been no opportunity for an unauthorised person to copy the key. Since the replacement of a lock may be costly and difficult. Departments should decide whether, having regard to all the circumstances surrounding the loss of a key, it is necessary to change the lock. However a lock must be changed if—
 - (a) the key has been lost in circumstances which suggest malicious intent:
 - (b) several keys to the one lock have been lost, even if there are no suspicious circumstances surrounding each loss.

Leakages

9. The Departmental Security Officer should first determine, in consultation with the branch concerned, whether in fact there has been a leakage. (For instance, a newspaper report may be merely an accurate guess based on information already published.) If a leakage has occurred and initial enquiries by the Departmental Security Officer have not provided some ready explanation, the matter should be promptly reported to the Australian Security Intelligence Organisation before further action is taken.

- 10. The Departmental Security Officer should then—
 - (a) establish the distribution of documents involved in the leakage;
 - (b) ascertain whether any copies are missing;
 - (c) inform the Australian Security Intelligence Organisation of details of (a) and (b), and also provide full names, date and place of birth, home address, and nationality of every person on the distribution list.
- 11. In some circumstances it may be desirable to obtain information by means of a written questionnaire.
- 12. Leakages by word of mouth, either deliberately or in careless talk, are the most difficult to prevent or trace, but the possibility that they may occur should always be borne in mind.

Minimising Damage

13. The Departmental Security Officer should see that those concerned are aware of the need to take all possible steps to limit the consequences of a breach of security. The measures that can be taken depend on the nature and content of the matter compromised. For example, cyphers and codes can be changed, and plans for particular operations, whether military or civil, may be capable of alteration.

Preventing Recurrence

14. Each incident may point to a weakness in security arrangements, or to failure by an individual to observe them. In every case the means by which security may be improved should be considered, or the lesson should be brought home to the individual responsible, even if no disciplinary action is necessary.

Possibility of Prosecution

15. A breach of security may constitute an offence against the Commonwealth Public Service Act and Regulations, the Crimes or Defence Acts or one of the relevant statutes mentioned in Chapter XII below, and the question of prosecution may have to be considered. Departmental enquiries must not be carried so far as to prejudice a prosecution, and when preliminary investigation indicates a possible breach of the Acts, Departments should consult the Commonwealth Crown Solicitor.

CHAPTER X

STAFF ENGAGED ON CLASSIFIED WORK

Responsibility of Departments

1. Departments are responsible for determining the branches, annexes, installations, etc., which are to be regarded as classified, and for administering the precautions which must be taken to prevent the employment on classified work of any person who is adversely regarded from a security viewpoint.

Security Clearance

- 2. The Australian Security Intelligence Organisation assists Departments by assessing the suitability from a security viewpoint of existing employees or applicants for employment engaged or to be engaged on classified work. A security clearance given by the Australian Security Intelligence Organisation means that at the date of the check no adverse information is held such as would render a person a security risk for the position which he or she holds or for which an application has been made; a clearance is thus not a testimonial to a person's security standing.
- 3. Personnel should not be employed or led to expect employment on classified work before being security cleared.
- 4. Departmental Security Officers should maintain lists of persons who have been security cleared or denied a clearance, showing the date and those specially cleared for access to TOP SECRET information. It will thus be possible to ensure that staff are not employed on duties for which they have not been security cleared. On transfer to another Department, the clearance or non-clearance should be notified as necessary.

Supervision of Staff

5. The supervision of staff engaged on classified work differs only in degree from the supervision of other staff. Every supervising officer should get to know his subordinates and not confine himself merely to observing how they discharge their official duties. This is particularly important in the case of staff engaged on TOP SECRET or SECRET work. Should the behaviour of

any individual give rise to concern from the security aspect, the matter should be brought to the notice of the Australian Security Intelligence Organisation at once.

Application of Acts and Regulations Dealing with Official Secrecy

6. The provisions of Acts and Regulations dealing with official secrecy and their application to members of the Commonwealth Public Service are dealt with in Chapter XII. Personnel who are to have access to TOP SECRET matter should be required to sign a declaration acknowledging their responsibility under these Acts, and upon leaving the Government Service should sign a further acknowledgment that their responsibility in this regard is a continuing one.

Persons Outside the Government Service

7. Measures regarding persons outside the Government Service who are to be entrusted with classified matter are dealt with in Chapter XI.

CHAPTER XI

CLASSIFIED MATTER ENTRUSTED TO PERSONS OUTSIDE THE GOVERNMENT SERVICE

Approval by Permanent Head

1. Classified matter is to be made available to persons or organisations outside the Government Service only with the approval of the Permanent Head of the originating Department.

Security Clearance

- 2. As in the case of Departmental staff, Departments are responsible for taking the necessary precautions to prevent the employment on classified work of outside personnel adversely regarded from a security viewpoint. The following procedure is desirable:—
 - (a) Where it is necessary for Departments to entrust classified matter outside the Government Service for example to consultants, universities, industries, contractors, etc. the names of those whom it is proposed to approach initially should be submitted to the Australian Security Intelligence Organisation for security assessment.
 - (b) Upon receipt of a clearance, Departments should approach the most senior person concerned and in consultation with him determine the extent of circulation of the classified matter in question. All persons who are to be entrusted with such matter should be the subject of a security assessment.
 - (c) Persons outside the Government Service whom it is proposed to include on Governmental committees, etc., dealing with classified matter should be similarly treated prior to appointment.
 - (d) Departments should maintain a list of outside persons who have been security cleared or denied a clearance, similar to the record of Departmental personnel (Chapter X. paragraph 4).

Application of Acts dealing with Official Secrecy

3. Application of the Acts dealing with official secrecy to persons outside the Government Service is dealt with in Chapter XII. Their responsibilities under these Acts should be brought to the notice of all such persons who are to be entrusted with classified matter, and an appropriate acknowledgment should be signed by those dealing with TOP SECRET matter.

General Security Arrangements

4. Before classified matter is actually handed over to outside persons or organisations. Departments are responsible for ensuring that their attention is drawn to the special precautions to be taken in connection with dissemination, custody and transmission, and that their security arrangements conform as nearly as possible to those of Departments. Particular emphasis should be laid on the importance of circulating classified matter only to those who need it for the efficient performance of their work, of acquainting individuals only with those facts which concern them, and of concealing the significance of matter wherever possible.

Government Contracts

5. Appropriate security provisions are included in contracts for the manufacture or supply of classified matter which are administered by the Departments of Supply and Defence Production. Similar regulations should be enforced by other Departments procuring classified matter from private contractors.

CHAPTER XII

ACTS AND REGULATIONS DEALING WITH OFFICIAL SECRECY

Introduction

1. The Commonwealth Public Service Act and Regulations, the Crimes Act 1914-1946, which deals generally with offences against the Commonwealth, and also certain other Acts mentioned below, contain provisions for the prevention of the unauthorised disclosure of official information. These provisions apply whatever the subject matter of the information; whether it is important or not is irrelevant. Any act or disclosure contrary to the provisions for official secrecy, as enacted and prescribed, is an offence against the law.

The Commonwealth Public Service Act and Regulations

- 2. The Commonwealth Public Service Act, which applies to persons employed in the Public Service of the Commonwealth, provides that regulations may be made for giving effect to the Act. In particular there is power for the making of regulations "for requiring officers to take oaths or affirmations of secrecy in relation to the matters coming to their knowledge in the course of their employment, and for prescribing the form of such oaths or affirmations" and also "for regulating the duties and conduct of officers".
- 3. The Commonwealth Public Service Regulations expressly forbid the use, other than for the discharge of official duties, of information obtained by an officer through his connexion with the Commonwealth Public Service, and the unauthorised disclosure of the contents of official papers or of any information concerning public business or official matters. These provisions are made by Regulations 34 and 35, as follows:—
 - "34. An officer shall not-
 - (a) use for any purpose, other than for the discharge of his official duties, information gained by or conveyed to him through his connexion with the Service; or

(b) publicly comment upon any administrative action or upon the administration of any Department:

Provided that nothing in this paragraph shall prevent an officer resident in any Territory within the

vent an officer resident in any Territory within the Commonwealth from publicly commenting upon

civic affairs relating to that Territory.

35. Except in the course of official duty, no information concerning public business or any matter of which an officer has knowledge officially shall be given, directly or indirectly, nor shall the contents of official papers be disclosed, by an officer without the express authority of the Chief Officer."

The Crimes Act, Part VI — Offences by and against Public Officers

- 4. This Part of the Crimes Act includes Section 70 which applies directly to every "Comonwealth Officer", an expression which by Section 3 is defined to mean any person holding office under the Commonwealth, and includes any person permanently or temporarily employed in the Public Service of the Commonwealth, or in or in connection with the Naval, Military, or Air Forces of the Commonwealth, or in the service of any public authority under the Commonwealth and includes an officer of the Commonwealth Bank.
- 5. Section 70 reads as follows: "Any person who, being a Commonwealth Officer, publishes or communicates any fact which comes to his knowledge by virtue of his office, and which it is his duty to keep secret, or any document which comes to his possession by virtue of his office, and which it is his duty to keep secret, except to some person to whom he is authorised to publish or communicate it, shall be guilty of an offence.

 Penalty: Imprisonment for two years."

The Crimes Act, Part VII - Breach of Official Security

6. Section 78 of this Part of the Crimes Act is of general application, and provides that if specified acts are done by "any person for any purpose prejudicial to the safety or interest of the Commonwealth or any part of the Queen's Dominions" then that person shall be guilty of an indictable offence, the penalty for which is imprisonment for seven years. In view of its general nature Section 78 is not here considered in detail.

- 7. Section 79 of Part VII also is of general application but this Section applies in particular to any person who "holds or has held office under the Queen or the Commonwealth", or who "holds or has held a contract made with or by or on behalf of the Queen or the Commonwealth" or who "is or has been employed under a person who holds or has held such an office or contract". In view of this particular application of Section 79 it may well be examined, as follows:—
 - (a) Section 79 applies where any person has in his possession or control any sketch, plan, photograph, model, article, note, document or information:—
 - (i) which relates to or is used in a prohibited place or anything in such a place, or
 - (ii) which has been made or obtained in contravention of Part VII of the Act, or
 - (iii) which has been entrusted in confidence to him by any person holding office under the Queen or the Commonwealth, or
 - (iv) which he has obtained owing to his position as a person who holds or has held office under the Queen or the Commonwealth, or as a person who holds or has held a contract made with or by or on behalf of the Queen or the Commonwealth, or as a person who is or has been employed under a person who holds or has held such an office or contract.
 - (b) In those circumstances the person is guilty of an offence, the penalty for which is imprisonment for seven years, if that person:—
 - (i) communicates the sketch, plan, photograph, model, article, note, document or information to any person, other than a person to whom he is authorised to communicate it, or a person to whom it is, in the interest of the Commonwealth or of some part of the Queen's Dominions, his duty to communicate it, or
 - (ii) retains the sketch, plan, photograph, model, article, note, or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it.

- (c) It is an offence also if any person receives any sketch, plan, photograph, model, article, note, document or information, knowing or having reasonable cause to believe, at the time when he receives it, that the communication to him is in contravention of Part VII of the Act, unless he proves that the communication to him was contrary to his desire. In this case also the penalty is imprisonment for seven years.
- (d) Prohibited places are defined by Section 80 of Part VII. The definition includes any place belonging to the Queen or the Commonwealth used for the purpose of building, repairing, making, or storing any ship, arms, or materials or instruments of use in time of war, or any plans or documents relating thereto.
- (e) Section 77 sets out definitions which apply to Part VII of the Act. It is provided that "the Commonwealth" includes the Government thereof, and includes any Territory under the control of the Commonwealth and the Government thereof; "document" includes part of a document; "model" includes design. pattern, and specimen; "sketch" includes any photograph or any other mode of representing any place or thing. Expressions referring to communicating or receiving include any communicating or receiving, whether in whole or in part, and whether the sketch, plan, model, article, note, document or information itself, or the substance, effect, or description thereof only, be communicated or received. Expressions referring to obtaining or retaining any sketch, plan, model, article, note, or document, include the copying or causing to be copied the whole or any part of any sketch, plan, model, article, note, or document. Expressions referring to the communication of any sketch, plan, model, article, note, or document, include the transfer or transmission of the sketch, plan, model. article, note, or document.
- 8. It will therefore be seen that:—
 - (a) Any person holding office under the Queen or the Commonwealth will be guilty of an offence under Section 79 if any article or document or information which he has obtained owing to his official position

is communicated by him except where he has authority to communicate it or a duty to communicate it. Also he will be guilty of an offence if such an article or document (as distinct from oral information) is retained by him when he has no right to do so or when it is contrary to his duty to do so.

- (b) Where there has been a lawful confidential communication of any article or document or information then the recipient is under a similar duty not to make any unauthorised communication thereof and not to retain it. Failure to observe this duty is an offence by that recipient under Section 79.
- (c) In the case of any article or document or information which relates to or is used in a prohibited place or anything in such a place, any unauthorised communication or retention thereof (as above) by any person is an offence under Section 79.
- (d) If any article or document or information has been made or obtained in contravention of Part VII of the Act then under Section 79 it is an offence for any person to communicate or retain it except as is authorised by that Section.
- (e) The mere receipt of any article or document or information is an offence under Section 79 by any person "knowing, or having reasonable ground to believe, at the time when he receives it" that the communication to him is in contravention of Part VII of the Act, unless he proves that the communication to him was contrary to his desire.

Other Provisions of the Crimes Act

9. Other sections of the Crimes Act provide that any person who aids, counsels, or procures, or is directly or indirectly knowingly concerned in or party to the commission of an offence shall be deemed to have committed that offence and shall be punishable accordingly (Section 5), and that any person who attempts to commit any offence shall be guilty of an offence and shall be punishable as if the attempted offence had been committed (Section 7).

- 10. In the investigation of any breaches of security it must be remembered that the consent of the Attorney-General to any prosecutions under Part VII of the Crimes Act is required by Section 85 which provides:—
 - "85. (1) A prosecution under this Part of this Act shall be instituted only by or with the consent of the Attorney-General or of a person acting under his direction:

Provided that a person charged with any offence against this Part of this Act may be arrested, or a warrant for his arrest issued and executed, and he may be remanded in custody or on bail, notwith-standing that the consent of the Attorney-General or a person acting under his direction has not been obtained, but no further proceedings shall be taken until that consent has been obtained.

(2) Nothing in this Section shall prevent the discharging of the accused if proceedings are not continued within a reasonable time."

The Defence Act 1903-1949

- 11. Section 73A of this Act provides:—
 - "73A (1) Any member of the Defence Force or officer in the Public Service of the Commonwealth who communicates to any person otherwise than in the course of his official duty any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air-force aerodrome or establishment or any other naval, military or air-force information shall be guilty of an offence.
 - (2) Any person who unlawfully obtains any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or air-force aerodrome or establishment, or to any of the defences of the Commonwealth or any other naval, military or air-force information, shall be guilty of an offence.

The punishment for an offence under Section 73A is:-

(i) if the offence is prosecuted summarily — a fine not exceeding £100, or imprisonment for six months, or

- both; or in the case of a body corporate a fine not exceeding £1000.
- (ii) if the offence is prosecuted on indictment a fine of any amount, or imprisonment for any term, or both."
- 12. Section 82 of the Defence Act provides:
 - "82. (1) Any person who, without lawful authority, makes or attempts to make any sketch, drawing, photograph, picture or painting of any fort, battery, fieldwork, fortification, aircraft, air-force establishment, aircraft material or any naval, military or air-force work of defence in the Commonwealth or of any portion there-of shall be liable to a penalty not exceeding £100 or, at the discretion of the Court, to be imprisoned, with or without hard labour, for any period not exceeding six months;

The Supply and Development Act 1939-1948

13. Section 25 of this Act provides for the observance of secrecy:—

"An officer or employee of the Department, a member of a Committee or of a Board constituted, or deemed to have been constituted, under this Act, a person performing any duty or function in relation to any matter specified in or arising under this Act or any regulation made under, or in force by virtue of, this Act and an officer of the Commonwealth or a State to whom information furnished in pursuance of this Act has been disclosed by virtue of his official position, shall not, except as allowed by this Act or the regulations, divulge any information or particulars furnished in pursuance of this Act or the regulations.

Penalty: Fifty pounds or imprisonment for three months or both."

The Defence (Special Undertakings) Act 1952

14. This Act deals with special defence undertakings and makes provision for prohibited areas and restricted areas to be declared for the purposes of the Act. Section 9, subsection 2 provides:—

"A person shall not, without lawful authority or excuse-

- (a) make a photograph, sketch, plan, model, article, note or other document of, or relating to, a prohibited area or anything in a prohibited area; or
- (b) obtain, collect, record, use, have in his possession, publish or communicate to some other person a photograph, sketch, plan, model, article, note or other document or information relating to, or used in, a prohibited area, or relating to anything in a prohibited area.

Penalty: Imprisonment for seven years."

- 15. Prosecutions under the Act require the consent of the Commonwealth Attorney-General or of a person acting under his direction, but the Act provides:—
 - "Section 28. (2) A person charged with an offence against this Act or the regulations may be arrested, or a warrant for his arrest may be issued and executed, and he may be remanded in custody or on bail, notwithstanding that the consent of the Attorney-General or of a person acting under his direction has not been obtained, but no further proceedings shall be taken until that consent has been obtained.
 - (3) Nothing in this section prevents the discharge of a person charged if proceedings are not continued within a reasonable time."

Various Other Commonwealth Acts

16. Provisions are contained in various other Commonwealth Acts for the preservation of the secrecy of information which is obtained pursuant to those Acts. Included among these are:—

Income Tax Assessment Act,
Sales Tax Assessment Act,
Navigation Act,
Commonwealth Electoral Act,
Australian Industries Preservation Act.

The Application of the Provisions to Public Servants and Others Employed by the Government and to Persons not in the Employ of the Government

17. Some of the provisions outlined above are of general application, their operation covers not only persons in the employ of the Government but also every person who is subject to and entitled to the benefit of the laws of the Commonwealth of Australia. Section 78 of the Crimes Act applies to any such person without restriction, and Section 79 also has this general application and in addition refers to the holding of office under the Queen or the Commonwealth; thus it applies particularly to members of the Commonwealth Public Service and persons employed by Commonwealth or State organisations or instrumentalities.

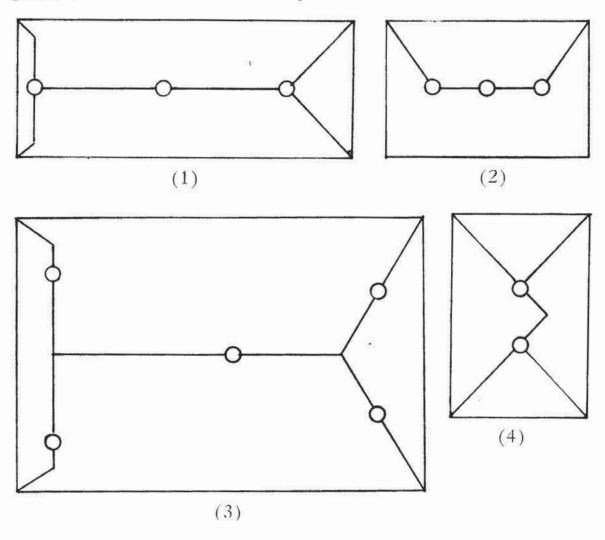
The Defence (Special Undertakings) Act also applies generally. Its operation covers all members of the community including public servants.

18 The Commonwealth Public Service Act and Regulations applies to persons employed in any capacity in the Public Service of the Commonwealth. Section 70 of the Crimes Act refers to acts done by any person permanently or temporarily employed in the Public Service of the Comonwealth, and also any other person who is within the definition of a Commonwealth officer as provided by that Act. The Defence Act partly applies to "any member of the Defence Force or officer in the Public Service of the Commonwealth", and in part is of general and unrestricted application. The Supply and Development Act refers specifically to "an officer or employee of the Department" and to other officials and employees and also to any "officer of the Commonwealth or a State to whom information furnished in pursuance of this Act has been disclosed by virtue of his official position". The various other Commonwealth Acts in the main apply directly to the persons (normally Public Servants) who are employed in the Departments operating by virtue of or in respect of the particular Act.

APPENDIX A

SEALING ENVELOPES

When TOP SECRET, SECRET or CONFIDENTIAL matter is prepared for despatch, the inner envelope should be sealed with wax in whichever of the four ways shown below is appropriate to the form of the envelope.



Note.—Sealing wax should be spread as thinly as possible, and the die of the seal pressed firmly into the wax to ensure that the seal cannot be removed intact.

624

APPENDIX B

CLASSIFIED EQUIPMENT IN TRANSIT

- 1. The following measures will be taken to safeguard classified equipment in transit:—
 - (a) The responsibility for making the security arrangements rests with the consignor. When the physical security passes out of his hands, it is his responsibility to ensure that the person temporarily in charge is made aware of the classified nature of his charge. The consignor is the factory, annexe, establishment, ship, station, unit, or formation, etc., having physical custody of the equipment when it has to be moved.
 - (b) The consignor will check the grading of the equipment before despatch as it may be appropriate at this stage to downgrade the equipment.
 - (c) The consignor is responsible for informing the consignee of the details of despatch and transport, in ample time for arrangements to be made for its reception. Route, time of departure and halting places must be varied for each particular consignment.
 - (d) TOP SECRET and SECRET equipment will be covered by a system of receipts at all points of transference of custody.
 - (e) Classified equipment will be carried in closed vehicles where possible. If this cannot be done, it will be crated, sheeted or otherwise camouflaged or concealed. If transport is by rail, and break of gauge necessitates unloading and reloading, special security precautions are to be taken.
 - (f) When TOP SECRET or SECRET equipment is delivered to sea ports, air ports or rail or road terminal points, a guard will be maintained during loading and unloading operations. Where equipment is placed into Bond Stores, a receipt will be obtained and a guard placed during storage.

- (g) Where lock-up sea stowage stipulated for classified equipment cannot be provided for reasons of size or expediency, the consignor will arrange with the Master of the vessel for the safe custody of the equipment during passage. The Master of the vessel will ensure that the transfer of custody at destination is made to an authorised representative of the consignee.
- (h) Drivers of vehicles and escorts of classified equipment will be security checked. They will be issued with written security instructions when accompanying TOP SECRET and SECRET equipment and will be given security instructions when accompanying CONFID-ENTIAL or RESTRICTED equipment. No indications of the nature or the purpose of the equipment is to be shown in these instructions.
- (i) Where private firms contract to move classified equipment, a security check on the firms' employees involved in the movement will be required, and an escort provided in accordance with paragraph 2 below.
- 2. The following specific rules will apply, subject to the above measures:—
 - (a) TOP SECRET Equipment-
 - (i) Rail TOP SECRET equipment, when transported by rail, will be loaded in a separate van which will be locked and sealed. An armed escort, including a Commissioned or Security Officer, will always be provided.
 - (ii) Road Movement of TOP SECRET equipment by road will be under escort of an armed guard in each vehicle, additional to the driver. If vehicles are in convoy, a Commissioned Officer or Security Officer will be appointed in overall command. No vehicle will ever be left unattended and no unauthorised persons will be permitted to see the equipment. This is particularly important during loading and un-

loading of vehicles, and at halts. In the event of a break-down, or where night halts are necessary, the officer in charge of the escort is to make parking arrangements with the nearest military authority, or failing that, with the Civil Police.

- (iii) Sea TOP SECRET equipment of a bulky nature, when transported by sea, will be sent in a Naval vessel, a Service transport or a vessel under Service control, in a lock-up stowage. It will bear the marking "LOCK-UP STOWAGE". TOP SECRET packages transported by sea, will be sent by "Safe Hand" method in a Naval vessel or in the personal care of the Master of a British vessel. (For details of "Safe Hand" method see Chapter V, paragraph 8.)
- (iv) Air -- TOP SECRET equipment carried by air will be despatched "Safe Hand" method in a Service aircraft or in the care of the Captain of an aircraft of a British airline company which has been authorised to carry "Safe Hand" matter. TOP SECRET equipment should not be carried by air where the route is over foreign territory, but if this is necessary it should be in charge of a courier.
 - (v) Post TOP SECRET equipment will never be sent by civil post.

(b) SECRET Equipment—

- (i) Rail SECRET equipment transported by rail is to be despatched in a separate locked van and is to be accompanied by an armed escort.
- (ii) Road -- SECRET equipment transported by road will be under the escort of an armed guard in each vehicle in addition to the

driver. No vehicle will ever be left unprotected and no unauthorised persons will be permitted to see the equipment. This is particularly important during loading, unloading, and at halts. In the event of a break-down or where night halts are necessary, the escort will make parking arrangements with the nearest military authority, or, failing that, with the Civil Police

- (iii) Sca -- SECRET equipment of a bulky nature, transported by sea, will be sent in a British vessel in a lock-up stowage and marked "LOCK-UP STOWAGE". SECRET packages sent by sea are to be sent "Safe Hand" method.
- (iv) Air --- SECRET equipment sent by air is to be sent "Safe Hand" method. The "Speed Pack" and "Precious Cargo" stowages are available in some aircraft for bulky equipment. If the route is over foreign territory, the equipment should be stowed in bags sealed with diplomatic seal so that, in the event of a landing, it is immune from foreign Customs inspection.
- (v) Post -- If a "Safe Hand" Service is not available, SECRET packages may be sent by registered mail to destinations within Australia.

(c) CONFIDENTIAL Equipment—

(i) Rail - CONFIDENTIAL equipment when sent by rail will be cased or otherwise concealed and loaded into a locked van. Where stowage is other than in a locked van, an escort is to be provided. Where break of railway gauge necessitates un loading and reloading, escort will be provided locally.

- vii) Road Equipment is to be sent in a locked van or truck. Where this is not possible, an escort, in addition to the driver of the vehicle, is to be provided. Vehicles must not be left unprotected.
- (iii) Sea To be transported in a British vessel in a lock-up stowage.
- (iv) Air If carried in Service aircraft no escort is required. If carried in civil aircraft, "Safe Hand" method is to be employed.
- (v) Post If sent through civil post, packages are to be sent registered method.
- (d) RESTRICTED Equipment-

RESTRICTED equipment is to be moved under conditions which will not give access or view to unauthorised persons.



COMMONWEALTH OF AUSTRALIA

SECURITY

CLASSIFIED MATTER

Z

GOVERNMENT DEPARTMENTS

INSTRUMENTALITIES

ATTORNEY-GENERAL'S DEPARTMENT Issued by the

MAY, 1954

REPRINTED JUNE, 1960 INCORPORATING AMENDMENTS Nos. 1 AND 2

RESTRICTED

35二十4 時間

000

RESTRICTED



COMMONWEALTH OF AUSTRALIA

SECURITY

CLASSIFIED MATTER

GOVERNMENT DEPARTMENTS

INSTRUMENTALITIES

ATTORNEY-GENERAL'S DEPARTMENT Issued by the

May, 1954

REPRINTED JUNE, 1960 INCORPORATING AMENDMENTS Nos. 1 AND 2

FOREWORD

I commend this booklet to the attention of all members of the Commonwealth Government Service of Australia.

routine matter of administration, but whether or not it is improperly used depends upon your or even international security or it may be a It is the duty of each one of you to safeguard the official information which is entrusted to you. It may be information affecting national integrity and your care.

The rules laid down in this booklet are designed to help you fulfil this duty, and it is essential that they should be faithfully observed.

PRIME MINISTER R. G. MENZIES

May, 1954

RESTRICTED

RESTRICTED

CONTENTS

Chapter	7.					I	Page
. п		INTRODUCTION	8	;	:	•	6
	Para. 1	General		:	:	•	
	8	Definitions	:	***	:		10
	6	Departmental	Security	Officers	:	:	33
	10	Enquiries on	Security	- C	÷	:	=
11	CLASSII	CLASSIFICATION OF OFFICIAL MATTER	OFFICIA	L MATT	ER		13
	Para. 1	Security Classifications	sifications	:			,,
	2	Unclassified Matter	latter	1	21	**	17
	3	Principles to be Applied in Classifying	be Appli	ed in C	lassify	/ing	
		Matter		:	2		33
	9	Responsibility for Classification and classification	for Class	sification		Re-	19
	7	Overclassification	ion		:	:	33
	6	Classification Marking	Marking		1	•	20
	12	Numbering	:	:	:	:	2
111	DISSEM	DISSEMINATION OF CLASSIFIED MATTER	CLASSIF	TED MA	TTE	: ~	21
	Para. 1	General — Th	- The "Need to Know" Principle	o Know"	Prine	ciple	2
	3		F and SEC	RET Reg	ristrie	. · · · · · · · · · · · · · · · · · · ·	
	4	Distribution of Classified Matter	of Classifie	d Matter	:		
	7	Reproduction of Classified Matter	of Classifi	ed Matter	:		21
	11	Discussion of Official Business	Official	Business	1	•	44
	12	Telephone Conversations	onversation	sı	:	:	**
JV	CUSTO	CUSTODY OF CLASSIFIED MATTER	SIFIED M	ATTER			ု
	Para. 1	Storage of Classified Matter	lassified M	Latter	:	*	
	7	Access to Storage Containers	orage Cor	ntainers	8		લ
	8	Combinations of Safes	of Safes	3	•	:	6
	6	Keys	:	:	*		2

MAY, 1954

Page 5

Chapter	VIII		X	× .	May, 195
C					
Page Protection of Classified Matter in Actual Use 26 Office and Area Inspection	Receipts for Custody Accounting for Classified Matter Held Department	MISSION OF CLASSIFIED MATTER Envelopes Carriage Within a Department	"Safe Hand" Transmission	CODEWORDS AND NICKNAMES	RESTRICTED
Chapter 10	12 13 14 17 20	V TRANSI Para. 1 5 6	8 9 10 112 115 116 117	VI CODEW Para. 1 5 6 VII CYPHER Para. 1 2 3	Puge 6

				Are Othe	
AREAS Areas					
and and and	Responsibility for Building and Security	Responsibility for Building and A Security Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Ot Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc.	Responsibility for Building and A Security	Responsibility for Building and A Security	Responsibility for Building and A Security Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Ot Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc. In CASES OF BREACH OF SECURI General Responsibility for Action Responsibility for Action Losses and Leakages
Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Accredited Representatives Control of Photography Custody of Keys	Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc	Access to Buildings and Areas	Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Othe Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc. N IN CASES OF BREACH OF SECURIT General	Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Othe Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc. N IN CASES OF BREACH OF SECURIT General Responsibility for Action	Access to Buildings and Areas Passes Visitors Visits by Press, Radio and Othe Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc. N IN CASES OF BREACH OF SECURIT General Responsibility for Action Responsibility for Action Losses and Leakages
Passes Visitors	Passes Visitors Visits by Press, Radio and Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc.	Passes	Passes	Passes	Passes Visitors Visits by Press, Radio and Other Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc. NIN CASES OF BREACH OF SECURITY General Responsibility for Action Losses and Leakages
Visitors Visits by Press, Radio and Accredited Representatives Control of Photography Custody of Keys	Visitors Visits by Press, Radio and Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc.	Visitors	Visitors	Visitors	Visitors Visits by Press, Radio and Other Accredited Representatives Control of Photography Custody of Keys Instructions to Guards, Sentries, etc. N IN CASES OF BREACH OF SECURITY General Responsibility for Action Losses and Leakages
Visits by Press, Radio and Accredited Representatives Control of Photography Custody of Keys	Visits by Press, Radio and Accredited Representatives Control of Photography	Visits by Press, Radio and Other Accredited Representatives	Visits by Press, Radio and Other Accredited Representatives	Visits by Press, Radio and Other Accredited Representatives	Visits by Press, Radio and Other Accredited Representatives
Control of Photography Custody of Keys		Control of Photography	Control of Photography	Control of Photography Custody of Keys Instructions to Guards, Sentries, etc N IN CASES OF BREACH OF SECURITY General Responsibility for Action	Control of Photography
:		Custody of Keys	Custody of Keys	Custody of Keys	Custody of Keys Instructions to Guards, Sentries, etc IN IN CASES OF BREACH OF SECURITY General Responsibility for Action Losses and Leakages
	14 Instructions to Guards, Sentries, etc	1 Instructions to Guards, Sentries, etc	Instructions to Guards, Sentries, etc IN CASES OF BREACH OF SECURITY Ceneral	Instructions to Guards, Sentries, etc IN IN CASES OF BREACH OF SECURITY General Responsibility for Action	Instructions to Guards, Sentries, etc IN CASES OF BREACH OF SECURITY Coneral Responsibility for Action Losses and Leakages
General Responsibility for Action Losses and Leakages	General Responsibility for Action Losses and Leakages Losses			Losses	
No. IN CASES OF BREACH OF SECURITY General Responsibility for Action Losses and Leakages Losses Leakages	General Responsibility for Action Losses and Leakages Leakages	Responsibility for Action Losses and Leakages Losses Leakages	Losses and Leakages Losses Leakages	Losses Leakages	Leakages
N IN CASES OF BREACH OF SECURITY General	General Responsibility for Action Losses and Leakages Losses	Responsibility for Action Losses and Leakages Losses Leakages Minimising Damage	Losses and Leakages Losses Leakages Minimising Damage	Losses Leakages	Minimising Damage
NIN CASES OF BREACH OF SECURITY General Losses and Leakages Losses Minimising Damage Minimising Damage Preventing Recurrence	General Responsibility for Action Losses and Leakages Leakages	Responsibility for Action Losses and Leakages Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution	Losses and Leakages Losses Leakages Minimising Damage Preventing Recurrence	Losses	Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution
ON IN CASES OF BREACH OF SECURITY General Losses and Leakages Losses Minimising Damage Preventing Recurrence Preventing Recurrence Preventing Of Prosecution	General Responsibility for Action Losses and Leakages	Responsibility for Action Losses and Leakages Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution	Losses and Leakages Losses Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution FNGAGED ON CLASSIFIED WORK	Leakages	Minimising Damage Preventing Recurrence Possibility of Prosecution FNGAGED ON CLASSIFIED WORK
ON IN CASES OF BREACH OF SECURITY General	General Responsibility for Action Losses and Leakages	Responsibility for Action Losses and Leakages Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK	Losses and Leakages Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK	Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK	Minimising Damage
General	General	Responsibility for Action Losses and Leakages	Losses and Leakages Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK Responsibility of Departments	Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK Responsibility of Departments	Minimising Damage
ON IN CASES OF BREACH OF SECURITY General Losses and Leakages Losses Minimising Damage Preventing Recurrence Preventing Recurrence Preventing of Prosecution Rossibility of Prosecution ENGAGED ON CLASSIFIED WORK Responsibility of Departments Security Clearance	General Responsibility for Action Losses and Leakages	Responsibility for Action Losses and Leakages	Losses and Leakages Losses Leakages Minimising Damage Preventing Recurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK Responsibility of Departments Security Clearance	Losses Leakages Preventing Becurrence Possibility of Prosecution ENGAGED ON CLASSIFIED WORK Responsibility of Departments Security Clearance	Minimising Damage
ON IN CASES OF BREACH OF SECURITY General Losses and Leakages Losses Minimising Damage Preventing Recurrence					H
General					E

CLASSI	TO PER-	, 1
Para. 1	SONS OUISIDE THE GOVERNMENT SERVICE Para, I Approval by Permanent Head	55
2		
3	ion of Acts dealing	i
4	General Security Arrangements	40
- u	Concrete Security Attangements	
9	Government Contracts	2
ACTS /	ACTS AND REGULATIONS DEALING WITH	
OFFICE	OFFICIAL SECRECY	55
Para, 1		
2	ct a	-
4	77	56
9	The Crimes Act, Part VII — Breach of Official Security	5
6	Other Provisions of the Crimes Act	59
11	The Defence Act 1903-1949	8
13	The Supply and Development Act 1939-1948	61
14	The Defence (Special Undertakings) Act	62
16	E	:
17	The Application of the Provisions to Public Servants and Others Employed by the Government and to Persons not in the	
	Employ of the Government	00
:		
Appendix A SEALIN	SEALING ENVELOPES	5
SELECTED THE PROPERTY	··· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··	Š

AMENDMENT SHEET

C meaning Br	- Finered by	June 1960		
nt Sheet	Date Entered	Reprint		
Amendment Sheet	Date Issued	March 1956	December 1950	
:	Vo	1		

May, 1954

CHAPTER 1

INTRODUCTION

General

It supersedes the Instructions for the Security of Official Documents and Information issued by the Prime Minister's Department on the 19th October, 1948, and will This booklet outlines the principles to be followed by Commonwealth Departments and Statutory Authorities in safeguarding official matter. be revised as necessary. The unauthorised disclosure of official information may ment to the Government to jeopardising the security not only of Australia, but of other countries in the British Commonwealth, and have serious consequences, ranging from administrative embarrassour Allies with whom information is shared. The security of official information is the personal concern of everyone in the Government Service, and all public servants should be aware of their responsibility in this regard.

primary duty of every public servant to be discreet in the use of any information obtained in an official capacity. The provisions In the first place, it must be emphasized that it is a of the Commonwealth Public Service Act and Regulations and of the Crimes, Defence and other Acts, in this regard, are set out in Chapter XII. Certain official matter requires to be specially protected.
 Such matter is allocated a security classification and is known as "classified matter"

ts physical security. Effective office security measures may often The security of classified matter depends primarily on the and Section which is enforced constantly so that observance becomes a habit. Such a system should ensure that access to their duties, and that adequate measures are taken at all times for result in some additional work and administrative inconvenience, integrity, discretion, and vigilance of officers who deal with it, and secondly, on an effective system within each Department, Branch classified matter is limited to those who require it in the course of out this must be accepted in the interests of national security.

MAY, 1954

RESTRICTED

Page 9

The amount of classified matter handled will vary greatly between Departments, according to their functions, and their security requirements may differ. However, the principles set out in this To ensure that classified matter is treated with equal care by all concerned, it is essential that a common standard of classifibooklet should be adhered to by all, and security instructions framed by Departments to suit their individual needs should be in cation and safeguarding should be observed by all Departments. accordance with these principles.

Definitions

For the purposes of this booklet the following definitions apply:

The term "Department" is used to cover any Australian Commonwealth Government Department, Service or Statutory Authority. (a)

The term "officer" includes any person permanently or temporarily employed in a Department as defined (b)

The term "matter" includes everything, regardless of its physical character, on or in which information is recorded or embodied. Books, reports, articles, notes, cordings, machinery, models, apparatus, devices, and letters, drawings, sketches, plans, photographs, reall other products or substances fall within the general Information which is transmitted orally is considered as "matter" for purposes of term "matter". security. (c)

The term "document" covers any form of recorded information, including printed, written, drawn or painted matter, sound recordings, photographs, films, etc. "Documents" are included in "matter" (p)

supplies, ammunition, etc. "Equipment" is included in "matter". (e) "Equipment" includes machinery, apparatus, devices.

Departmental Security Officers

senior officer should be appointed Departmental Security Officer rests with the Permanent Head. For administration purposes a on a full or part time basis, according to the varying requirements The responsibility for security within each Department

RESTRICTED

May, 1954

RESTRICTED

of Departments. This officer will be concerned with the issuing of instructions on all aspects of security, with their observance, and with action in case of breaches of security.

Enquiries on Security

Departments to the Director-General, Attorney-General's Department, "D" Branch, Box 5105 BB, G.P.O., Melbourne. Any enquiries on security matters should be addressed by

MAY, 1954

CHAPTER II

CLASSIFICATION OF OFFICIAL MATTER

Security Classifications

degree of protection requiring special protection is, according to the classifications or gradings, each with its own rules. This system is used in common by British and United States authorities. The four security classifications or gradings are:—

TOP SECRET SECRET CONFIDENTIAL RESTRICTED

These classifications are defined hereunder and some illustrations are given of their application to both civil and defence matters. The illustrations are not intended to be exhaustive but to provide a general guide for the preparation of departmental instructions. Each Department should carefully consider the four definitions and formulate examples suited to its individual needs.

TOP SECRET

Information and material (matter), the unauthorised disclosure of which would cause exceptionally grave damage to the nation, politically, economically, or from a security aspect. This category is reserved for the nation's closest secrets and is to be used with great reserve. Very little matter belongs in the TOP SECRET category.

Illustrations

- (a) Very important political documents dealing with such matters as negotiations for major alliances, etc.
- (b) Major governmental projects such as drastic proposals to adjust the nation's economy (before official publication).
- (c) Matter relating to new and far reaching experimental, technical and scientific developments in methods of warfare or defence, e.g., vital matter relating to

MAY, 1954

atomic warfare, defence against biological warfare, or matter affecting future operational strategy. . A TOP SECRET grading is justified if:

(i) a project is likely to influence military strategy materially;

(ii) it gives us a prolonged military advantage over

other nations;
(iii) it is liable to compromise some other project similarly graded. (d) Critical information relating to vital strategic areas and the supply of vital strategic materials.

Information which would indicate the capabilities or major successes of our intelligence services or which would imperil secret sources. (e)

Critical information about cryptography so far as it relates to devices and equipment under development. (£)

Certain compilations of data or items which individually may be classified SECRET or lower, but which collectively should be put in a higher grade. 60

B.

Information and material (matter), the unauthorised disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation or of any governmental activity thereof, or would be of great advantage to a foreign nation.

This classification should be used only for highly important matter and is the highest classification ordinarily used.

Illustrations

- would be in the TOP SECRET category) with other (a) High level directives dealing with important negotiations (as distinct from major negotiations which countries.
- Proposals for new schemes of governmental or other controls, foreknowledge of which would seriously prejudice their operation. 9
- Matter relating to certain new methods of warfare or defence, including scientific and technical developments, not classified as TOP SECRET, e.g., new 0

RESTRICTED

May, 1954

RESTRICTED

designs of Service aircraft, guided projectiles, tanks, radar and anti-submarine devices. A SECRET grading is justified if:

(i) a project materially influences a major aspect of

(ii) a novel principle applicable to existing important military tactics;

the project is sufficiently revolutionary to result in a major advance in existing techniques or in projects is involved

(iv) it is liable to compromise some other projects the performance of existing secret weapons;

already so graded.

(d) War plans or details of schemes for the defence of areas other than vital strategic areas, including plans or particulars of operations connected with them.

maps, etc., relating to important defences, establish-Vital military information, including photographs, ments, and installations. (e)

Intelligence which is not in the TOP SECRET category but which would reveal a secret source, or the value of which depends upon concealing the fact that we possess it. (£)

Cryptographic devices and equipment unless specifically assigned to a lower classification. 8

ally may be classified CONFIDENTIAL or lower, but Certain compilations of data or items which individuwhich collectively, should be put in a higher grade. (h)

CONFIDENTIAL Ü

cause administrative embarrassment, or unwarranted injury to Information and material (matter), the unauthorised disclosure of which, while not endangering the national security, would be prejudicial to the interests or prestige of the nation, would Most matter will, on proper analysis, be classified no an individual, or would be of advantage to a foreign power. higher than CONFIDENTIAL.

Illustrations

(a) Plans of Government projects such as land development, hydro-electric schemes, road development, or development of areas.

May, 1954

- (b) Routine Service reports, e.g., on operations and exercises, which contain information of value but not of vital interest to a foreign power.
 - c) Routine Intelligence reports.
- (d) Technical matter not of major importance but which has a distinct military value or requires protection otherwise, e.g., new weapons calculated to influence minor tactics or Service tests of war equipment of a standard pattern. A CONFIDENTIAL grading is justified if:
 - (i) the project is more than a routine modification or logical improvement of existing materials and is sufficiently advanced to result in substantial improvement in the performance of existing CONFIDENTIAL, weapons;
 - (ii) the project is sufficiently important potentially to make it desirable to postpone knowledge of its value reaching a foreign nation;
 - (iii) it is liable to compromise some other project already so graded.
 - (e) Certain personnel records and staff matters.
- (f) Certain compilations of data or items which individually may be classified RESTRICTED, or which may be unclassified, but the aggregation of which enhances their security value.

D. RESTRICTED

Information and material (matter), which requires special protection other than that determined to be TOP SECRET, SECRET or CONFIDENTIAL.

Illustrations

- (a) Departmental books of instruction and training and technical documents intended for official use only or not intended for release to the public.
- (b) Routine information relating to the supply and procurement of military stores.
- (c) Minor modifications and routine tests of equipment.
- (d) Certain compilations of data or items which individually may be unclassified but which in the aggregate warrant a classification.

Page 16

STRICTED

MAY, 1954

RESTRICTED

Note.—Documents, while not containing more actual information than has been published in the Press or otherwise issued by unofficial agencies, may confirm the accuracy or otherwise of such published material and/or give official views thereon. Where it is necessary to protect official confirmation or comment from unauthorised disclosure, such documents should be appropriately classified.

Unclassified Matter

2. Matter may be marked "Unclassified" if it is necessary to indicate that no security classification is required. However, all official information must be protected. The fact that information is not classified or is marked "Unclassified" does not eliminate the necessity for preventing its unauthorised disclosure. (The provisions of the Public Service Act and Regulations and of the Crimes Act and other Statutes mentioned in Chapter XII apply equally to all official information, whether classified or unclassified.)

Principles to be Applied in Classifying Matter

- 3. Classification of Documents. The following are the more important principles to be followed in classifying documents:—
 - (a) A document is to be classified as soon as possible during its preparation.
- (b) Each document is graded on its merits, that is to say it is graded according to the nature, source, and implications of the information contained therein. Factors such as the grading of other documents in the same series, or the grading of a classified file of which a document happens to be part, should not influence the grading of a document.
- (c) If it is practicable to indicate pages or passages within a document which merit varying classifications, this should be done. In such cases the overall classification of the document must be clearly shown at the beginning and must, of course, not be lower than the highest classified portion.
- (d) A document must not bear a lower classification than the highest classification of any of its appendices or attachments. Each attachment, etc., must be graded on its own individual merits.

MAY, 1954

(e) There is no need to allot to a subsequent document a classification as high as that of an earlier one which it quotes or refers to, provided the quotation is limited to the reference number, the date, and matter not in itself justifying a classification higher than that of the subsequent document.

A file containing classified documents is graded according to the highest classification of any documents be found desirable to break a file into two or more TOP SECRET (bright red), SECRET (salmon contained therein. For this reason, it may sometimes parts, one part to contain the higher category papers. Note.—Distinctive file covers should be provided for pink), and CONFIDENTIAL (green).

Re-classification of Documents

a) Classified documents should be kept under constant revision and "downgraded" to a lower category as the need for protection diminishes, or made unclassified when classification is no longer necessary.

the originating Documents must be re-classified only on the instruc-tions or with the permission of the originating authority, who should inform all recipients or holders of the particular documents of the new classification. In some cases it may be possible for the originating authority to indicate at the time of issue that a document may be downgraded after a given date. (p)

When a document is re-classified the old security classification should be deleted in ink and the new one substituted. The deletion should be signed and dated by the officer responsible and a note made of any documentary authority for it. 0

Cypher telegrams bearing the paraphrase warning (see Chapter VII, paragraph 2) should never be downgraded below RESTRICTED. (P)

The same general principles as apply to 5. Equipment. The same general principles and documents are to be followed in classifying equipment.

would be a document describing the equipment. However, the components of such equipment are to be (a) Equipment is to be graded in the same category as classified on their merits.

Page 18

RESTRICTED

MAY, 1954

RESTRICTED

- (b) The initial secrecy grading of equipment procured through the Departments of Supply and Defence Production is reviewed by a Technical Security Grading Committee. Unless it conflicts with other equipment gradings, the Committee normally adopts the classification placed upon the equipment by the sponsoring Department.
- not under contract for manufacture or supply with Departments are responsible for grading equipment or through the Departments of Supply and Defence Production. (c)
- Equipment of any apparent importance in the very early stages of design and development, i.e., before its ultimate military value is clearly determined, is to be treated as at least SECRET. (P)
- Classified equipment must be kept constantly under review by Departments and downgraded as soon as In certain circumstances, it may be necessary to upgrade equipment. Where applicable. Departments are to notify the Technical Securify Grading Committee immediately of any changes in security classification. circumstances permit. (e)

Responsibility for Classification and Re-classification

ment. Only a senior officer should be authorised to approve TOP SECRET and SECRET classifications. Officers should also be designated to approve the re-classification of matter originating In each Department, specified officers should be authorised to approve the classification of matter originating in the Departin the Department.

Over-classification

matter in the minds of personnel, encourages neglect for the rules Matter is to be assigned the lowest possible classification consistent with its being properly safeguarded. Over-classification In allotting a classification, the officer responsible should always must be avoided, since it depreciates the importance of classified of protection, and thus endangers the whole system of security. consider whether compromise of the matter would in fact cause the damage envisaged in the relevant definition.

RESTRICTED

Page 19

may enable documents to be given a lower classification than would The use of codewords and nicknames (see Chapter VI) otherwise be the case, or may eliminate the need for classification.

Classification Marking

- ferably by rubber stamp) with the appropriate classification at the top and bottom of each page, including the front cover and the Classified books, pamphlets, letters, memoranda, etc., and all copies thereof are to be plainly and conspicuously marked (pretitle page of books and pamphlets. The marking is to be placed so that it is clearly visible when pages are fastened together.
- a way that the classification is reproduced on any copies made therefrom. Negatives in roll form and films should be marked at graphs, films, etc., are to be marked in accordance with the above principles. Drawings, negatives, etc., should be marked in such Other classified documents such as drawings, maps, photothe beginning and end and containers should also be marked.
- means. In certain special cases where equipment cannot be kept from general observation, it may not be in the best interests of ing, etching, attaching a classification plate, or other appropriate Classified equipment is normally to be marked by stampsecurity to mark it.

Numbering

of distribution and enquiry in case of a breach of security. In particular cases of importance, this procedure should be extended SECRET matter is to bear a copy number to facilitate recording Any classified matter issued in a series should bear a serial number so that non-receipt of a particular item is noticed. to SECRET matter.

RESTRICTED

CHAPTER 111

DISSEMINATION OF CLASSIFIED MATTER

General - The "Need to Know" Principle

- necessary for the entire contents of a classified document to be the information. A balanced assessment of these conflicting claims is often a matter of some difficulty. The guiding principle is that information should be passed only to those officers to whom it is 1. Failure to impart information on a sufficiently wide basis may lead to lack of co-ordination and co-operation. On the other made available to an officer, he should be acquainted only with hand, too wide a circulation will tend to prejudice the security of necessary for the fulfilment of their duties (that is those who "need to know."). Officers are not entitled to have access to classified Where it is not matter solely by virtue of their status or office. those facts relevant to his duties.
 - rangements are necessary to ensure that this work is entrusted to matter in the course of their duties, certain other members of the staff such as registry clerks and typists will necessarily handle this matter in the normal course of administration. Special arauthorised persons under conditions which do not permit others to In addition to those officers who require to study classified view or have access to the matter.

TOP SECRET and SECRET Registries

in separate registries in segregated areas. TOP SECRET and SECRET registries are to be staffed by selected persons authorised TOP SECRET and SECRET matter must be maintained to handle such matter, and are not to be accessible to others.

Distribution of Classified Matter

- Each Department should authorise officers to be responsible for determining the distribution of classified matter.
- A record is to be maintained of all persons within a be made available only to persons specifically authorised to receive it and each TOP SECRET document or item is to be treated Department having access to a TOP SECRET document or item, TOP SECRET Distribution. TOP SECRET matter is to individually.

May, 1954

RESTRICTED

Page 21

all those outside a Department to whom a TOP SECRET document or item is transmitted, and all those to whom TOP SECRET information is disclosed.

6. Classified matter is to be made available to persons or bodies outside the Government Service only with the approval of the Permanent Head of the originating Department. The measures to be taken to safeguard such matter are outlined in Chapter XI below.

Reproduction of Classified Matter

7. Copies of classified matter are to be kept to a minimum, as the risk that the matter may fall into unauthorised hands increases in proportion to the number of copies in existence.

8. TOP SECRET matter is not to be reproduced in whole or in part except with the approval of the originating authority. This permission will not extend beyond a specified number of copies which are to be accorded the same treatment as the original.

9. The typing, roneoing, etc., of TOP SECRET and SECRET matter should be carried out under the supervision of an authorised officer in a segregated area. All materials and waste incidental to the reproduction of classified matter should be accounted for and safeguarded or destroyed in the manner prescribed in this booklet (see Chapter IV, paragraphs 5 and 20).

10. When TOP SECRET, SECRET and CONFIDENTIAL matter is reproduced by printing, the necessary safeguards must be provided at each stage.

Discussion of Official Business

11. Officers must guard against discussing matters of a classified nature, and indeed official business of any kind, in places where there is any possibility of being overheard by unauthorised persons.

Telephone Conversations

12. The insecurity of telephone conversations, and restrictions on the use of the telephone for transmitting classified information, are dealt with in Chapter V.

RESTRICTED

MAY, 1954

RESTRICTED

CHAPTER IV

CUSTODY OF CLASSIFIED MATTER

Storage of Classified Matter

Documents

- (a) TOP SECRET and SECRET documents are to be stored, when not in actual use or under guard, in vaults, safes or other equivalent containers fitted with dial type combination locks. Key type safes should not be used.
- (b) CONFIDENTIAL documents are to be stored, when not in actual use or under guard, in secure vaults, safes, safe-file cabinets or their equivalent, having secure locks (preferably dial type).
- (c) RESTRICTED documents are to be stored in a locked room or container equipped with a reasonably secure locking device, or are to be given equivalent protection.
- 2. Containers. The quality of containers required to afford the necessary protection will depend on a number of other security factors and it is therefore not possible to define specifications to cover every case. When determining the suitability of containers Departments should bear in mind the following factors, examples of the application of which are mentioned below:—

(a) Location

If the container is located in AUSTRALIA a lower standard can be accepted than would be the case if the container were to be located in a foreign country, e.g., in an Australian Embassy abroad.

Containers located in isolated, easily entered buildings must be of higher quality than those located in, say, the upper stories of buildings, the entry to which is restricted.

MAY, 1954

for use in foreign countries should not be locally purchased as such purchases may be subject to pre-delivery tampering. All these safes should be fitted with a 4-wheel indirect drive combination lock.

System of Guarding

Guarding can range from cases in which no guard is provided and the container is left unattended for periods of 48 hours or more (e.g., over the weekend) to conditions under which the container is subject to safes or strongrooms can have time clocks installed near them so that a check can be kept on guards regular inspection by armed guards. inspections.)

Burglar Alarm Systems (c)

However, for the storage of TOP SECRET matter the principle should be accepted that the highest Where these are installed in conjunction with armed guards lower standards of containers can be accepted. standard of container is necessary, since circumstances may arise in which the other protective systems become inoperative for a period.

(d) Protection against Unauthorised Removal

in an isolated building, steps should be taken to ensure that the container cannot be easily removed from the building. This may sometimes be done by using a larger and heavier container than would Particularly abroad or where a container is located normally be required, or by bricking and cementing a small container into position. When in doubt as to the suitability of a container, Departments may refer to the Director-General of the Australian Security Intelligence Organisation for technical advice.

Equipment

denied access to or view of it at all times. Access to (a) TOP SECRET and SECRET equipment is to be so stored and protected that unauthorised persons are areas and buildings containing such equipment is to be controlled.

Page 24

RESTRICTED

RESTRICTED

- (b) CONFIDENTIAL and RESTRICTED equipment is to be so stored and protected that access to it is denied to unauthorised persons.
- Separate instructions for the storage of cryptographic equipment are issued to the Departments concerned. (0)
- classified equipment is stored or is in operational use The custody of classified equipment is to accord with the principles outlined above, but precautions will vary according to the nature of the equipment, the storage facilities available, and the position of the equipment during operational use. In establishments where a security officer should be designated to ensure that all necessary measures for safeguarding the equipment are taken.
- sheets passed through duplicating machines, and all materials and biotting paper, stencils, newly used typewriter ribbons, waste being used for preparing or reproducing classified matter, must be Shorthand notebooks, carbon treated as classified matter themselves, until they are to be destroyed as classified waste (see paragraph 20 below). Shorthand Notebooks, etc.
- an examination. When not in actual use or under guard, containers should be stored in the same way as the matter they are used to 6. Containers used to transmit Classified Matter. The security of containers used to transmit classified matter is to be unauthorised person has had any opportunity of examining the regarded as compromised when a key is lost and also when an lock, since an expert is able to produce a suitable key after such transmit.

Access to Storage Containers

possess the combination or keys to storage space or have access to the material stored therein. Containers are to be kept locked Only a minimum number of authorised persons should when not under the direct supervision of a person officially entrusted with the combination, keys or the contents.

Combinations of Safes

Combinations of safes are to be classified as high as the highest security classification of the matter protected, and safeguarded accordingly. Combinations are to be changed at least

MAY, 1954

RESTRICTED

May, 1954

every three months and at other times as considered necessary (as when a person knowing the combination severs his connection with the office concerned).

The custody of keys is dealt with in Chapter VIII.

Protection of Classified Matter in Actual Use

persons are present. If a room containing classified matter has to be left unoccupied for a few minutes during working hours the door must be locked; at all other times classified matter must be Those using classified matter must take every precaution to prevent deliberate or casual inspection of it by unauthorised persons. Papers should never be left lying open when unauthorised stored as prescribed above.

Office and Area Inspection

11. Office or area inspection should be made daily after working hours to ensure that no classified matter is left unprotected, and that all safes, filing cabinets, windows, doors, gates, etc., are locked.

Receipts for Custody

is to be covered by a receipt system. Departments are responsible for ensuring that a receipt system applies in special cases where receipts are required for the custody of classified matter other than The custody of TOP SECRET matter within Departments TOP SECRET

Accounting for Classified Matter Held

and a check should be carried out periodically in order to bring to light any deficiencies. A record must also be maintained of A record of TOP SECRET matter held must be maintained classified matter which, on the instructions of the originator, must be accounted for periodically to the originator.

Removal of Classified Matter from a Department

Classified matter should not normally be taken out of a Department unless it is required for official reference elsewhere, e.g., at a conference. TOP SECRET matter must never under any circumstances be taken home.

Page 26

RESTRICTED

MAY, 1954

RESTRICTED

15. Before taking TOP SECRET, SECRET and CONFIDEN-TIAL matter out of a Department, the approval of a responsible return of all classified matter taken away overnight is also to be senior officer is to be obtained. A record of the removal and kept by the appropriate registry.

The officers removing and approving the removal of classified matter from a Department, are responsible for ensuring that it is adequately protected at all stages. When not actually in use it should be kept in a locked container and guarded by the officer concerned, unless it can be kept in an approved safe.

Destruction of Classified Documents and Equipment

ments for pulping are to be torn in small pieces and the supervising officer must watch the process of pulping until an advanced stage half-burnt fragments can be carried away by the draught of the fire and must see that the ashes are reduced to powder. Docu-The only satisfactory methods of destruction of classified documents are by fire or pulping. When destruction is authorised, documents are to be burnt or pulped under supervision of an authorised officer. This officer must ensure that no unburnt or has been reached.

and/or identification impossible, and is to be carried out under supervision of an authorised officer. The method of destruction 18. When it is necessary to dispose of classified equipment, destruction is to be in such a manner as to make reconstruction will vary according to the nature of the equipment concerned. Necessary destruction may be limited to those portions of the equipment which incorporate, the classified features.

A record is to be retained and appropriately certified of the destruction of classified documents and equipment.

Destruction of Office Waste

the systematic collection, custody, and destruction in accordance with the methods outlined above, of all office waste of a classified Department must ensure that satisfactory arrangements exist for The careless disposal of waste matter constitutes one of the most dangerous sources of leakage of information.

CHAPTER V

TRANSMISSION OF CLASSIFIED MATTER

Envelopes

1. TOP SECRET, SECRET and CONFIDENTIAL matter is to be enclosed in two opaque envelopes. The inner envelope is to show the classification and full address and is to be sealed with wax or wafers so as to prevent or reveal tampering (the correct method of sealing and some recommendations of wafers are shown in Appendix A). The outer envelope is to be fully addressed but must not show the security classification. The address of the sender should be shown on the outer envelope. RESTRICTED matter may be enclosed in one envelope provided this does not disclose the classification. Where matter is for delivery by "Safe Hand" (see paragraph 8 below) the outer envelope should be inscribed accordingly in bold letters, and bear a number for identification purposes.

does not come in direct contact with the inner cover. The size of the envelope should be approximate to the size of the contents so that the envelope and its fastenings do not suffer strain and to minimize the risk of any of its contents being extracted.

3. The outer envelope of TOP SECRET matter should be addressed to a Department in the normal manner. Opening instructions should be shown on the inner envelope which should, if necessary, be addressed to the individual for whom it is intended. TOP SECRET and SECRET matter is to be opened only by the addressee or a representative who is authorised to open such matter.

4. Where the originating Department cannot effect delivery to the office of the addressee, and use is made of another Department or Statutory Authority as the transmitting agent, an inner envelope and an outer envelope should be used for all classified matter, the inner envelope showing:—

(a) the full address of the addressee, together with name or appointment;

(b) the originating Department;

MAY, 1954

(c) a reference number for identification purposes;

(d) the appropriate security grading.

The outer envelope should bear no indication of the security classification and should be addressed to the appropriate authority at the transmitting Department, who will remove the outer envelope and forward the inner envelope in accordance with the practice of his Department to the addressee.

Carriage within a Department

5. For internal circulation within a Department located in one area, TOP SECRET matter should be passed by hand of responsible officers. If this is not practicable, TOP SECRET matter may be delivered by authorised messenger personally to the recipient or his authorised representative, in a locked container or enclosed in two envelopes as prescribed in paragraphs 1 to 3 above. SECRET matter may be enclosed in a single envelope DENTIAL matter may be enclosed in a single envelope DENTIAL matter may be sent in a single envelope marked "SECRET" provided this is sent direct by hand. CONFI-TONFILMENTIAL: RESTRICTED matter may be sent in a single envelope marked without a cover, as considered advisable.

Carriage Outside a Department or Area

Despatch and Carriage Within Australia

(a) TOP SECRET matter, also classified code and cypher books and appliances, must never be despatched by civil post, but by "Safe Hand" (see paragraph 8 below).

(b) SECRET matter should be despatched by "Safe Hand". If this service is not available the only alternative means of despatch to be used is registered mail.

(c) Postal registration of CONFIDENTIAL matter is discretionary for the originating Department. (However, CONFIDENTIAL equipment is to be sent by registered mail.) RESTRICTED matter may be sent by ordinary mail.

CONFIDENTIAL and RESTRICTED matter may be carried by authorised messenger between buildings in the same town. Envelopes should not be carried loose but should be enclosed in securely fastenel containers. If a van is used it must be locked whenever it is left unattended.

RESTRICTED

MAY, 1954

RESTRICTED

7. Carriage Outside Justralia. All classified matter should be forwarded by "Safe Hand", with the following exception. CONFIDENTIAL matter may be sent by registered mail and RESTRICTED matter by ordinary mail to a destination within British territory, provided that, if carried by air, the route does not traverse or touch non-British territory.

"Safe Hand" Transmission

8. Transmission of matter by "Safe Hand" means that it is despatched to the addressee in the personal care of an authorised officer or succession of authorised officers who are personally responsible for its carriage and safekeeping. At each handover, a receipt must be obtained showing identification number of the package, time, date, etc. The following methods are used:—

(A) Carriage Entirely Within Australia:

(i) By hand of a responsible officer or succession of officers appointed to deliver the matter to the addressee.

(ii) Care of the Captain of an aircraft of an Australian Airline Company which has been authorised to carry,"Safe Hand" matter.

(B) Carriage Outside Australia:

(a) Between points within British Territory (including Australia) and, if carried by air, on a route which does not traverse or touch non-British territory.

 By hand of a responsible officer or succession of officers appointed to deliver the matter to the addressee.

By diplomatic bag through the Department of

External Affairs.

(iii) Care of the Captain of an Aircraft of a British Airline Company which has been authorised to carry "Safe Hand" matter. Departments should refer, in the first instance, to the Department of External Affairs in connection with arrangements for the use of this method.

(iv) Care of the Master of a British vessel; the matter is placed in the personal care of the Master. Departments should make arrangements for transmission by this method through the Department of the Navy which has facilities for the despatch of all classified matter by sea route.

MAY, 1954

- (b) To or from a point in a Foreign Country, or by an air route which traverses or touches non-British territory.
- (i) By hand of a responsible officer who is in possession of a diplomatic passport.
- By diplomatic bag through the Department of External Affairs. (ii)
- (iii) Care of the Master of a British vessel; the matter is placed in the personal care of the Master. Departments should make arrangements for transmission by this method through the Department of the Navy.

Carriage by Officers Travelling Overseas

seas should be sent ahead by the means prescribed in paragraphs Classified matter required by an officer travelling over-8 (B) (a) and (b) above.

Receipts for Transmission

- The transmission of TOP SECRET and SECRET matter is to be covered by a receipt system. The addressee or his authorised representative is to sign and check the accuracy of the receipt and the sender is to check its return.
- Departments may decide whether in any instances re-ceipts are to be obtained for other classified matter.

Transmission by Telephone

"translate" snatches of "scrambled" conversation. Privacy equipment should therefore be regarded only as a device that will, in by deliberate interception. The privacy equipment (previously known as the "secraphone" or "scrambler") at present in use in is possible. Deliberate interception is also possible to an expert with suitable equipment, and it may be possible for a trained ear to No form of telephone conversation — even on a direct line connection, etc., the possibility of telephone operators and engineers overhearing conversations in the performance of their duty, or some Government Departments, does not afford a high degree of security and is not a "secret" telephone system. Cross-connection of lines over which privacy telephone conversations are in progress The risk of leakage may arise from casual interception by crossor between two extensions from the same switchboard-is secure. most instances, defeat casual eavesdropping.

Page 32

May, 1954

RESTRICTED

privacy telephone only when the need for speed outweighs the need to guard against leakage. There is less objection to the 13. TOP SECRET information must never be transmitted by open or privacy telephone. SECRET information must never be transmission by telephone of CONFIDENTIAL and RESTRICTED information, but, even so, every effort should be made to render the conversation as obscure as possible to eavesdroppers. As a general rule CONFIDENTIAL information should not be transconveyed over the open telephone, and should be transmitted by mitted over open telephone lines.

Vote.-The foregoing is for guidance. Users of speech privacy equipment must in all cases observe current detailed instructions issued with or in connection with such equip-

14. Care must be taken when referring to a cypher telegram, not to give any indication which might lead to a compromise of

Printing Telegraphy (Teleprinter)

the cypher used (see Chapter VII).

mission by these means. In this connection, a message bearing a paraphrase warning should be paraphrased before re-transmission even in cypher. If paraphrase is not possible the re-transmission must be in one time or Category A System and the cypher staff must be warned that the text is an unparaphrased version of a Printing telegraphy (e.g., teleprinter) circuits cannot be regarded as a secure means of transmission. All messages classified CONFIDENTIAL or above should be encrypted for trans-Category B message (see Chapter VII).

Telegram, Cable or Wireless

Classified information must not be despatched by telegram, cable or wireless in plain language.

Transmission of Classified Equipment

The measures to be taken to safeguard classified equipment in transit are set out in Appendix B.

CODEWORDS AND NICKNAMES

Codewords

- 1. A Codeword is used to provide security cover in referring to some particular classified matter or project. Examples of the the use of a codeword include:—
- (a) Providing a name for plans, projects and operations;
 - (b) Concealing intentions in documents, communications and discussions pertaining to plans, projects and operations;
- (c) Designating geographical locations in conjunction with (a) and (b) above.
 - Codewords are invariably to consist of one word only.
- 3. Advice on the allocation and use of codewords is given in directives issued by the Joint Intelligence Committee, Department of Defence, Melbourne. Requests for codewords are to be made through Departments to the Joint Secretaries of that Committee. Such requests should distinguish between words required for designating geographical locations and those required for other security purposes.
- 4. The use of words as codewords, other than those obtained from the Joint Intelligence Committee, is not authorised.

Department of Supply

5. A special procedure applies to the Department of Supply, which, in addition to codewords for operational purposes, uses codenames for all their ideas and/or projects and/or equipment.

Nicknames

- A nickname is a name used for administrative convenience in referring to some particular matter in which security cover is not required. It may be used as and when convenient for unclassified and RESTRICTED matter only. The user is responsible for selecting a nickname and for informing all concerned of its meaning.
- To avoid any confusion with a codeword or with Department of Supply codenames, nicknames must always consist of two separate words. Care should be taken that the two words are kept distinct and that they do not consist of pairs of words normally associated with each other (e.g., CROSS ROADS).

Max, 1954 (amendment No. 1 March, 1956)

RESTRICTED

CHAPTER VII

CYPHER SECURITY

Cypher Categories

The cyphers used by the British Commonwealth fall into two categories:

Those for which it is unnecessary to paraphrase Category A.

tion to persons outside the Government Services of British Commonwealth countries. This category the verbatim text before publication or distribuincludes all one-time cyphers and some non-onetime cyphers.

phrasing precaution is necessary in the event of Certain non-one-time cyphers for which the parapublication or outside distribution, because the accurate fitting of the verbatim text to the cryptogram would endanger the cypher key. Category B.

The majority of cyphers now used are Category A systems.

Telegrams Requiring' Safeguarding of the Verbatim Text

headed with a warning to the effect: "This message must be paraphrased if it is to be communi-Occasionally the copy of a telegram will be round to be

cated to persons outside British Government Departments."

This indicates that a Category B cypher has been used. It will be rare for such a telegram to be of current date but it is not infrequently to be found in the case of telegrams dated prior to September, 1950.

Publication of Texts of Cypher Telegrams

published or communicated in any way to anyone not in the Government Service of a British Commonwealth country or the United States Government Service, the following rules must be Whenever it is necessary for the text of a Category B cypher telegram (i.e., one bearing the paraphrase warning) to be observed unless the telegram is dated earlier than January. 1944:-

(i) The telegram must be thoroughly paraphrased; the entire make-up of the message must be

No mention must be made of the fact that the telegram was a cypher telegram.

The Date-Time Group, the Time of Origin, the Fime of Handing In, or any other identification transmitted en clair must not be quoted. Even the encrypted serial number should not be quoted if this is unnecessary.

Encrypted addresses and delivery instructions must, wherever possible, be omitted. (iv)

External addresses and signatures which were transmitted with, but not encrypted in the same system as, the text of the telegram must be expressed in normal plain language and not in the form as transmitted. ()

Reason for Special Precautions

mitted in a Category B cypher (which may have been obtained by wireless interception) together with the clear text of the same message would constitute a grave danger to the security of the authorised persons of the encyphered version of a message transsystem concerned. The effects could be far-reaching, affecting both future and past traffic and even affecting the security of other The reason for the above rules is that possession by un-Category B cypher systems.

Co-operation by Originators

the possibility of publication. Where publication is likely the message should be marked "FOR TRANSMISSION IN OTP" (One Originators of classified messages should bear in mind Fime Process) or "CATEGORY A CYPHER" according to instructions issued in their Departments; the need for paraphrasing before publication could then, in nearly all cases, be eliminated.

In no circumstances may originators dictate the text or portions of the text of classified messages by telephone, even if nor may messages already transmitted in a Category B system (i.e., the telephone is fitted with speech privacy equipment (Secraphone). with the paraphrase warning on the distribution copy) be confirmed by telephone.

RESTRICTED

MAY, 1954

RESTRICTED

Cypher Security Committee

Committee is responsible for recommending further special instructions on the subject of cypher security which are brought to the notice of those concerned. Committee which is part of the Higher Defence Machinery. The Cypher security is dealt with through the Cypher Security

CHAPTER VIII

SECURITY OF BUILDINGS AND AREAS CONTAINING CLASSIFIED MATTER

Responsibility for Building and Area Security

Each Department is responsible for ensuring that the building(s) and area(s) or portion thereof which it occupies are adequately safeguarded both during and after office hours.

Access to Buildings and Areas

- 2. All possible means of access to buildings should be examined and, if necessary, locks should be strengthened, bars fitted to ground floor windows, etc.
- provision of patrols or guards, etc., will vary according to the site and the nature of the matter to be protected. 3. Buildings and areas or portions thereof containing TOP SECRET and SECRET matter should, where practicable, have one entrance only, controlled during working hours by a Peace Officer or other authorised officer. Access can be further controlled by segregating sections within a security area. Precautions to be taken after working hours, e.g., installation of burglar alarms,

Passes

- In some cases a pass system is essential to security, but the fact that passes have been issued does not automatically ensure security. The issue of passes is advisable in a large Department or a large building housing several Departments, or in an area where access is granted only to certain officers of a Department.
- bered and to provide the ideal protection (which may not always be necessary or practicable) they should bear the following in-5. Each officer receiving a pass should sign for it in a register in the presence of the Departmental Security Officer or the uppropriate administrative officer. Passes should be serially numformation:-

 - (a) photograph and description of holder;(b) signature of holder and issuing officer;
- c) an embossed seal over the two signatures;

RESTRICTED

(d) conditions of issue;

(e) instructions to a finder.

Passes need not necessarily indicate the issuing Department and must not state the buildings or areas to which they give access, except in code. Passes should be checked periodically. The loss of a pass must be reported immediately.

and should either be replaced by a set in a different colour or revalidated by a stamp that cannot easily be forged. It is advisable for a new set of passes always to be held in reserve in case All sets of passes are liable to become compromised in time of emergency.

Whether or not a pass system operates, officers should be required to sign a register upon entering and leaving a building written advice should be lodged with guard posts, and guards should be instructed not to admit employees during silent hours, unless the appropriate authority has been received. outside working hours. Where overtime is to be worked, prior

Where control of entry is necessary either by a pass system or by recognition, written instructions regarding visitors. To be effective. measures for the control of visitors should include the following:workmen, etc., should be given to doorkeepers.

(a) A register should be signed by all visitors and should show times of arrival and departure, name, business, the Department or firm from which the visitor comes. The Departmental Security Officer should peruse this register periodiand the officer to be visited.

Visitors should be issued with a form or badge authorising entry and this should be collected by the doorkeeper at the exit. If a form is used it should be signed by the officer interviewed upon completion of the visit. (p)

particularly, the doorkeeper should telephone the officer to be visited and should see that the visitor is In TOP SECRET, SECRET and prohibited areas escorted to his office. The officer interviewed is responsible for providing the visitor with escort out of 3

Page 42

RESTRICTED

May, 1954

RESTRICTED

(d) It may not be necessary to observe all the above procedure in the case of designated senior official visitors, but a record of the visits should be kept.

Officers should see that papers are protected from view and that visitors are not left unattended in rooms Care should be taken to prevent visitors from seeing classified matter which does not concern containing classified matter. (e)

Where necessary, bags, cases, parcels, etc., carried by visitors should be subject to control.

Visits by Press, Radio and Other Accredited Representatives

other accredited representatives to factories or annexes where classified equipment is being produced, the following security If permission is granted for visits by press, radio and principles are to be observed.

a) Classified matter which is not to be viewed must be segregated and protected from observation.

(b) An undertaking of secrecy is to be signed.

Script and photographs relating to classified equipment and projects are to be submitted for approval before release to press and radio representatives.

(d) A security officer should accompany representatives throughout the visit.

Control of Photography

11. Security regulations in regard to the use of cameras will vary with the security classification of a project or establishment tions should ensure that there is no danger of classified matter being unofficially photographed, and where necessary a register of cameras should be maintained and films submitted to the security or of certain sections of an establishment. Local security instrucofficer for clearance before printing.

Custody of Keys

Measures for safeguarding keys require constant attention Such measures to prevent insecure practices from developing. are to include the following:-

is to be periodically checked, at least quarterly. In addition, it is recommended that there should be an (a) All keys are to be recorded in a central register which

MAY, 1954

RESTRICTED

occasional check of all keys without warning, to ensure that the regulations for custody are being observed.

- (b) Only in exceptional circumstances should keys be removed from official premises. When it is necessary to remove a key, it should be securely attached by a chain to the clothing of the officer concerned and should never leave his person. (It must be remembered that to take an impression of a key is a very easy matter.) Such keys should not be marked or labelled.
- (c) Both during and after office hours, keys, including the keys of unlocked rooms, cupboards, drawers, etc., should either be in charge of a responsible officer or should be placed in a locked box which is stored in a safe place, preferably a combination safe. Where a building is under continuous armed guard the locked box should be placed in the care of the guard. Keys should not be left where they can be seen by anyone passing. (Highly skilled locksmiths can, after a glance at a key, often produce a duplicate that will, with very little adjustment, operate the lock.) The practice of keeping keys on nails in locked or unlocked drawers or other similar places must be prohibited.
- (d) Duplicate keys should be placed in a sealed container and kept in a combination safe.
- (e) It should be impressed upon all officers that duplicate keys may not be cut without permission of a responsible senior authority.
- 13. The loss of a key must be reported immediately. Action to be taken in the event of such a loss is outlined in Chapter IX. It should be noted, however, that even when a lost key is recovered the security of the lock may be compromised, depending on the circumstances surrounding the loss.

Instructions to Guards, Sentries, etc.

14. The duties of guards, sentries, watchmen, etc., should be clearly detailed in Departmental security regulations. A copy of the relevant parts of these regulations should be handed over by

Page 44

RESTRICTED

May, 1954

RESTRICTED

guards, etc., to their reliefs, but should not be available for scrutiny by unauthorised persons. In addition, guards, sentries, etc., should be fully instructed in their powers of apprehension and detention of persons who attempt to gain unauthorised admission.

MAY, 1954

CHAPTER 1X

ACTION IN CASES OF BREACH OF SECURITY

General

- 1. No practicable system of security can afford complete protection against the skilled agent and no system is proof against foolishness or negligence. However, an efficient system will, with the least possible delay, draw attention to any breach of security which may occur, and will narrow the field of enquiry.
- The success of investigations depends primarily on the time factor, and every officer should instantly report to the Departmental Security Officer any loss or any other possible case in which security may have been compromised. Investigation should be commenced immediately and any assistance required should be sought as early as possible.
- 3. In dealing with a breach of security the main objectives are—
- (a) to find out what happened;
- (b) to minimise the damage done;
- (c) to prevent a recurrence.

Responsibility for Action

- 4. The Department in which a breach of security occurs is responsible for undertaking the necessary investigation, if it originated the matter involved. If not, the breach is to be reported to the originating Department and the investigation will be undertaken either by the Department in which the breach occurred or the originating Department, as agreed upon.
- 5. While the primary responsibility for action rests with the Department or Departments concerned, the advice of the Australian Security Intelligence Organisation may, and in some cases should, be sought. In such cases the Australian Security Intelligence Organisation will indicate whether it wishes to take part in the investigation.

MAY, 1954

RESTRICTED

Losses and Leakages

6. For the purposes of this chapter breaches of security are divided into two classes—

- (a) loss where classified matter is missing;
- (b) leakage where classified matter has come to the knowledge of unauthorised persons.

Losses

7. The Departmental Security Officer should first ascertain the basic facts of the loss and, in consultation with the branch concerned, should assess its importance. If initial enquiries show that the loss is not simply due to carelessness or is not otherwise readily explicable, and that therefore there may be some improper motive behind it, the Australian Security Intelligence Organisation should at once be informed so that it may determine whether there is a case for suspecting espionage.

8. The loss of a key may have more widespread effects than the loss of a document. Even when a key is recovered, the lock must be regarded as compromised, unless it is established beyond reasonable doubt that there has been no opportunity for an unauthorised person to copy the key. Since the replacement of a lock may be costly and difficult, Departments should decide whether, having regard to all the circumstances surrounding the loss of a key, it is necessary to change the lock. However a lock must be changed if—

- (a) the key has been lost in circumstances which suggest malicious intent;
- (b) several keys to the one lock have been lost, even if there are no suspicious circumstances surrounding

Leakages

9. The Departmental Security Officer should first determine, in consultation with the branch concerned, whether in fact there has been a leakage. (For instance, a newspaper report may be merely an accurate guess based on information already published.) If a leakage has occurred and initial enquiries by the Departmental Security Officer have not provided some ready explanation, the matter should be promptly reported to the Australian Security Intelligence Organisation before further action is taken.

Page 48

RESTRICTED

MAY, 1954

RESTRICTED

- 10. The Departmental Security Officer should then-
- (a) establish the distribution of documents involved in the
- b) ascertain whether any copies are missing;
- (c) inform the Australian Security Intelligence Organisation of details of (a) and (b), and also provide full names, date and place of birth, home address, and nationality of every person on the distribution list.
- 11. In some circumstances it may be desirable to obtain information by means of a written questionnaire.
- 12. Leakages by word of mouth, either deliberately or in careless talk, are the most difficult to prevent or trace, but the possibility that they may occur should always be borne in mind.

Minimising Damage

13. The Departmental Security Officer should see that those concerned are aware of the need to take all possible steps to limit the consequences of a breach of security. The measures that can be taken depend on the nature and content of the matter compromised. For example, cyphers and codes can be changed, and plans for particular operations, whether military or civil, may be capable of alteration.

Preventing Recurrence

14. Each incident may point to a weakness in security arrangements, or to failure by an individual to observe them. In every case the means by which security may be improved should be considered, or the lesson should be brought home to the individual responsible, even if no disciplinary action is necessary.

Possibility of Prosecution

15. A breach of security may constitute an offence against the Commonwealth Public Service Act and Regulations, the Crimes or Defence Acts or one of the relevant statutes mentioned in Chapter XII below, and the question of prosecution may have to be considered. Departmental enquiries must not be carried so far as to prejudice a prosecution, and when preliminary investigation indicates a possible breach of the Acts, Departments should consult the Commonwealth Crown Solicitor.

May, 1954

STAFF ENGAGED ON CLASSIFIED WORK

Responsibility of Departments

prevent the employment on classified work of any person who is 1. Departments are responsible for determining the branches, annexes, installations, etc., which are to be regarded as classified, and for administering the precautions which must be taken to adversely regarded from a security viewpoint.

Security Clearance

- be engaged on classified work. A security clearance given by the Australian Security Intelligence Organisation means that at the date of the check no adverse information is held such as would render a person a security risk for the position which he or she holds or for which an application has been made; a clearance is The Australian Security Intelligence Organisation assists Departments by assessing the suitability from a security viewpoint of existing employees or applicants for employment engaged or to thus not a testimonial to a person's security standing.
- Personnel should not be employed or led to expect employment on classified work before being security cleared.
 - showing the date and those specially cleared for access to TOP SECRET information. It will thus be possible to ensure that staff are not employed on duties for which they have not been security cleared. On transfer to another Department, the clearance or Departmental Security Officers should maintain lists of persons who have been security cleared or denied a clearance, non-clearance should be notified as necessary.

Supervision of Staff

vising officer should get to know his subordinates and not confine himself merely to observing how they discharge their official duties. This is particularly important in the case of staff engaged on TOP SECRET or SECRET work. Should the behaviour of The supervision of staff engaged on classified work differs only in degree from the supervision of other staff. Every super-

any individual give rise to concern from the security aspect, the matter should be brought to the notice of the Australian Security Intelligence Organisation at once.

Application of Acts and Regulations Dealing with Official Secrecy

and upon leaving the Government Service should sign a further acknowledgment that their responsibility in this regard is a con-Public Service are dealt with in Chapter XII. Personnel who are to have access to TOP SECRET matter should be required to sign The provisions of Acts and Regulations dealing with official secrecy and their application to members of the Commonwealth a declaration acknowledging their responsibility under these Acts, tinuing one.

Persons Outside the Government Service

7. Measures regarding persons outside the Government Service who are to be entrusted with classified matter are dealt with in Chapter XI.

RESTRICTED

CHAPTER XI

CLASSIFIED MATTER ENTRUSTED TO PERSONS OUTSIDE THE GOVERNMENT SERVICE

Approval by Permanent Head

Classified matter is to be made available to persons or organisations outside the Government Service only with the approval of the Permanent Head of the originating Department.

Security Clearance

responsible for taking the necessary precautions to prevent the employment on classified work of outside personnel adversely regarded from a security viewpoint. The following procedure is As in the case of Departmental staff. Departments are desirable:-

contractors, etc. - the names of those whom it is (a) Where it is necessary for Departments to entrust classified matter outside the Government Service for example to consultants, universities, industries, proposed to approach initially should be submitted to the Australian Security Intelligence Organisation

tion of the classified matter in question. All persons approach the most senior person concerned and in consultation with him determine the extent of circulawho are to be entrusted with such matter should be Upon receipt of a glearance. Departments should the subject of a security assessment. for security assessment. (P)

proposed to include on Governmental committees, etc., Persons outside the Government Service whom it is dealing with classified matter should be similarly treated prior to appointment. (0)

Departments should maintain a list of outside persons similar to the record of Departmental personnel who have been security cleared or denied a clearance, (Chapter X. paragraph 4). (p)

May, 1954

RESTRICTED

MAY, 1954

Application of Acts dealing with Official Secrecy

3. Application of the Acts dealing with official secrecy to persons outside the Government Service is dealt with in Chapter XII. Their responsibilities under these Acts should be brought to the notice of all such persons who are to be entrusted with classified matter, and an appropriate acknowledgment should be signed by those dealing with TOP SECRET matter.

General Security Arrangements

Before classified matter is actually handed over to outside persons or organisations, Departments are responsible for ensuring that their attention is drawn to the special precautions to be taken in connection with dissemination, custody and transmission, and that their security arrangements conform as nearly as possible to those of Departments. Particular emphasis should be laid on the importance of circulating classified matter only to those who need it for the efficient performance of their work, of acquainting individuals only with those facts which concern them, and of concealing the significance of matter wherever possible.

Government Contracts

for the manufacture or supply of classified matter which are administered by the Departments of Supply and Defence Produc-Appropriate security provisions are included in contracts tion. Similar regulations should be enforced by other Departments procuring classified matter from private contractors.

RESTRICTED

CHAPTER XII

ACTS AND REGULATIONS DEALING WITH OFFICIAL SECRECY

Introduction

the Crimes Act 1914-1946, which deals generally with offences against the Commonwealth, and also certain other Acts mentioned These provisions apply whator not is irrelevant. Any act or disclosure contrary to the provisions for official secrecy, as enacted and prescribed, is an offence below, contain provisions for the prevention of the unauthorised ever the subject matter of the information; whether it is important The Commonwealth Public Service Act and Regulations, disclosure of official information. against the law.

The Commonwealth Public Service Act and Regulations

- provides that regulations may be made for giving effect to the Act. In particular there is power for the making of regulations relation to the matters coming to their knowledge in the course of their employment, and for prescribing the form of such oaths or affirmations" and also "for regulating the duties and conduct of The Commonwealth Public Service Act, which applies to "for requiring officers to take oaths or affirmations of secrecy in persons employed in the Public Service of the Commonwealth, officers".
- information obtained by an officer through his connexion with the Commonwealth Public Service, and the unauthorised disclosure of the contents of official papers or of any information concerning public business or official matters. These provisions are made by The Commonwealth Public Service Regulations expressly forbid the use, other than for the discharge of official duties, of Regulations 34 and 35, as follows:-
- "34. An officer shall not—
- his official duties, information gained by or conveyed to him through his connexion with the Service; or (a) use for any purpose, other than for the discharge of

MAY, 1954

May, 1954

RESTRICTED

RESTRICTED

(b) publicly comment upon any administrative action or upon the administration of any Department: Provided that nothing in this paragraph shall pre-

vent an officer resident in any Territory within the Commonwealth from publicly commenting upon civic affairs relating to that Territory.

cerning public business or any matter of which an officer directly, nor shall the contents of official papers be disclosed, by an officer without the express authority of the Except in the course of official duty, no information conhas knowledge officially shall be given, directly or in-Chief Officer."

The Crimes Act, Part VI - Offences by and against Public Officers

This Part of the Crimes Act includes Section 70 which wealth, or in or in connection with the Naval, Military, or Air Forces of the Commonwealth, or in the service of any public applies directly to every "Comonwealth Officer", an expression which by Section 3 is defined to mean any person holding office under the Commonwealth, and includes any person permanently or temporarily employed in the Public Service of the Commonauthority under the Commonwealth and includes an officer of the Commonwealth Bank.

Commonwealth Officer, publishes or communicates any fact which comes to his knowledge by virtue of his office, and which it is his duty to keep secret, or any document which comes to his possession Section 70 reads as follows: "Any person who, being a by virtue of his office, and which it is his duty to keep secret, except to some person to whom he is authorised to publish or communicate it, shall be guilty of an offence. Penalty: Imprisonment for two years."

The Crimes Act, Part VII - Breach of Official Security

Commonwealth or any part of the Queen's Dominions" then that person shall be guilty of an indictable offence, the penalty for person for any purpose prejudicial to the safety or interest of the Section 78 of this Part of the Crimes Act is of general which is imprisonment for seven years. In view of its general application, and provides that if specified acts are done by nature Section 78 is not here considered in detail.

RESTRICTED

RESTRICTED

this Section applies in particular to any person who "holds or has held office under the Queen or the Commonwealth", or who "holds or has held a contract made with or by or on behalf of the Queen or son who holds or has held such an office or contract". In view of this Section 79 of Part VII also is of general application but the Commonwealth" or who "is or has been employed under a perparticular application of Section 79 it may well be examined, as follows:-

Section 79 applies where any person has in his possession or control any sketch, plan, photograph, model, article, note, document or information: (i) which relates to or is used in a prohibited place or anything in such a place, or which has been made or obtained in contravention of Part VII of the Act, or

which has been entrusted in confidence to him by any person holding office under the Queen or the Commonwealth, or

Queen or the Commonwealth, or as a person who or on behalf of the Queen or the Commonwealth, or as a person who is or has been employed under which he has obtained owing to his position as a person who holds or has held office under the holds or has held a contract made with or by a person who holds or has held such an office or (iv)

offence, the penalty for which is imprisonment for In those circumstances the person is guilty of

seven years, if that person:-

model, article, note, document or information to any person, other than a person to whom he is authorised to communicate it, or a person to whom it is, in the interest of the Commonwealth or of some part of the Queen's Dominions, his duty (i) communicates the sketch, plan, photograph, to communicate it, or

retains the sketch, plan, photograph, model, article, note, or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it.

MAY, 1954

- plan, photograph, model, article, note, document or information, knowing or having reasonable cause to believe, at the time when he receives it, that the communication to him is in contravention of Part VII of the Act, unless he proves that the communication to him was contrary to his desire. In this case It is an offence also if any person receives any sketch, also the penalty is imprisonment for seven years. (c)
 - Prohibited places are defined by Section 80 of Part VII. The definition includes any place belonging to the Queen or the Commonwealth used for the purpose of building, repairing, making, or storing any ship, arms, or materials or instruments of use in time of war, or any plans or documents relating thereto. (p)
 - wealth and the Government thereof; "document" in-cludes part of a document; "model" includes design, wealth" includes the Government thereof, and includes graph or any other mode of representing any place or thing. Expressions referring to communicating or itself, or the substance, effect, or description thereof only, be communicated or received. Expressions resketch, plan, model, article, note, or document, include Section 77 sets out definitions which apply to Part VII of the Act. It is provided that "the Commonany Territory under the control of the Commonpattern, and specimen; "sketch" includes any photoreceiving include any communicating or receiving, ferring to obtaining or retaining any sketch, plan, model, article, note, or document, include the copying or causing to be copied the whole or any part of any pressions referring to the communication of any whether in whole or in part, and whether the sketch, plan, model, article, note. document or information the transfer or transmission of the sketch, plan, model, sketch, plan, model, article, note, or document. article, note, or document. (e)

It will therefore be seen that:-

(a) Any person holding office under the Queen or the Commonwealth will be guilty of an offence under Section 79 if any article or document or information which he has obtained owing to his official position

RESTRICTED

Max, 1954

RESTRICTED

document (as distinct from oral information) is re-tained by him when he has no right to do so or when to communicate it or a duty to communicate it. Also ne will be guilty of an offence if such an article or is communicated by him except where he has authority it is contrary to his duty to do so.

- cation of any article or document or information then the recipient is under a similar duty not to make any tain it. Failure to observe this duty is an offence by Where there has been a lawful confidential communiunauthorised communication thereof and not to rethat recipient under Section 79. (P)
- which relates to or is used in a prohibited place or cation or retention thereof (as above) by any person In the case of any article or document or information anything in such a place, any unauthorised communiis an offence under Section 79. (0)
- made or obtained in contravention of Part VII of the If any article or document or information has been Act then, under Section 79 it is an offence for any person to communicate or retain it except as is authorised by that Section. (p)
- at the time when he receives it" that the communication to him is in contravention of Part VII of the Act, unless he proves that the communication to him son "knowing, or having reasonable ground to believe, The mere receipt of any article or document or information is an offence under Section 79 by any perwas contrary to his desire. (e)

Other Provisions of the Crimes Act

accordingly (Section 5), and that any person who attempts to commit any offence shall be guilty of an offence and shall be be deemed to have committed that offence and shall be punishable Other sections of the Crimes Act provide that any person ingly concerned in or party to the commission of an offence shall punishable as if the attempted offence had been committed (Secwho aids, counsels, or procures, or is directly or indirectly knowtion 7).

MAY, 1954

RESTRICTED

In the investigation of any breaches of security it must be remembered that the consent of the Attorney-General to any prosecutions under Part VII of the Crimes Act is required by Section 85 which provides:- (1) A prosecution under this Part of this Act shall be instituted only by or with the consent of the Attorney-General or of a person acting under his direction:

Provided that a person charged with any offence against this Part of this Act may be arrested, or a warrant for his arrest issued and executed, and he may be remanded in custody or on bail, notwithstanding that the consent of the Attorney-General or a person acting under his direction has not been obtained, but no further proceedings shall be taken until that consent has been obtained.

Nothing in this Section shall prevent the discharging of the accused if proceedings are not continued within a reasonable time,"

The Defence Act 1903-1949

Section 73A of this Act provides:-

(1) Any member of the Defence Force or officer in the his official duty any plan, document, or information relating to any fort, battery, field work, fortification, Public Service of the Commonwealth who communicates to any person otherwise than in the course of wealth, or to any factory, or air-force aerodrome or or defence work, or to any defences of the Commonestablishment or any other naval, military or airforce information shall be guilty of an offence.

ment, or information relating to any fort, battery, field work, fortification, or defence work, or air-force aerodrome or establishment, or to any of the defences Any person who unlawfully obtains any plan, docuof the Commonwealth or any other naval, military or air-force information, shall be guilty of an offence. (2)

The punishment for an offence under Section 73A is:-

exceeding £100, or imprisonment for six months, or (i) if the offence is prosecuted summarily — a fine not

RESTRICTED

MAY, 1954

RESTRICTED

both; or in the case of a body corporate a fine not exceeding £1000.

if the offence is prosecuted on indictment — a fine of any amount, or imprisonment for any term, or both."

Section 82 of the Defence Act provides:-

material or any naval, military or air-force work of defence in the Commonwealth or of any portion therefortification, aircraft, air-force establishment, aircraft of shall be liable to a penalty not exceeding £100 or, at the discretion of the Court, to be imprisoned, with or without hard labour, for any period not exceeding six (1) Any person who, without lawful authority, makes or attempts to make any sketch, drawing, photograph, picture or painting of any fort, battery, fieldwork, months;

tention of committing any breach of the provisions of this section, shall be liable to a penalty not exceeding any naval, military or air-force work of defence with sketching, drawing, photographing or painting materials or apparatus in his possession, with the in-Any person who, without lawful authority, enters or aircraft, air-force establishment, aircraft material or approaches any fort, battery, field-work, fortification,

The Supply and Development Act 1939-1948

Section 25 of this Act provides for the observance of secrecy:

this Act and an officer of the Commonwealth or a State to whom information furnished in pursuance of this Act has been disclosed by virtue of his official position, shall not, except as allowed by this Act or the regulations, divulge any information "An officer or employee of the Department, a member of a Committee or of a Board constituted, or deemed to have been constituted, under this Act, a person performing any duty or function in relation to any matter specified in or arising under this Act or any regulation made under, or in force by virtue of, or particulars furnished in pursuance of this Act or the regula-

Penalty: Fifty pounds or imprisonment for three months or both."

RESTRICTED

The Defence (Special Undertakings) Act 1952

14. This Act deals with special defence undertakings and makes provision for prohibited areas and restricted areas to be declared for the purposes of the Act. Section 9, subsection 2 pro-

"A person shall not, without lawful authority or excuse-

(a) make a photograph, sketch, plan, model. article, note or other document of, or relating to, a prohibited area or anything in a prohibited area; or

(b) obtain, collect, record, use, have in his possession, publish sketch, plan, model, article, note or other document or information relating to, or used in, a prohibited area, or or communicate to some other person a photograph, relating to anything in a prohibited area.

Penalty: Imprisonment for seven years."

Prosecutions under the Act require the consent of the Commonwealth Attorney-General or of a person acting under his direction, but the Act provides:-

"Section 28. (2) A person charged with an offence against or a warrant for his arrest may be issued and executed, and he may be remanded in custody or on bail, notwithstanding that the consent of the Attorney-General or of a person actbut no further proceedings shall be taken ing under his direction has not been obtained, this Act or the regulations may be arrested until that consent has been obtained.

charge of a person charged if proceedings Nothing in this section prevents the disare not continued within a reasonable time. (3)

Various Other Commonwealth Acts

Provisions are contained in various other Commonwealth Acts for the preservation of the secrecy of information which is obtained pursuant to those Acts. Included among these are:-

Income Tax Assessment Act. Sales Tax Assessment Act,

Navigation Act,

Commonwealth Electoral Act,

Australian Industries Preservation Act.

RESTRICTED

May, 1954

RESTRICTED

Others Employed by the Government and to Persons not in The Application of the Provisions to Public Servants and the Employ of the Government

tralia. Section 78 of the Crimes Act applies to any such person without restriction, and Section 79 also has this general application the Commonwealth; thus it applies particularly to members of the of the Government but also every person who is subject to and entitled to the benefit of the laws of the Commonwealth of Ausand in addition refers to the holding of office under the Queen or application, their operation covers not only persons in the employ Some of the provisions outlined above are of general Commonwealth Public Service and persons employed by Commonwealth or State organisations or instrumentalities.

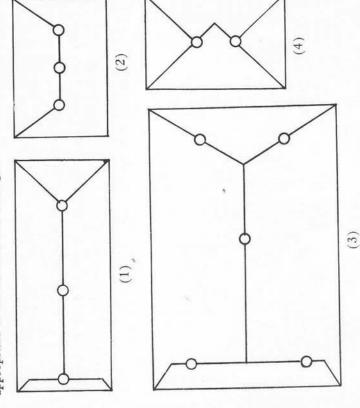
The Defence (Special Undertakings) Act also applies generally. Its operation covers all members of the community including public servants.

that Act. The Defence Act partly applies to "any member of the Defence Force or officer in the Public Service of the Commonwealth", and in part is of general and unrestricted application. The done by any person permanently or temporarily employed in the Public Service of the Comonwealth, and also any other person who The Defence Act partly applies to "any member of the Supply and Development Act refers specifically to "an officer or employee of the Department" and to other officials and employees Acts in the main apply directly to the persons (normally Public Servants) who are employed in the Departments operating by applies to persons employed in any capacity in the Public Service of the Commonwealth. Section 70 of the Crimes Act refers to acts is within the definition of a Commonwealth officer as provided by and also to any "officer of the Commonwealth or a State to whom information furnished in pursuance of this Act has been disclosed by virtue of his official position". The various other Commonwealth The Commonwealth Public Service Act and Regulations virtue of or in respect of the particular Act.

APPENDIX A

SEALING ENVELOPES

When TOP SECRET, SECRET or CONFIDENTIAL matter is prepared for despatch, the inner envelope should be sealed with wax or waters in whichever of the four ways shown below is appropriate to the form of the envelope.



Note.—Sealing wax should be spread as thinly as possible, and the die of the seal pressed firmly into the wax to ensure that the seal cannot be removed intact.

Page 65 Max, 1954 (amendment No. 2 Dec., 1956)

In order to guard against unauthorised removal without detec-tion, the following points should be observed in the provision and use of wafers:-

- (1) They should be made of paper of suitable quality with a serrated edge.
- (2) They should have good adhesive qualities.
- They should for preference bear the name of the originating authority. (3)
- (4) The originating authority should overstamp all wafers with a wide rubber stamp."

RESTRICTED

APPENDIX B

The following measures will be taken to safeguard CLASSIFIED EQUIPMENT IN TRANSIT classified equipment in transit:

- ments rests with the consignor. When the physical security passes out of his hands, it is his responsibility to ensure that the person temporarily in charge is made aware of the classified nature of his charge. The consignor is the factory, annexe, establishment, ship, station, unit, or formation, etc., having physical (a) The responsibility for making the security arrangecustody of the equipment when it has to be moved.
- before despatch as it may be appropriate at this stage The consignor will check the grading of the equipment to downgrade the equipment. (P)
- signee of the details of despatch and transport, in ample time for arrangements to be made for its reception. Route, time of departure and halting places The consignor is responsible for informing the conmust be varied for each particular consignment. (c)
- TOP SECRET and SECRET equipment will be covered by a system of receipts at all points of transference of custody. (p)
 - Classified equipment will be carried in closed vehicles where possible. If this cannot be done, it will be crated, sheeted or otherwise camouflaged or con-If transport is by rail, and break of gauge necessitates unloading and reloading, special security precautions are to be taken. cealed. (e)
- points, a guard will be maintained during loading and unloading operations. Where equipment is placed into Bond Stores, a receipt will be obtained and a guard When TOP SECRET or SECRET equipment is delivered to sea ports, air ports or rail or road terminal (£)

May, 1954

RESTRICTED

Page 67

Max, 1954 (amendment No. 2 Dec., 1956)

SECRET and SECRET equipment and will be given security instructions when accompanying CONFID-(h) Drivers of vehicles and escorts of classified equipment will be security checked. They will be issued with written security instructions when accompanying TOP No indications of the nature or the purpose of the equipment ENTIÁL or RESTRICTED equipment. is to be shown in these instructions.

volved in the movement will be required, and an Where private firms contract to move classified equipment, a security check on the firms' employees inescort provided in accordance with paragraph 2 below.

The following specific rules will apply, subject to the above measures:-

(a) TOP SECRET Equipment-

ported by rail, will be loaded in a separate TOP SECRET equipment, when transvan which will be locked and sealed. An armed escort, including a Commissioned or Security Officer, will always be provided. (i) Rail

guard in each vehicle, additional to the missioned Officer or Security Officer will Movement of TOP SECRET equipment driver. If vehicles are in convoy, a Comvehicle will ever be left unattended and by road will be under escort of an armed no unauthorised persons will be permitted to see the equipment. This is particularly important during loading and unbe appointed in overall command. ii) Road

RESTRICTED

RESTRICTED

event of a break-down, or where night halts are necessary, the officer in charge of the escort is to make parking arrange-ments with the nearest military authoading of vehicles, and at halts. In the ority, or failing that, with the Civil Police.

(iii) Seat

nature, when transported by sea, will be port or a vessel under Service control, in a lock-up stowage. It will bear the marking "LOCK-UP STOWAGE". TOP SECRET packages transported by sea. will be sent by "Safe Hand" method in a Naval vessel or in the personal care of the Master of a British vessel. (For details of "Safe Hand" method see TOP SECRET equipment of a bulky sent in a Naval vessel, a Service trans-Chapter V, paragraph 8.)

line company which has been authorised to carry "Safe Hand" matter. TOP SECRET equipment should not be carin a Service aircraft or in the care of the TOP SECRET equipment carried by air will be despatched "Safe Hand" method Captain of an aircraft of a British airried by air where the route is over foreign territory, but if this is necessary it should be in charge of a courier. (iv) Air

TOP SECRET equipment will never be sent by civil post. (v) Post

(b) SECRET Equipment—

SECRET equipment transported by rail is to be despatched in a separate locked van and is to be accompanied by an armed escort. (i) Rail

guard in each vehicle in addition to the SECRET equipment transported by road will be under the escort of an armed (ii) Road

MAY, 1954

military authority, or, failing that, with SECRET equipment of a bulky nature, the Civil Police

(iii) Sea

halts are necessary, the escort will make

parking arrangements with the nearest

British vessel in a lock-up stowage and marked "LOCK-UP STOWAGE". SECtransported by sea, will be sent in a RET packages sent by sea are to be sent "Safe Hand" method, SECRET equipment sent by air is to be sent "Safe Hand" method. The "Speed (iv) Air

Pack" and "Precious Cargo" stowages are available in some aircraft for bulky ed in bags sealed with diplomatic seal so equipment. If the route is over foreign territory, the equipment should be stowthat, in the event of a landing, it is immune from foreign Customs inspection.

If a "Safe Hand" Service is not available, SECRET packages may be sent by registered mail to destinations within Aus-(v) Post

(c) CONFIDENTIAL Equipment—

by rail will be cased or otherwise con-cealed and loaded into a locked van. CONFIDENTIAL equipment when sent van, an escort is to be provided. Where Where stowage is other than in a locked break of railway gauge necessitates un-loading and reloading, escort will be provided locally. (i) Rail

RESTRICTED

May, 1954

RESTRICTED

- (ii) Road Equipment is to be sent in a locked van or truck. Where this is not possible, an escort, in addition to the driver of the vehicle, is to be provided. Vehicles must not be left unprotected.
- To be transported in a British vessel in a lock-up stowage. iii) Sea
- If carried in Service aircraft no escort is required. If carried in civil aircraft, "Safe Hand" method is to be employed. (iv) Air
- (v) Post If sent through civil post, packages are to be sent registered method.
- (d) RESTRICTED Equipment—

RESTRICTED equipment is to be moved under conditions which will not give access or view to unauthorised persons.



RUSI of Victoria Library Ground Floor, H Block Victoria Barracks Southbank VIC 3006 03 9282 5918 rusi vic@defence.gov.au



Securing Government Business

Protective security guidance for executives

Approved October 2014

Amended April 2015

Version 2.1

© Commonwealth of Australia 2014

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 3.0 AU licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.itsanhonour.gov.au).

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Commercial and Administrative Law Branch Attorney-General's Department 3–5 National Cct BARTON ACT 2600

Telephone: 02 6141 6666

copyright@ag.gov.au

Document details		
Security classification	Unclassified	
Dissemination limiting marking	Publicly available	
Date of next review	October 2017	
Authority	Attorney-General	
Author	Protective Security Policy Section Attorney-General's Department	
Document status	Approved 21 October 2014 This document replaces Securing Government Business – Protective security guidance for executives – Version 1 Amended April 2015	

Contents

Am	nendments	ii
1.	Directive on the Security of Government Business	
2.	Australian Government Protective Security Policy	2
	Directive on the Security of Government Business	2
	Governance arrangements, core policies and mandatory requirements	3
	Protocols, standards and guidelines	4
	Agency specific policies and procedures	4
3.	Applicability of the Protective Security Policy Framework	5
4.	Legislation	6
App	pendix 1—Mandatory Requirements—summary table	A1-1
	Governance	A1-1
	Personnel security	A1-3
	Information security	A1-4
	Physical security	A1-5
Apr	pendix 2—Legislation	A2-1

Amendments

No.	Date	Location	Amendment
1.	April 2015	Throughout	Update links
2.			
3.			

1. Directive on the Security of Government Business

The Australian Government is committed to effectively managing the protective security risks to Government business and building increased trust, confidence and engagement with the Australian people and our international partners.

The Government requires agency heads to have in place effective protective security arrangements to ensure:

- their respective agency's capacity to function
- the safety of those employed to carry out the functions of government and those who are clients of government
- official resources and information the agency holds in trust, both from and for the public, and those provided in confidence by other countries, agencies and organisations, are safeguarded.

To achieve this, agency heads are to apply the <u>Protective Security Policy Framework</u> and promote protective security as part of their agency's culture. A progressive protective security culture that engages with risk will foster innovation, leading to the increased productivity of Government business.

The Australian Government, through my Department, will continue to develop and refine protective security policy that promotes the most efficient and effective ways to secure the continued delivery of Government business.

Senator the Hon George Brandis QC Attorney-General

21 October 2014

2. Australian Government Protective Security Policy

2.1 Australia's protective security policy is organised in a tiered, hierarchical structure—the *Protective Security Policy Framework* (PSPF).



Figure 1—Protective Security Policy Framework

Directive on the Security of Government Business

2.2 The Directive on the Security of Government Business (Section 1) is the keystone of the protective security policy. It articulates the Government's requirement for protective security to be a business enabler that allows agencies to work together securely in an environment of trust and confidence.

Governance arrangements, core policies and mandatory requirements

2.3 The governance arrangements and core policies in the PSPF describe the higher level mandatory requirements. All applicable agencies and bodies (see Section 3. Applicability of the Protective Security Policy Framework) are to comply with the mandatory requirements. These requirements cover governance, personnel security, information security, and physical security.

Governance. Agencies are to implement protective security governance arrangements and are to:

- Use risk management principles and policies appropriate to agency functions and the security threats faced in developing, implementing and maintaining:
 - protective security measures
 - business continuity management plans
 - fraud control plans
- Prepare, monitor and review their security plans to ensure they are complying with the mandatory requirements.
- Report annually to their portfolio Minister on the level of agency compliance with the PSPF.
- Develop a culture of security through strong programs of security awareness and education to ensure employees fully understand their security responsibilities.
- Remain accountable for the efficient and secure performance of outsourced functions.
- Investigate security incidents promptly and with sensitivity.

<u>Personnel security</u>. Agencies are to ensure the people they employ are suitable and meet high standards of integrity, honesty and tolerance at and throughout the period of their engagement. Where necessary, people are to be security cleared to the appropriate level.

Information security. Agencies are to ensure:

- They appropriately safeguard all official information to ensure its confidentiality, integrity, and availability by applying safeguards so that:
 - only authorised people access information through approved processes
 - information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
 - information is classified and labelled as required
- Information created, stored, processed, or transmitted in or over government information and communication technology (ICT) systems is to be properly managed and protected throughout all phases of a system's life cycle in accordance with the PSPF. This includes the *Australian Government Information Security Manual* (ISM), produced by the Australian Signals Directorate.

Physical security. Agencies are to provide and maintain:

- A safe working environment for their employees, contractors, clients and the public.
- A secure physical environment for their official resources.

The mandatory requirements are summarised at **Appendix 1**.

Protocols, standards and guidelines

- 2.4 The PSPF contains the key practice documents including:
 - Protocols for the conduct of Government specific protective security activities to meet the mandatory requirements.
 - Better practice guidelines.
 - References to other protective security and risk management documents, including applicable Australian and International Standards.
- 2.5 These documents standardise protective security practices across Government to provide assurance in asset sharing, support interagency business, and help meet international obligations.

Agency specific policies and procedures

- 2.6 Agencies are to develop specific protective security policies and procedures (Figure 1) that meet their business needs. These policies and procedures should complement and support other agency operational procedures.
- 2.7 Agency protective security policies and procedures are to take into account the risks created by the agency for others, as well as the risks inherited from business partners.

3. Applicability of the Protective Security Policy Framework

- 3.1 As a policy of the Australian Government, the following agencies¹ must apply the PSPF to the extent that their enabling legislation allows:
 - Non-corporate Commonwealth entities subject to the <u>Public Governance, Performance</u> <u>and Accountability Act 2013</u> (Cth) (PGPA Act).
 - Corporate Commonwealth entities and companies subject to the PGPA Act that have received Ministerial direction to apply the general policies of the Australian Government.
 - Other bodies established for a public purpose under a law of the Commonwealth and other Australian Government agencies, that have received a notice from the relevant Minister that the PSPF applies to them.
- 3.2 The Australian Government requires non-government organisations that access security classified information to enter into a Deed of Agreement to apply the PSPF to that information.
- 3.3 The Commonwealth expects state and territory government agencies that hold or access Commonwealth security classified information at CONFIDENTIAL and above to apply the PSPF to that information.

¹ In the PSPF, a reference to 'agency' (or 'Australian Government agency') means an entity or body in the first three categories referenced above. Reference to an 'agency head' means the head or chief executive of an agency.

4. Legislation

- 4.1 Although the PSPF is not legally prescribed, it supports legislation relevant to protective security and reflects the aims and objectives of the Australian Government.
- 4.2 Some agencies are responsible for collecting or processing official information for which there are legislative security requirements. These requirements take precedence over the PSPF. Where the relevant legislation mandates lower standards than the PSPF, agencies are encouraged to meet the PSPF's higher standards.
- 4.3 As a valuable resource, information is only to be released in accordance with the policies, legislative requirements and directives of Government, the Parliament and the courts. The unauthorised disclosure of information held by the Australian Government is subject to the sanction of criminal law.
- 4.4 The general legislative obligations applicable to all agencies are outlined at **Appendix 2**.

Appendix 1—Mandatory Requirements—summary table

	Governance		
1	<u>GOV-1</u>	Agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware and meet the requirements of the Protective Security Policy Framework.	
2	GOV-2	 To fulfil their security obligations, agencies must appoint: a member of the Senior Executive Service as the security executive, responsible for the agency protective security policy and oversight of protective security practices an agency security adviser (ASA) responsible for the day-to-day performance of protective security functions an information technology security adviser (ITSA) to advise senior management on the security of the agency's Information Communications Technology (ICT) systems 	
3	GOV-3	Agencies must ensure that the agency security adviser (ASA) and information technology security adviser (ITSA) have detailed knowledge of agency-specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.	
4	GOV-4	Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised every two years or sooner where changes in risks and the agency's operating environment dictate.	
5	<u>GOV-5</u>	Agencies must develop their own set of protective security policies and procedures to meet their specific business needs.	
6	GOV-6	Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standards AS/NZS ISO 31000:2009 Risk management—Principles and guidelines and HB 167:2006 Security risk management.	

7	GOV-7	For internal audit and reporting, agencies must:
		undertake an annual security assessment against the mandatory requirements detailed within the Protective Security Policy Framework
		report their compliance with the mandatory requirements to the relevant portfolio Minister
		The report must:
		contain a declaration of compliance by the agency head
		state any areas of non-compliance, including details on measures taken to lessen identified risks
		In addition to their portfolio Minister, agencies must send a copy of their annual report on compliance with the mandatory requirements to:
		the Secretary, Attorney-General's Department
		the Auditor General
		Agencies must also advise any non-compliance with mandatory requirements to:
		the Director, Australian Signals Directorate for matters relating to the Australian Government Information Security Manual (ISM).
		the Director-General, Australian Security Intelligence Organisation for matters relating to national security
		the heads of any agencies whose people, information or assets may be affected by the non-compliance
8	GOV-8	Agencies must ensure investigators are appropriately trained and have procedures in place for reporting and investigating security incidents and taking corrective action, in accordance with the provisions of the:
		Australian Government protective security governance guidelines— Reporting incidents and conducting security investigations, or
		Australian Government Investigations Standards
9	<u>GOV- 9</u>	Agencies must give all employees, including contractors, guidance on Sections 70 and 79 of the <i>Crimes Act 1914</i> , section 91.1 of the <i>Criminal Code Act 1995</i> , the <i>Freedom of Information Act 1982</i> and the <i>Information Privacy Principles</i> contained in the <i>Privacy Act 1988</i> , including how this legislation relates to their role.
10	<u>GOV-10</u>	Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Australia is a party.
11	GOV-11	Agencies must establish a business continuity management (BCM) program to provide for the continued availability of critical services and assets, and other services and assets when warranted by a threat and risk assessment.

12	GOV-12	Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.
13	GOV-13	Agencies must comply with section 10 of the <i>Public Governance, Performance</i> and Accountability Rule 2014 and the Commonwealth Fraud Control Policy.
		Personnel security
14	PERSEC 1	Agencies must ensure that their personnel who access Australian Government resources (people, information and assets): • are eligible to have access • have had their identity established • are suitable to have access
		agree to comply with the Government's policies, standards, protocols and guidelines that safeguard the agency's resources from harm
15	PERSEC 2	Agencies must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.
16	PERSEC 3	Agencies must identify, record and review positions that require a security clearance and the level of clearance required.
17	PERSEC 4	Agencies must ensure their personnel with ongoing access to Australian Government security classified resources hold a security clearance at the appropriate level, sponsored by an Australian Government agency.
18	PERSEC 5	Before issuing an eligibility waiver (citizenship or checkable background) and prior to requesting an Australian Government security clearance an agency must: • justify an exceptional business requirement • conduct and document a risk assessment • define the period covered by the waiver (which cannot be open-ended) • gain agreement from the clearance applicant to meet the conditions of the
		waiverconsult with the vetting agency
19	PERSEC 6	Agencies, other than authorised vetting agencies, must use the Australian Government Security Vetting Agency (AGSVA) to conduct initial vetting and reviews.
20	PERSEC 7	Agencies must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their agencies.

21	PERSEC 8	Agencies and vetting agencies must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.
22	PERSEC 9	Agencies must have separation policies and procedures for departing clearance holders, which includes a requirement to:
		inform vetting agencies when a clearance holder leaves agency employment or contract engagement
		advise vetting agencies of any security concerns
		Information security
23	INFOSEC 1	Agency heads must provide clear direction on information security through the development and implementation of an agency information security policy, and address agency information security requirements as part of the agency security plan.
24	INFOSEC 2	Each agency must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency's information environment.
25	INFOSEC 3	Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.
26	INFOSEC 4	Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual.
27	INFOSEC 5	Agencies must have in place control measures based on business owner requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Agency access control rules must be consistent with agency business requirements and information classification as well as legal obligations.
28	INFOSEC 6	Agencies must have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks, infrastructures and applications.
29	INFOSEC 7	Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the agency operates.

	Physical security		
30	PHYSEC 1	Agency heads must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the agency security plan.	
31	PHYSEC 2	 Agencies must have in place policies and procedures to: identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases, agencies may have to extend protection and support to family members and others report incidents to management, human resources, security and law enforcement authorities, as appropriate provide information, training and counselling to employees maintain thorough records and statements on reported incidents 	
32	PHYSEC 3	Agencies must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.	
33	PHYSEC 4	Agencies must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.	
34	PHYSEC 5	Agencies must show a duty of care for the physical safety of those members of the public interacting directly with the Australian Government. Where an agency's function involves providing services, the agency must ensure that clients can transact with the Australian Government with confidence about their physical wellbeing.	
35	PHYSEC 6	Agencies must implement a level of physical security measures that minimises or removes the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.	
36	PHYSEC 7	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its agencies to implement heightened security levels.	

Appendix 2—Legislation

Laws applicable to agencies may include, but are not limited to, the following legislative instruments.

Public Governance, Performance and Accountability Act 2013

The *Public Governance, Performance and Accountability Act 2013* (Cth) (PGPA Act) replaced the *Financial Management and Accountability Act 1997* (Cth) (FMA Act) and the *Commonwealth Authorities and Companies Act 1997* (Cth) (CAC Act) on 1 July 2014. The PGPA Act operates on four principles:

- government should operate as a coherent whole
- a uniform set of duties should apply to all resources handled by Commonwealth entities
- performance of the public sector is more than financial
- engaging with risk is a necessary step in improving performance.

The PGPA Act is consistent with the PSPF in that it obligates authorised authorities (agency heads) to manage the risks within their entity (agency) while providing assurance.

Crimes Act 1914(Cth)

The *Crimes Act 1914* (Cth) (Crimes Act) contains provisions relating to the protection of prescribed official information and sets out the penalties for the unauthorised disclosure of that information. Section 70 of the Crimes Act makes it an offence for a Commonwealth officer, or a former Commonwealth officer, to disclose any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer that he or she is, or was at the time of ceasing to be a Commonwealth officer, bound not to disclose.

Commonwealth officers are also bound by provisions dealing with the protection of official secrets. Section 79 of the Crimes Act makes it an offence to communicate or receive official secrets in certain circumstances. This includes where a person is entrusted with information by a Commonwealth officer and the person has a duty to treat the information as secret.

Criminal Code Act 1995(Cth)

Section 91.1 of the *Criminal Code* Act 1995 (Cth) makes it an offence to engage in conduct that amounts to espionage. Such conduct includes communicating or making information available without authority for delivery to another country or foreign organisation.

Defence Act 1903 (Cth)

The *Defence Act 1903* (Cth) contains similar provisions to the Crimes Act for preserving the secrecy of information relating to any defence works relevant to the defence of the Commonwealth.

Australian Security Intelligence Organisation Act 1979 (Cth) and Intelligence Services Act 2001 (Cth)

Commonwealth officers are also subject to offences for unauthorised handling of specific types of information. For example, subsection 18(2) of the *Australian Security Intelligence Organisation Act* 1979 (Cth) makes it an offence to communicate information received from Australian Security

Intelligence Organisation in various circumstances. Sections 39 and 40 of the *Intelligence Services Act* 2001 (Cth) also prohibit communication of information prepared by the Australian Secret Intelligence Service or the Australian Signals Directorate.

Public Service Act 1999 (Cth)

Section 13 of the *Public Service Act 1999*(Cth) sets out the Australian Public Service Code of Conduct. Public Service Regulation 2.1, made under that Code, broadly provides that an APS employee must not disclose material where:

- that disclosure could be prejudicial to the effective working of Government, or
- where that material was received or communicated in confidence.

There are some exceptions to this requirement where, for example, the disclosure was authorised by the agency head, or where the disclosure is made in the course of the employee's duties.

Further information about regulation 2.1, and the Code of Conduct, is available from the Ethics Advisory Service on (02) 6202 3737.

Freedom of Information Act 1982 (Cth) and Privacy Act 1988(Cth)

Disclosure of official information should only occur if that disclosure is authorised. Authorisation may be granted under the express authority of an agency head, subject to the provisions of the *Freedom* of *Information Act 1982* (Cth) (the FOI Act) and the *Privacy Act 1988* (Cth) (the Privacy Act).

The general principle underlying the FOI Act is that government documents should be made available to the general public except where a document is exempt from the operation of the Act, subject to an exemption under division 2 of Part IV of the FOI Act, or subject to a conditional exemption under division 3 of Part IV and disclosure would be contrary to the public interest. The broad aim of the FOI Act is to provide a mechanism for individuals to check and seek to correct information held on government files (if necessary), enhance the transparency and accountability of government, ensure the community can participate in the democratic processes, and facilitate the wide availability of government information.

The Privacy Act sets out the Australian Privacy Principles (APPs), which provide legislative standards on how Australian Government agencies and certain private sector activities (for example, consumer credit reporting) handle personal information—ie, information or opinions that can identify a living person. The APPs relate to the collection, storage, security, access, use and disclosure of personal information, and provide individuals with a right of access to, and correction of, personal information about themselves. The APPs also set out various exceptions to their application, which can be viewed in Schedule 1 of the Privacy Act.

Work Health and Safety Act 2011 (Cth)

While most of the legislation relevant to protective security is concerned with the protection of official information, an employer may also need to implement protective security measures to ensure it meets its duty of care obligations under the *Work Health and Safety Act 2011*(Cth).



DEFENCE INSTRUCTIONS (GENERAL)

Amendment

ADMIN 20–29 AMDT NO 2

Defence Security Manual

Complete Revision

Department of Defence CANBERRA ACT 2600

21 May 2010

Issued with the authority of the Chief of the Defence Force and the Secretary of the Department of Defence pursuant to section 9A of the *Defence Act 1903* for members of the Australian Defence Force.

Issued with the authority of the Secretary pursuant to section 20 of the *Public Service Act 1999* for Department of Defence Australian Public Service employees.

DR I.J. WATT, AO

A.G. HOUSTON, AC, AFC Air Chief Marshal Chief of the Defence Force

LIST B—ISSUE NO ADMIN B/2/2010

Single Service filing instructions Sponsor:

This instruction should be filed as: Intelligence and Security Group

NAVY ADMIN 101–40 Sponsor contact:

2. ARMY ADMIN 20–161 Deputy Secretary Intelligence and Security

3. AIR FORCE ADMIN 6–65 Review Date: 25 May 2013

Cancellation

DI(G) ADMIN 20-29 ISSUE NO ADMIN B/2/2007 of 16 FEB 2007 (AL1) is cancelled.

Note

This Instruction cancels all documents listed in annex A.



DI(G) ADMIN 20–29
File as: (NAVY ADMIN 101–40
(ARMY ADMIN 20–161
(AIR FORCE ADMIN 6–65
(Complete Revision)

DEFENCE SECURITY MANUAL

INTRODUCTION

- 1. The Australian Government's policy on protective security is promulgated in the *Australian Government Protective Security Manual* (PSM) and the *Australian Government Information and Communications Technology Security Manual* (ISM). The PSM and the ISM are the source of the security principles and set out the minimum standards to which all Australian Government agencies, including Defence, must adhere.
- 2. The *electronic Defence Security Manual* (eDSM) has been designed as an online manual that is responsive to the protective security requirements in the PSM and ISM and provides additional Defence-specific security guidance. The eDSM was developed in consultation with security stakeholders across Defence.
- 3. This Instruction revokes and replaces *Defence Security Manual*, edition 2 with the eDSM, and cancels the specific security-related Defence Instructions, Departmental Security Instructions and DEFGRAMs detailed in annex A.

POLICY STATEMENT

- 4. In support of the Australian Government, Defence has established protective security policy, objectives and measures aimed to safeguard its capabilities and mission. A statement of overall protective security policy is available in eDSM, part 1—'Protective Security Policy and Governance'.
- 5. A statement of policy relating to aspects of protective security associated with each eDSM part is available under the heading Policy within each eDSM part.

SCOPE

- 6. This Instruction authorises the eDSM as the principal reference for protective security policy within Defence.
- 7. This Instruction applies to Defence personnel including members of the Australian Defence Force (ADF), Australian Public Service (APS) employees, and equivalents from other Defence organisations on exchange to Defence. Defence personnel are, and external service providers may be, under contractual obligations, bound by the security policy contained in the eDSM, and by reference from it, the requirements set out in the PSM and ISM.

DEFINITIONS

8. Definitions are included in each eDSM part and within the eDSM's Glossary.

ROLES AND RESPONSIBILITIES

- 9. Key roles and responsibilities for protective security in Defence are detailed in eDSM, part 1.
- 10. The Chief of the Defence Force (CDF) and the Secretary of Defence have designated the Chief Security Officer (CSO) as the Agency Security Adviser (ASA) for Defence. In this role, the CSO must perform all of the responsibilities mandated of an ASA and, as such, is responsible for ensuring that Defence's policies and practices within the eDSM remain valid and current with the PSM and ISM, as published from time to time, and meet Defence's business needs. For further information on the delegated responsibilities of the CSO see Joint Directive 01/2009.
- 11. Future amendments to the eDSM will be announced through a dedicated bulletin board on the eDSM site.

IMPLEMENTATION

12. Commanders and managers are responsible for the implementation of protective security policy in their military or business units and, through contractual provisions, the implementation of policy by external service providers with whom they have a contractual relationship.

COMPLIANCE REGIME

- 13. Compliance requirements for protective security are detailed in eDSM, part 1 and within each eDSM part under the heading Compliance Requirements. Compliance with mandatory requirements in the eDSM is a mandatory requirement of this Instruction. Mandatory requirements in the eDSM are described through the use of the words 'should' and 'should not', 'must' and 'must not' or, if the mandatory requirement is restated from the PSM or ISM, 'must' and 'must not'. In circumstances where it is not possible to comply with a mandatory requirement of the eDSM, the waiver and dispensation process set out in eDSM, part 2:1—'Waivers and Dispensations' must be initiated. For further information see eDSM, part 2:1.
- 14. This Instruction constitutes an order to members of the ADF from the CDF. As such, a breach of any mandatory requirement set out in this Instruction may lead to administrative action, or disciplinary action under the *Defence Force Discipline Act 1982*, being taken against a member for the breach.
- 15. This Instruction also constitutes a lawful and reasonable direction to APS employees in the Department of Defence (including APS employees in the Defence Materiel Organisation) by the Secretary under section 13(5) of the *Public Service Act 1999*. As such, a breach of any mandatory requirement set out in this Instruction may lead to action being taken against an APS employee for breach of the APS Code of Conduct.

MONITORING AND REPORTING

16. Monitoring and reporting arrangements for compliance with protective security policy are detailed in eDSM, part 1 under the heading 'Security Governance'.

RELATED POLICY AND LEGISLATION

17. The PSM and ISM are authoritative Commonwealth policy documents that set out the protective security principles and minimum standards that Commonwealth agencies and their employees must adhere to in order to fulfil their portfolio responsibilities. Related legislation is detailed in eDSM, part 1 under the heading 'External Conformance'.

Annex:

A. List of cancelled Defence Instructions, Departmental Security Instructions and DEFGRAMs

Sponsor: Deputy Secretary Intelligence and Security

ANNEX A TO DI(G) ADMIN 20–29

File as: (NAVY ADMIN 101–40 (ARMY ADMIN 20–161 (AIR FORCE ADMIN 6–65

(Complete Revision)

LIST OF CANCELLED DEFENCE INSTRUCTIONS, DEPARTMENTAL SECURITY INSTRUCTIONS AND DEFGRAMS

Defence Instruction Number	Title		
Defence Instruction (General) (DI(G)) OPS 07–17	Security Policy on BlackBerry		
DI(G) OPS 13-10	Conduct of security inspections under the Defence Protective Security Alert System—SAFEBASE		
DI(G) PERS 55-2	Defence Security Authority: the security clearance process		
DI(G) PERS 52-1	Defence Identity and Access Control Cards		
Departmental Security Instruction Number	Title		
2/2005	Security policy on the use of multi-function devices within Defence		
3/2004	Defence Standards for commercial grade Information and Communications Technology equipment cabinets		
2/2004	Defence Special Compartmented Information—codeword recordkeeping		
1/2004	Security clearance requirements in Defence request documentation		
4/2003	Policy on external connections to the Defence Information Environment		
3/2003	Classification of standard operating environment for the Defence Information Environment		
3/2002	Use of cordless telephones within Defence environments		
9/99	Security considerations for unit home pages		
5/99	Telephone security—classified and unclassified discussions		
DEFGRAM Number	Title		
476/2009	Release of the Electronic Defence Security Manual		
421/2009	Pre-release of e-Defence Security Manual policy relating to weapons and explosive ordnance		
595/2008	Security clearance request processing priorities		
273/2008	Recognition of certain foreign security clearances		
272/2008	Overseas visit authorisation requests: online process		
706/2007	New online visits process for requesting overseas visit approvals		
363/2006	Use of Australian Defence Force identity cards and Department of Defence access cards		



Defence Security and Vetting Service Intelligent security for an insecure world

DSM Companion Document

Defence Security Context				
Version	1	Publication date	9 July 2015	
Optimised for	Screen; Print; Screen Reader			
Releasable to	Defence and Defence industry			
Copyright	© Commonwealth of Australia 2010 This work is copyright. Apart from any use as permitted under the <i>Copyright Act 1968</i> , no part may be reproduced by any process without prior written permission from the Department of Defence. Requests and inquiries concerning reproduction and rights should be addressed to Defence Publishing Services, Department of Defence.			

Defending Australia and its National Interests www.defence.gov.au

Defence Security Context

Purpose

1. This part outlines the fundamental elements of security in order to demonstrate how the Defence Security Manual (DSM) contributes to security in Defence as a whole. This section provides the greater security context within which Defence operates.

Why Do We Do Security?

- 2. The Department of Defence needs to develop robust protective security arrangements in order to defend Australia and its national interests. To do this, Defence must be able to:
 - a. safeguard its people and clients from foreseeable risks;
 - b. limit the potential for compromise of the confidentiality, integrity and availability of its official information and assets:
 - c. protect its assets from loss or misuse;
 - d. facilitate the appropriate sharing of information in order for the Government to effectively do business; and
 - e. support the continued delivery of its essential business in the face of disruptions caused by all types of hazards.
- 3. Managing security risks proportionately and effectively enables Defence to provide the necessary protection for Defence assets.

What Is Security and What Are We Securing?

- 4. Security is the protection and preservation of an organisation's assets people, property, information, activities and capabilities from sources of harm that could weaken, compromise or destroy them.
- 5. **Security for Defence personnel**. This includes all defence employees, defence employees engaged locally overseas, defence civilians, defence members and the equivalents from other defence organisations on exchange to Defence, contracted civilians and authorised visitors.
- 6. **Security of Defence property**. The security of all defence property, which includes assets and infrastructure, is critical in order for Defence to conduct its business. Defence's assets include buildings, bases and associated infrastructure, weapons, munitions and explosives, platforms, vehicles and equipment, and ICT infrastructure.
- 7. **Security of Defence information**. Defence's information is saved in hard and soft-copy form and in the minds of our people. Increasingly, this information is accessed and exchanged via information and communications technology (ICT) systems. In addition to safeguarding our own information, Defence has an increasing requirement to access and therefore to protect foreign-sourced information.
- 8. **Security of Defence activities**. Defence's activities include the location and number of operational units and their equipment, personnel, tactics, training, practices, staffing and readiness, intelligence collection, sources and methods, new and potential weapons systems and platforms, and operational support systems.

Defence Security Context Page 2 of 9

- 9. **Security of allies' information, assets and personnel**. When required, Defence has a responsibility to maintain the security of all people, property, information, activities and capabilities of our allies.
- 10. **Security of Defence's Reputation International**. Defence's reputation facilitates the effective and efficient conduct of its functions and allows for the maintenance of constructive relationships with allies. We must protect our reputation and relationships from the potential impacts of inappropriate behaviour, inappropriate release of information and inadequate protection of our assets and capabilities.
- 11. **Security of Defence's Reputation Domestic**. The Australian public must have confidence in a Defence Organisation that is able to sufficiently protect itself and the assets of its allies. Defence must maintain this trust by enacting effective security regimes that enable it to defend Australia and its national interests.

Security From Whom?

- 12. **Threat Groups**. Defence security is designed to counter threats from foreign governments (including Foreign Intelligence Services (FIS)), trusted insiders, terrorist organisations, criminal organisations, issue motivated groups and maverick individuals.
- 13. **Foreign Governments**. Defence needs policies and procedures in place to effectively counter attempts of FIS to compromise security.
- 14. FIS may try to elicit information on Defence capabilities. This information could be used to harm ADF personnel, information and assets or alternatively improve their own defence capabilities. FIS attempts to gain unauthorised access to information at any level can compromise Australia's strategic advantage and alliances. FIS can collect and distribute intelligence that not only impacts their own country's interest but can also severely impact Australian security.
- 15. **Trusted Insiders**. A trusted insider is a current or previous employee who has knowledge of the organisation and how it operates. They have, or did have, access to information and assets, including Defence ICT systems. Motivated by personal reasons, trusted insiders have the capacity to engage in adverse activity, including physical and cyber sabotage.
- 16. **Terrorist Organisations**. Terrorist organisations may use violence, or the threat of violence, against defence personnel and property with the intention of intimidating or damaging the Australian Government; and advancing religious, ideological or political agendas. Terrorism poses a direct threat to Defence's capabilities, operations and assets.
- 17. **Criminal Organisations**. Criminal organisations of numerous configurations have an interest in defence assets. The actions of organisations such as criminal motorcycle groups and cyber-criminal groups directly threaten the security of assets, through:
 - a. corruption of government officials to gain advantage:
 - b. theft of weapons, explosive ordnance and other assets with monetary value;
 - c. theft of personal, financial and commercially important information from IT systems; and
 - d. using malware to sabotage IT systems.
- 18. **Issue-Motivated Groups (IMG)**. IMG pose a threat to Defence through their actions that may seek to inhibit, damage or compromise Defence activities or assets in order to communicate a larger political message. IMG have used a myriad of tactics in the past to inhibit Defence in carrying out its functions, including violence, confrontational tactics (protest), trespass, vandalism, and more recently, cyber-attack and data theft.

Defence Security Context Page 3 of 9

19. **Maverick Individuals**. A maverick individual is an issue-motivated person, possibly a disgruntled exemployee, who sees value in causing disruption. Maverick individuals are generally non-conformists, driven by a particular concern or dispute. They can sometimes be unstable to deal with, act on impulse and may make poor decisions.

Security From What?

- 20. Each of the groups identified above that are deemed a threat to Defence could utilise a range of techniques to threaten Defence capability:
 - a. **Direct attacks on Defence personnel, assets and bases.** Threat groups may utilise direct attacks on Defence, be it through armed attack, cyber attacks, attacks and harassment of defence personnel, or an attack on Defence property, information, activities and capabilities.
 - b. **Security lapses.** Threat groups will look to exploit any non-compliance of security procedures or poor security processes to harm, weaken, compromise or destroy Defence's assets.
 - c. **Trusted Insiders / Maverick Individuals.** Threat groups may identify and exploit Trusted Insiders or Maverick Individuals, either wittingly or unwittingly, to infiltrate Defence systems and harm, weaken, steal, compromise or destroy Defence's assets.

Security by What Means?

What are we securing?

21. The Australian Government/Defence owns a wide variety of assets that require some form of protection against the threat actors described in paragraphs 1.12 to 1.19. For a threat actor to harm Australian Government or Defence assets (including people, information, physical assets, ICT systems and capabilities), there must be some kind of value or importance attached to the asset beyond its dollar value. If there was no other value, there would be no ideological basis for the threat, and therefore no requirement to apply additional protective security. This gives us the concept of a 'security-protected asset' - an asset that requires more than just standard 'fire and theft' protection. See DSM Part 2:7 Business Impact Levels for more information.

What are our assets worth?

- 22. Security-protected assets are 'graded' to show how valuable they are to the Australian Government or Defence. The grading is based on the consequence to Defence capability or the National interest if the assets were to be compromised, lose integrity or become unavailable for use. The grading of an asset is represented by a Business Impact Level (BIL, see Part 2:7) and if required, a classification (consequence of compromise).
- 23. Asset or system owners and information originators will grade the assets they are responsible for and inform users and custodians of this grading by the use of various mediums, including protective markings, Security Classification and Categorisation Guides, and asset databases.

Note: Unless you are an asset owner, you will most likely not be required to assign a BIL for any asset. Asset owners are generally Group Heads and Service Chiefs, or appointed delegates.

24. **Information as an asset**. Information is also an asset. In that context information systems are assigned BILs. These apply to the system itself or the collection of records that it contains. For example, a business critical logistics system will have a high availability requirement in addition to any classification of the data it holds.

Defence Security Context Page 4 of 9

Note: Unless you are a system owner you will most likely not be required to assign a BIL for any ICT system. System owners are generally Group Heads and Service Chiefs, or appointed delegates. However you will in the course of your duties classify the information that you generate. Security Classification and Categorisation Guides assist you in this purpose.

Note: Asset or system owners and information originators should be aware that aggregation of information from a variety of sources can affect the business impacts of a loss of confidentiality, integrity or availability of information in accordance with BILs assessments.

25. To find out more information about the assessment and grading process of assets see DSM Part 2:7 Business Impact Levels and Part 2:30 Classification and Protection of Official Information.

What does the grading tell me as a user or custodian?

26. A BIL or a classification informs a user or custodian of the minimum required levels of protection they must apply, or are recommended to apply, to the asset. They also provide the user or custodian the basis for developing a consequence level for any security risk assessment they conduct.

How are efficient, effective and economical security controls achieved?

- 27. It is a requirement that all custodians conduct a security risk assessment in order to determine the most appropriate security controls to apply to protect the asset. The need to conduct a risk assessment is not only a requirement of the PSPF, but also of the *Public Governance, Performance and Accountability Act* 2013 (Cth).
- 28. Risk assessments are used to determine the most efficient, effective and economic means of protecting an asset and justify whether:
 - a. the minimum prescribed security controls are enough to protect the asset;
 - b. more than the minimum security controls are required to protect the asset; or
 - c. the minimum prescribed security controls are impractical, costly or inappropriate for the asset.
- 29. The protection of assets, information and people are not assessed in isolation of each other within the same unit, facility or base. The overuse of controls can be averted, and financial savings can be made when 'like' assets are aggregated and risk assessed together at a whole-of-facility level.
- 30. To find out more about the security risk assessment process, see DSM Part 1:2 Security Risk Governance [UNDER CONSTRUCTION] and Part 2:2 Security Risk Management and Planning.

What security controls need to be applied?

- 31. Once a security risk assessment is conducted, the asset, system or information custodian has enough information at their disposal to commence applying security controls based on the 'security-in-depth' principle. Security-in-depth uses multiple layers of security measures to enhance protection and reduce the opportunity for unauthorised access to Defence assets. It is based on the premise that a series of protective measures is more robust than a single line of defence. In other words, security-in-depth ensures that our assets are not reliant on any one measure for protection.
- 32. The application of security controls form the bulk of detail within the DSM and are separated into a series of parts based on the core protective security policies of the PSPF and ISM:
 - a. the DSM Part 2:20 series provides information on the application of personnel security controls, including security clearances, temporary access to resources, contact reporting and protected identities;

Defence Security Context Page 5 of 9

- b. the DSM Part 2:30 series provides information on the application of information and administrative security controls, including classifying and information handling (both domestic and foreign sourced), physical transfer of information and assets, and escorting requirements;
- the DSM Part 2:40 series provides information on the application of security controls for the
 procurement of services, the management of projects and the running of the Defence Industry
 Security Program;
- d. the DSM Part 2:50 series provides information on the application of ICT security controls including ICT systems, portable electronic devices, COMSEC and electronic office equipment; and
- e. the DSM Part 2:60 series provides information on the application of physical security controls including access control measures, guarding requirements, asset (including weapons and explosive ordnance) handling and audiovisual requirements.
- 33. **Working with defence industry**. The above requirements are equally applied to external service providers who work for or within Defence. Commanders and managers who are required to engage with external service providers need to be aware of specific industry-related security requirements; for these, see the DSM Part 2:40 series.

Security awareness and monitoring

- 34. Employees must be informed by their commanders or managers on the appropriate application of protective security in their workplace. The DSM is too generic to achieve this, therefore a series of local awareness products are to be used to inform employees, including, but not limited to:
 - a. base/unit/facility security plans see DSM Part 2:2 Security Risk Management and Planning;
 - b. SAFEBASE plans see DSM Part 2:3 SAFEBASE;
 - c. regular security training and awareness briefings see DSM Part 2:5 Security Training and Awareness; and most importantly
 - d. base/unit/facility security standing orders/standard operating procedures see DSM Part 1.0 The Defence Security Manual.
- 35. Commanders and managers have a responsibility to monitor their subordinate's compliance with the security requirements outlined in the DSM. If there are security behaviours of concern, or changes of circumstances regarding their subordinates, it is imperative that supervisors report their concerns to the Australian Government Security Vetting Agency via the prescribed reporting mechanisms, see DSM Part 2:20 *Personnel Security Clearance Process*.
- 36. Individuals also have responsibilities to ensure their ongoing suitability to hold a security clearance. This is a collection of measures that are known as security clearance 'aftercare' and include a responsibility to advise the Australian Government Security Vetting Agency when there are changes to one's personal situation (eg. Martial status, living arrangements, finances etc). As a clearance holder you should also report significant changes in the personal circumstances of other clearance holders where you believe there may be implications for security.

How are controls assessed and accepted?

37. Once controls are applied, security authorities, acting on behalf of the Secretary and CDF, must be satisfied that the application of security controls are adequate enough to deal with the assessed risk against the asset or ICT system. This is done through the application of the accreditation process and the

Defence Security Context Page 6 of 9

engagement of accrediting authorities (which should occur as early as possible), see DSM Part 2:4 Facilities and ICT System Accreditation for further information.

Ongoing compliance and performance assessment

- 38. It is important that security controls are maintained throughout the life cycle of the asset or ICT system. Commanders and managers, as well as security authorities, will assess compliance and performance of protection measures at regular intervals to ensure security controls are still adequate. Intervals are determined by a tiering system; facilities that deal with higher risk assets will be assessed at more frequent intervals than those in lesser tiers. ICT systems are reassessed when they're changed or at regular intervals as ICT controls can degrade quickly. When standards cannot be met, dispensations can sometimes be used to evaluate, approve and document non-compliance or variations within certain parameters. For further information, see DSM Part 2.1 *Dispensations*.
- 39. The results obtained through regular assessment are used to inform those responsible for the security of Defence (including the Secretary and CDF and the Defence Minister) of the state of security in the organisation. The results are also used to inform higher level protective security strategies, which in turn are used to inform security policies and plans. For further information, see DSM Part 1:2 *Defence Security Assurance and Reporting* [UNDER CONSTRUCTION].

What Should Security Culture Look Like?

- 40. In order to have a successful security regime, Defence needs to ensure that its people understand that they all have a role to play in the protection of themselves and their assets, which reinforces the principle that 'security is everyone's business'.
- 41. **Individuals**. At the individual level, all Defence personnel and external service providers play a key role in delivering effective protective security. They need to undertake that role instinctively and continuously. They need to:
 - a. be aware of, and alert to, the principal security treats to Defence responding positively and immediately to any lapse in security they identify as being suspicious, ongoing, unusual or persistent;
 - b. understand their role in responding to security alerts at the current or higher SAFEBASE alert levels:
 - c. report security incidents and suspicious behaviour by anyone in a timely and comprehensive manner; and
 - d. practice good security practice and encourage those around them to do the same.
- 42. **Commanders and managers.** Commanders and managers at all levels set the tone for Defence's security culture. They are to:
 - instil security awareness and a sense of security responsibility in their subordinates;
 - b. understand that security policy does not remove risk, but rather reduces risk to a level that is as low as reasonably practical;
 - c. identify, understand, mitigate and manage the security risks they are responsible for;
 - d. monitor their security environment and proactively adjust risk mitigation measures as appropriate; and

Defence Security Context Page 7 of 9

- e. test and practice security processes and procedures.
- 43. **Senior Leaders**. Senior leaders must recognise protective security as an enabler not an inhibitor of effective business. They are to:
 - a. actively promote security;
 - b. understand the risks that have been accepted by subordinates and the accumulation of risk in their area of responsibility; and
 - c. contribute actively to the implementation, management and monitoring of agreed risk controls.
- 44. Defence's most senior leaders need to be confident that they understand the threats to Defence, have clearly identified where and to what extent risk is to be managed, and ultimately be satisfied the risks have been mitigated to an appropriate level.
- 45. Defence's most senior leaders need to accept that an organisation as complex and dynamic as Defence will not be compliant with all aspects of government policy at all times and need to be willing to accept risk that is managed through a comprehensive risk assessment and management process.
- 46. **Support**. At all levels, Defence's people, and commanders and managers are supported by trained, diligent security specialists, able to dedicate an appropriate level of effort to their protective security tasks. Security specialists are to:
 - a. support commanders and managers at all levels to identify, understand, mitigate and manage their protective security risks in an active and proactive manner;
 - b. build and support a strong security culture;
 - c. ensure security checks and reports are completed in a comprehensive and timely manner; and
 - d. report incidents in a timely manner and support follow-up actions and investigations where appropriate.

Defence Security Context Page 8 of 9

Appendixes and Attachments		
N/A	This part currently has no annexes or attachments	

Defence Security and Vetting Service Intelligent security for an insecure world

Defence Security Context Page 9 of 9



Defence Security and Vetting Service Intelligent security for an insecure world

DSM Supplementary Document

Annex A to DSM Part 1:0 Defence Security Manual					
Version	1	Publication date	9 July 2015	Amendment list	25
Optimised for	Screen; Print; Screen Reader				•
Releasable to	Defence and Defence industry				
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document.				
Copyright	© Commonwealth of Australia 2010 This work is copyright. Apart from any use as permitted under the <i>Copyright Act 1968</i> , no part may be reproduced by any process without prior written permission from the Department of Defence. Requests and inquiries concerning reproduction and rights should be addressed to Defence Publishing Services, Department of Defence.				

Defending Australia and its National Interests www.defence.gov.au



Security Document Hierarchy

- 1. The Defence Security Manual (DSM) receives its mandate from a set hierarchy of documents. The following outlines where the DSM is situated in regards to this hierarchy.
- 2. **Directive on the Security of Government Business.** The Secretary of Defence and the CDF are given specific direction from the Attorney-General to protect Defence's people, information and assets, at home and overseas, through the Directive on the Security of Government Business.
- 3. **Protective Security Policy Framework (PSPF).** The PSPF, which is issued by the Attorney-General's Department and endorsed by Cabinet, is the authoritative source document for protective security policies, principles, standards and procedures to be followed by all Australian Government agencies to protect its people, information and assets, at home and overseas.
- 4. **Information Security Manual (ISM).** The ISM, issued by the Australian Signals Directorate (ASD), is the authoritative source document for ICT security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official information and resources.
- 5. **Cabinet Handbook.** The Cabinet Handbook reflects the discretion the Prime Minister has to organise the management of the Cabinet. The Handbook outlines the underlying principles of Cabinet government and general expectations for Cabinet business and meetings, with detailed arrangements included in its annexes. The Handbook is to be used as a resource for staff involved in the development and progression of Cabinet business. Security related elements of the Cabinet Handbook, particularly the handling and storage of Sensitive: Cabinet information are given policy effect in Defence though the DSM.
- 6. **Defence Security Manual (DSM).** The DSM, issued by the Defence Security and Vetting Service (DS&VS), translates the PSPF and ISM to reflect the Defence context and is the authoritative source document for Defence protective security policy, principles, standards and procedures across Defence and defence industry.
- 7. **Security Standing Orders (SSOs)**. SSOs, issued by commanders and managers, complement the DSM, and are the authoritative source documents for localised protective security policy and procedures for military and business units or Defence Industry Security Program member facilities. It is recommended SSOs comprise security instructions and requirements that are specific to a unit or facility, for example, if required, instructions that detail how a particular DSM requirement is to be implemented in the local unit or facility environment. SSOs are to:
 - a. feature as a part of any security awareness activity associated with induction;
 - b. remain current and readily accessible to all staff;
 - c. not contravene the DSM: and
 - d. accord with applicable security plans (refer DSM Part 2:2 Security Risk Management and Planning).
- 8. The content of SSOs will be highly dependent on each unit or facility's security environment so the DS&VS does not maintain a standard template. However, information that could be included in SSOs includes:
 - a. details of security appointments;
 - b. references to applicable security plans and associated SAFEBASE enclosures;
 - c. internal processes to support overseas travel notification, and contact and incident reporting;

- d. local security briefing requirements for staff;
- e. local access arrangements, including visitor controls;
- f. local clear desk policy, 'close-of-business' checks, lock-up procedures and security key management processes;
- g. localised storage measures for classified information and security-protected assets;
- h. local arrangements for the transfer of classified information, for example identification of registries and Safehand couriers;
- i. specific requirements for the use of laptops and portable electronic devices;
- j. listings of prohibited items, if necessary by building; and
- k. any localised security awareness regime.
- 9. **Security Register.** Security registers complement SSOs. They are designed to capture all matters of security interest relevant to the unit or facility not detailed in the SSOs.

Example: Local requirements for security briefings in SSOs would be supported by the registration of security briefings in a security register. As a further example, SSOs would refer to any local requirements associated with security containers, while the security register would detail the location of security containers and record combination changes.

- 10. The security officer generally maintains the security register on behalf of their commander or manager. It is recommended that commanders and managers inspect the register no less than quarterly to maintain effective oversight of security issues affecting the unit and for which they are responsible.
- 11. The DS&VS maintains a template spreadsheet security register, which is recommended for use and is available for download here (Security Register), on the DS&VS intranet site and on the Defence Online Service Domain portal for defence industry. The template is divided into numerous worksheets covering a range of data capture topics that are recommended as part of any security register.

Annex A to DSM Part 1:0 Page 3 of 4

Appendixes and Attachments		
N/A	This part currently has no annexes or attachments	

Defence Security and Vetting Service Intelligent security for an insecure world



Defence Security and Vetting Service Intelligent security for an insecure world

Defence Security Manual

DSM Part	1:0 Defence Security Manual				
Version	5	Publication date	9 July 2015	Amendment list	25
Optimised for	Screen; Print; Screen	Reader			
Releasable to	Defence and Defence	industry			
Seeking Advice	For further advice on any aspect of DSM policy, click on the following link: http://spintranet.defence.gov.au/dsa/policy-and-advice/Pages/psac.aspx				
Copyright	© Commonwealth of Australia 2010 This work is copyright. Apart from any use as permitted under the <i>Copyright Act 1968</i> , no part may be reproduced by any process without prior written permission from the Department of Defence. Requests and inquiries concerning reproduction and rights should be addressed to Defence Publishing Services, Department of Defence.				

Introduction

- 1. The Australian Government's policy on protective security is promulgated in the *Australian Government Protective Security Policy Framework* (PSPF) and the *Australian Government Information and Security Manual* (ISM). The PSPF and the ISM are the source of the security principles and set out the minimum standards to which all Australian Government agencies, including Defence, must adhere.
- 2. The *Defence Security Manual* (DSM) is the publication which implements in Defence and defence industry the minimum standards of the PSPF and the ISM. It has been designed as an online manual that is responsive to changes in the protective security requirements in these documents. It also provides additional Defence-specific minimum security standards and guidance where there is no whole-of-government equivalent.
- 3. The DSM as Defence's security manual puts the PSPF and ISM into a Defence context when implementing Government security policy within Defence. Any conflict between the manuals should be raised with the Defence Security and Vetting Service (DS&VS) as Defence may have chosen to implement a differing or additional security standard that is more appropriate to Defence's business requirements or security risk profile while still meeting the intent of government policy.¹
- 4. The DSM is used by commanders and managers at all levels to manage risk through security processes and procedures that meet their specific business needs and address security risks in a pragmatic and flexible way. The DSM describes the protective security policies, principles and standards to be followed by Defence personnel and by external service providers under contract.
- 5. Defence's protective security policy and governance arrangements described in the DSM provide the framework for a systematic and coordinated approach to security risk management and security-in-depth. The DSM was developed in consultation with security stakeholders.
- 6. Further explanation of the security document hierarchy is provided in annex A.

Policy Statement

- 7. In support of the Australian Government, Defence will establish protective security objectives and employ protective security measures to safeguard its people, capabilities, assets and mission. Defence's protective security objectives are to:
 - a. protect Defence's people from harm;
 - b. protect Defence information, assets and infrastructure against unauthorised access, sabotage, wilful damage, theft or disruption;
 - c. ensure that only loyal, reliable and trustworthy persons who have an established need are permitted access to classified Defence information and security-protected assets;
 - d. prevent unauthorised disclosure of classified information, whether deliberate or accidental; and
 - e. protect the information and assets of other nations in accordance with security agreements and obligations between Australia and those nations.

DSM Part 1:0 Page 2 of 8

¹ Where the DSM departs from a PSPF or ISM standard in order to meet Defence specific requirements this will be noted in the DSM.

- 8. To achieve its protective security objectives, Defence will:
 - apply a systematic and coordinated approach to managing security risks based on the policies and practices outlined in the PSPF, ISM, DSM, ADF security doctrine and any relevant legislation;
 - b. ensure that planning against security risks forms part of its culture by integrating it into Defence's policy, practices, training, and strategic and organisational goals;
 - c. ensure that security awareness forms part of all employees' induction, and ongoing security awareness is included as part of their performance assessments;
 - conduct security reviews and planning that are based on comprehensive, current and reliable information;
 - ensure that security risk planning and treatment are focused on areas where there is a significant risk identified through current security reviews and incident reporting;
 - f. ensure that protective security plans provide treatments that are appropriate to the level of risk and are cost-effective; and
 - g. monitor and assess its operating environment and protective security treatments on a regular basis.

Definitions

9. Definitions are included in each DSM part and within the Glossary.

Sponsorship

10. All chapter parts within this manual are sponsored by the Defence Intelligence and Security Group.

Roles and Responsibilities

- 11. An overview of key strategic roles and responsibilities for protective security in Defence are detailed in DSM Part 1:1The Defence Security Organisation. Each DSM part also specifies detailed roles and responsibilities relevant to that topic.
- 12. The Secretary of Defence and the Chief of the Defence Force (CDF) have designated the First Assistant Secretary Security and Vetting Service (FASS&VS) as the Agency Security Adviser (ASA) for Defence. In this role, the FASS&VS must perform all of the responsibilities mandated of an ASA by the PSPF. The FASS&VS is responsible for ensuring that Defence's protective security policies and practices within the DSM remain valid and aligned with the PSPF and ISM. The FASS&VS is also responsible to ensure the DSM supports Defence's mission.

Delegations

13. Information regarding the delegation of protective security responsibilities is detailed in DSM Part 1:1The Defence Security Organisation.

Implementation

14. Each Group Head and Service Chief is responsible and accountable for the management of protective security within their Group or Service. They are to ensure that all processes and procedures required for the

DSM Part 1:0 Page 3 of 8

effective implementation of the DSM and the ISM within their Group or Service are clearly promulgated in appropriate instructions, guides, manuals, standing orders and standard operating procedures (SOPs) within 12 months of the DSM or ISM being issued or any part amended.

Note: Groups and Services should refrain from quoting or re-stating requirements of the DSM or ISM in lower level policy, procedures and standing orders. Lower level documents should reference the DSM or ISM in order to permit ease of updating.

15. Commanders and managers are responsible and accountable to their Group Head or Service Chief for the implementation of protective security policy in their military or business units and, through contractual provisions, the implementation of policy by external service providers with whom they have a contractual relationship.

Authority

16. The DSM is authorised in accordance with Defence Instruction (General) ADMIN 20-29 – *Defence Security Manual* (signed 21 May 2010), and is issued with the authority of the CDF and the Secretary of the Department of Defence pursuant to section 9A of the *Defence Act 1903* for members of the Australian Defence Force, and with the authority of the Secretary pursuant to section 20 of the *Public Service Act 1999*, for Department of Defence Australian Public Service employees.

Applicability and Enforceability

- 17. DI(G) ADMIN 20-29 imposes requirements that must be complied with in this manual, a breach of which may result in disciplinary measures being taken (and in the case of external service providers, giving rise to the possibility of breach of contract). Mandatory requirements of this manual are identified in accordance with the section *Compliance Requirements* below.
- 18. In accordance with the DI(G), the mandatory requirements of this manual constitute a general order to Defence Members for the purposes of the *Defence Force Discipline Act 1982* (DFDA). Non-compliance with any mandatory requirement may result in disciplinary action being taken in accordance with the DFDA. In addition, the requirements contained in the DI(G) are also intended to have effect as a direction to Defence employees by the Secretary for the purpose of s13(5) of the *Public Service Act 1999* (s 13(5) forms part of the *APS Code of Conduct*). As a result, non-compliance by Defence Employees with any mandatory requirement in this manual may be referred for investigation and possible sanction in accordance with Public Service Act 1999. The DI(G) also provides that, Defence personnel who award or manage contracts must include the requirement that external service providers must comply with the mandatory requirements of the manual in the terms of the contract, where the manual is directly relevant to the work the external service provider is performing in Defence. Failure by an external service provider to comply with the mandatory requirements of this manual may result in a breach of contract.

Referencing of ISM Controls

- 19. The DSM gives effect to the ISM as the source of ICT security policy within Defence. ISM content is not duplicated in the DSM unless there is a specific reason for doing so. The DSM does, however, contain references to some specific ISM controls in order to draw the reader's attention to their obligations under the ISM. Where references occur, the ISM control number is referred to in short form, for example ISM Control (1204). It is recommended that readers refer to the latest published version of the ISM for the complete control. ISM control numbers remain consistent across ISM versions. References to an ISM control always refer to the latest updated version of the control.
- 20. In some instances, the DSM modifies the content of an ISM control and replaces it with a Defence compliance requirement of a differing standard in order to meet Defence's business requirements or risk tolerance. Where this occurs, the ISM control is revoked by the phrase; *'This DSM compliance requirement replaces in entirety ISM Control (XXXX)*. The revocation of an ISM control by the DSM occurs under the

DSM Part 1:0 Page 4 of 8

authority of the Secretary. If the DSM standard is lower than that presented in the ISM, it is the equivalent of an ISM dispensation against the implementation of the specified control within Defence. A dispensation need not be submitted in these instances.

Compliance Requirements

21. Mandatory requirements in the DSM and ISM are identified through the use of the terms **must** / **must not** and **should** / **should not**. Compliance with these requirements is mandatory. Non-compliance is a reportable security incident, unless the appropriate authority has considered the justification for a policy exception and accepted the associated risk through the granting of a dispensation.

Note: Dispensations are used to evaluate, approve and document policy exceptions to the mandatory minimum standards of the DSM and the ISM. Failure to obtain a dispensation when required is a failure to manage security risk. For further information regarding dispensations, see DSM Part 2.1 *Dispensations*.

- 22. Within Defence, the authority to approve a policy exception to a DSM or ISM requirement through the granting of a dispensation is as follows:
 - a. Non-compliance with **must** / **must not** requirements represents a high risk to agency people, information, assets, facilities and ICT systems. Unless otherwise specified in the DSM, through the use of a dispensation indicator, policy exceptions to:
 - (1) a Non-ICT must / must not requirement are to be approved by the relevant Group Head, relevant Service Chief or an appointed delegate no lower than the level of SES Band 1/O-7; and
 - (2) an ICT-related must / must not requirement are to be approved by the Secretary, following consultation with the relevant ICT Accreditation Authority. If the requirement is derived from an ISM control labelled 'ASD', Director ASD's approval is also required. This DSM compliance requirement replaces in its entirety ISM Control (0001).
 - b. Non-compliance with should / should not requirements represents a medium to low risk to agency people, information, assets, facilities and ICT systems. Unless otherwise specified in the DSM, through the use of a dispensation indicator, policy exceptions to:
 - a Non-ICT should / should not requirement is to be approved by a commander or manager; and
 - (2) an ICT-related should / should not requirement is to be approved by the relevant Group Head, relevant Service Chief or an appointed delegate no lower than the level of SES Band 1/O-7 following consultation with the relevant ICT Accreditation Authority. This DSM compliance requirement replaces in entirety -ISM Control (1061).
 - c. Where the authority to approve a policy exception in the DSM departs from the requirements specified in paragraphs a. and b. above, due to whole-of-government protective security policy requirements or departmental security risk governance arrangements, the mandatory requirement will be separately marked with a dispensation indicator identifying the appropriate approving authority. The indicator is in the form [Auth: XXXX].
 - (1) Some dispensations cannot be further delegated and remain with the assigned position. Such dispensations are marked with the dispensation indicator [Auth: XXXX, No Delegate];

Example: [*Auth: Sec*] is used to denote where the Secretary of Defence is the appropriate approving authority, but this authority may be delegated, [*Auth: DepSec DSR, No Delegate*] indicates that only the DepSec DSR may approve the dispensation.

DSM Part 1:0 Page 5 of 8

- d. Where a policy exception to a mandatory requirement cannot be authorised, due to obligations imposed by whole-of-government protective security policy, legislation or departmental security risk governance arrangements, the mandatory requirement will be separately marked with a dispensation indicator [Auth: None] indicating that compliance is mandatory in every instance except emergency non-compliances.
- e. 'Recommend' and 'may' are used to denote a sensible protective security practice. While policy exceptions do not need to be documented or approved, they should be informed by sound risk management principles.
- 23. The DSM includes non-mandatory guidance for the benefit of protective security practitioners. As there is no requirement to comply with non-mandatory guidance, it does not use the compliance terminology detailed at paragraph 21. Unless otherwise indicated, the language used in DSM guidance is subject to the standard dictionary definition.2

Monitoring and Reporting

24. Under the PSPF, Defence is required to implement a protective security monitoring and ministerial reporting scheme to ensure the effectiveness of protective security measures within the department. The effectiveness of the DSM is monitored under that scheme as detailed in DSM Parts 1:2 Security Risk Governance and 1:3 Security Assurance and Reporting [BOTH UNDER CONSTRUCTION].

Related policy and legislation

25. Related legislation, internal and external conformance documents are detailed in the 'Related Policy and Legislation' section on the DSM website.

DSM Amendment

Release and review dates

26. The DSM is a living document which is reviewed and updated on an 'as required' basis. Each DSM Part carries a separate amendment number and date of effect. It is anticipated that all parts will be updated at least every three years. However, consistent with SODI processes, each DSM part will be reviewed at least every five years from the date of last amendment. DSM amendment release dates and mandatory SODI review dates for each part are listed in annex B.

Change authorisation

- 27. The DSM requires amendment from time-to-time due to a range of factors. A change authorisation matrix, found at annex C, provides a rigorous and transparent framework for determining the consultation and approval authorities for new or amended policies. The matrix is based on an assessment of:
 - a. the anticipated change in Defence's risk exposure resulting from the expected policy outcomes;
 - the magnitude of organisational change required to effect and sustain policy implementation;
 and
 - c. associated workforce and financial implications.

DSM Part 1:0 Page 6 of 8

_

² The Macquarie Dictionary.

Note: Further information regarding consultation and approval authorities can be found in DSM Part 1:1 *The Defence Security Organisation*.

Proposal for amendment

- 28. Proposals to amend a DSM part are to be supported by evidence of multiple dispensation requests that pertain to the policy. The presence of numerous dispensations against a policy part provides the strongest feedback for the need of a policy change.
- 29. Proposals for DSM amendments that are 'Routine' and above are to be forwarded to Defence Security Advisory Group (DSAG) representatives for the relevant Group or Service. The DSAG will assess your request for a policy change in consultation with stakeholders and, if appropriate, may have the matter placed in the DSAG agenda. Amendments considered 'Incidental' may be forwarded to the DS&VS; see the Defence Security Portal for further information: http://intranet.defence.gov.au/security/dsm/dsm_contacts.html.

Publishing of amendments

30. Amendments to the DSM will be published on the DSM webpage via an 'amendment list'. The amendment list itself can be obtained on the DSM homepage and from a hyperlink at the beginning of each DSM Part. Amendment lists will be announced formally via a DEFGRAM, and informally using the security community network.

Archiving old DSM parts

31. The DSM part(s) subject to amendment will be given an updated version number located at the beginning of each part. Old versions of each part will be archived and are available for viewing here: http://intranet.defence.gov.au/dsa/dsm/archive/index.html

Annexes and Attachments			
Annex A	Security document hierarchy (current version published on 9 July 2015)		
Annex B	DSM amendment release and review dates (current version published on 9 July 2015)		
Annex C	DSM change authorisation matrix (current version published on 9 July 2015)		

Defence Security and Vetting Service Intelligent security for an insecure world



Defence Security and Vetting Service Intelligent security for an insecure world

Defence Security Manual

DSM Part	2:20 Personnel Security Clearance Process				
Version	7	Publication date	16 September 2016	Amendment list	27
Optimised for	Screen; Print; Scree	n Reader			
Releasable to	Defence, Defence I	ndustry			
Compliance Requirements	contract may be, bor (ISM). Failure to con action under the release force Discipline Act Mandatory requirem must not and should the appropriate autheither accepted the apermanent alternative. The terms 'recomme compliance need no sound risk materials.	Defence personnel are, and external service providers subject to the terms and conditions of their contract may be, bound by security policy contained in the DSM and Information Security Manual (ISM). Failure to comply with the mandatory requirements of the DSM and ISM may result in action under the relevant contract provision or legislation including, but not limited to; the <i>Defence Force Discipline Act 1982</i> , the <i>Public Service Act 1999</i> , and the <i>Crimes Act 1914</i> . Mandatory requirements in the DSM and ISM are identified through the use of the terms must / must not and should / should not . Compliance with these requirements is mandatory unless the appropriate authority, if applicable, has considered the justification for non-compliance and either accepted the associated risk through the granting of a dispensation, or has accepted a permanent alternative process which meets the intent of the DSM. The terms 'recommend' and 'may' are used to denote a sensible security practice and non-compliance need not be approved or documented. Note: Non-compliance with a sensible security practice ought to be informed by sound risk management principles. The DSM compliance regime is detailed in DSM Part 2:1 <i>Dispensations</i> .			
Copyright	© Commonwealth of Australia 2010				
	no part may be repro Department of Defer	oduced by any proc nce. Requests and	se as permitted under ess without prior writte inquiries concerning re ces, Department of De	en permission from the production and rights	e

Introduction

- 1. The security clearance process forms part of the Defence protective security framework and ensures that only those people recognised as suitable, obtain and retain access to security classified information and assets.
- 2. The vetting process is a subset of the security clearance process that is used to assess the suitability of an applicant to hold and maintain a clearance. Vetting for Defence and non-exempt agencies is undertaken by the Australian Government Security Vetting Agency (AGSVA). AGSVA conducts vetting in accordance with the Protective Security Policy Framework (PSPF), Interagency Agency Security Forum (IASF) guidelines and bulletins, and AGSVA internal vetting procedures.
- 3. The purpose of Defence Security Manual (DSM) Part 2:20 is to detail the management and administration of security clearances.

Policy

4. Defence personnel and external service providers are to be security cleared to the level commensurate with the level of classified information or assets they are required to access, or the responsibilities they hold.

Process

Security clearance levels

- 5. The four levels of personnel security clearances issued under the PSPF are:
 - a. **Baseline**: permits ongoing access to Australian Government information and assets that are security classified up to and including PROTECTED;
 - b. **Negative Vetting Level 1** (NV1): permits ongoing access to Australian Government information and assets that are security classified up to and including SECRET;
 - c. **Negative Vetting Level 2** (NV2): permits ongoing access to Australian Government information and assets that are security classified up to and including TOP SECRET; and
 - d. **Positive Vetting** (PV): permits access to information and assets at all classification levels. This includes access to certain types of caveat and codeword information that require a PV as prerequisite for access.

Note: Clearance requirements for CHARLIE, DELTA, ECHO and GAMMA compartments are contained in DSM Part 2.30 *Classification and Protection of Official Information*

- 6. The former clearance levels issued by Defence were:
 - a. Entry Only: A basic security check that permitted access to a specified Defence base or establishment, but did not grant access to official information;
 - b. RESTRICTED: permitted ongoing access to Australian Government information and assets that are security classified up to RESTRICTED;

Note: A RESTRICTED clearance now permits access to PROTECTED information within Defence and Defence industry under a waiver issued by the Secretary. See below for transition arrangements.

DSM Part 2:20 Page 2 of 26

- c. CONFIDENTIAL: permitted ongoing access to Australian Government information and assets that are security classified PROTECTED and CONFIDENTIAL;
- d. SECRET: permitted ongoing access to Australian Government information and assets that are security classified up to and including SECRET;
- e. TOP SECRET NV: permitted ongoing access to Australian Government information and assets that are security classified up to and including TOP SECRET;
- f. TOP SECRET PV: permitted access to Australian Government information and assets at all classification levels, including certain types of caveat and codeword information.
- 7. The following table summarises how the former clearances are recognised by AGSVA.

Table 2:20-1: AGSVA Recognition of Former Clearances

Former Clearance Level	Current Clearance Level
ENTRY ONLY	No longer recognised
RESTRICTED	Transition arrangements apply (see below)
PROTECTED	Automatically recognised as Baseline
CONFIDENTIAL	Transition arrangements apply (see below)
HIGHLY PROTECTED	Transition arrangements apply (see below)
SECRET	Automatically recognised as NV1
TOP SECRET NV	Automatically recognised as NV2
TOP SECRET PV	Automatically recognised as PV

Transition Arrangements for RESTRICTED Clearance Holders

- 8. The Secretary has issued a waiver permitting all RESTRICTED clearance holders access to PROTECTED information and systems in the course of their Defence duties.
- 9. This waiver allows Defence and Defence industry personnel, who currently hold RESTRICTED clearances, access to PROTECTED systems and intermittent access to PROTECTED information within Defence. The waiver covers all Defence employees, including Australian Public Servants (APS), Australian Defence Force (ADF) members, ADF Reserve members, contractors, secondees and locally engaged staff.
- 10. As a result of the waiver, existing employees with a RESTRICTED clearance are not required to upgrade to a BASELINE clearance unless, due to changed circumstances, the RESTRICTED clearance holder requires a security clearance review or a higher clearance.
- 11. It is recommended that supervisors identify personnel who require regular and ongoing access to PROTECTED information to fulfil their duties and request a clearance upgrade from RESTRICTED to BASELINE.

Note: A decision to upgrade from RESTRICTED to BASELINE should be made with respect to the actual information the employee needs to access, not on the basis of needing to access a PROTECTED network.

- 12. For contractors, the waiver only applies to access to PROTECTED information and systems associated with their employment contract with Defence. Contractors who work for multiple departments may be required to undertake a BASELINE clearance if their work with those departments brings them into contact with PROTECTED information or systems.
- 13. Defence employees permanently transferring to another department will be required to upgrade from RESTRICTED to BASELINE if access to PROTECTED information is required.
- 14. In the case of Defence employees being temporarily seconded to another department, prior agreement should be sought from the gaining department with regard to the recognition of a RESTRICTED clearance within the gaining department. The gaining department is not obliged to grant access to their PROTECTED material and may request a secondee to undertake an upgrade to BASELINE.

Transitional Arrangements for CONFIDENTIAL and HIGHLY PROTECTED Clearance Holders

- 15. Existing CONFIDENTIAL clearance holders **must** [Auth:None] upgrade to NV1 upon scheduled revalidation or transfer to a new position within Defence that requires access to information classified up to and including SECRET.
- 16. Existing HIGHLY PROTECTED clearance holders requiring access to information classified up to and including SECRET **must** [Auth:None] upgrade to NV1 on employment with Defence.

Note: Defence did not issue HIGHLY PROTECTED clearances; therefore this will only affect employees and contractors transferring from other agencies.

Determining the Requirement for Security Clearances

17. The number of people who require clearances to perform their work should be kept to a minimum. It is a managerial decision as to which duties and tasks require a position to have access to security classified information and assets and therefore require the person filling the position to hold a security clearance.

ADF and APS

18. As a condition of service, all new APS employees are required to gain and maintain a minimum of a BASELINE security clearance and all new ADF members are required to gain and maintain a minimum of an NV1 security clearance.

Note: Existing employees are bound by their original terms of engagement.

Contracted Employees

19. Due to the breadth and scope of outsourced activities, there is no minimum clearance requirement for contractors. Clearance requirements for contractors are determined by Defence contract managers on the basis of their need to access classified information, networks, assets or secure areas.

Standing Offer Panels

20. Where the relationship between Defence and a panel member has been formalised through a Deed of Standing Offer; the Panel manager will determine the requirement and sponsor clearances for personnel employed by panel companies.

Potential Suppliers

21. Identification as a potential supplier under a limited tender process (including sole supplier) establishes a business relationship between that potential supplier and Defence. The Defence Request For Tender (RFT) manager will determine the requirement and sponsor clearances for personnel employed by that potential supplier.

DSM Part 2:20 Page 4 of 26

Potential Industry or Academic Partners

- 22. Defence recognises other forms of business relationships with industry and academic partners. FAS S&VS will accept formal notification from a 2 Star / SES band 2 Officer that such a relationship exists. That formal notification is to include:
 - a. the nature of the relationship and rationale for requiring clearances; and
 - b. a management plan for sponsorship and maintenance of those clearances.
- 23. FAS S&VS will consider such requests and where approved, will provide a sponsorship number for the requesting organisation to use in lieu of a contract number.

Capability Development and Organisational Change

- 24. The granting and management of security clearances represents a considerable cost to the department. In order for AGSVA to remain responsive to Defence requirements, changes to the number and level of security clearances required across Defence are to be considered during capability development processes and the development of Net Personnel Operating Cost (NPOC) estimates.
- 25. Where the introduction of a new capability or other organisational change will result in a requirement for large numbers (50+) of new clearances or upgrades to existing clearances across a Group or Service, the originating area **must** [Auth:None] advise and consult Assistant Secretary Vetting (ASV) on the increased vetting throughput requirements and NPOC considerations.
- 26. Group Heads and Service Chiefs are required to annually forecast their vetting demand or confirm that no significant change in vetting requirements is anticipated. Groups and Services should consult AGSVA to quantify the resources required by AGSVA to meet the expected demand.

Note: The demand forecast should be updated when circumstances identify that a change in the number, or a change in the profile of clearances across their Group or Service will occur.

Staff churn through posting, resignation, reassignment or other routine personnel movement will generate requests for vetting of replacement personnel. This is considered to be business as usual and does not constitute a change requiring notification to the AGSVA.

Line Managers and Unit Commanders are to consider how a small number of changes within their area of responsibility will contribute to the cumulative requirements for their Group or Service. All changes should be reported through Group or Service channels to enable development of requirement forecasting.

Example: Changes could occur due to the planned introduction of a new capability, an organisational change, or a shift in the threat environment. If new positions requiring security clearances are created or if a group of existing personnel will require a security clearance upgrade to work in a new organisational structure; the AGSVA is to be advised as soon as is practical.

Determining the Requirement for NV1 and NV2 Clearances

- 27. All positions requiring a security clearance above BASELINE are managed as Designated Security Assessment Positions (DSAP).
- 28. In assessing the applicability of a DSAP, a commander or manager, or contract manager **must** [Auth: None] decide which positions and associated roles entail duties that can only be performed with access to security classified information and assets classified CONFIDENTIAL or above.

Note: Access to CONFIDENTIAL information and assets is used as the minimum requirement for assessing the applicability of DSAP because the clearance required to access CONFIDENTIAL information, NV1, also permits access to SECRET information.

DSM Part 2:20 Page 5 of 26

29. Even where access to security classified information or assets is not required, some individuals may work in positions of high responsibility, and may have delegations and duties that, if mishandled or abused, could cause Defence considerable harm or reputational damage. These may include personnel whose duties require them to have wide-ranging, highly discretionary access that provides them with the ability and opportunity to cause extensive harm, particularly where the potential for undetected wrongdoing is high or may take significant time to become evident. Positions meeting this criterion **must** be identified as a DSAP and the supporting rationale or risk assessment **must** be recorded.

Example: Defence policy requires a NV1 security clearance if a person independently accesses bulk explosive ordnance. In this instance the DSAP will be NV1 and the duties of the position should record that the clearance is required for independent access to bulk explosives. For further information on this policy see DSM Part 2:67 *Explosive Ordnance Security*.

30. If there is dispute about the relevance of a DSAP to the duties of a position this should be addressed through line management with resolution to be sought at the lowest practicable level. If resolution can not be achieved, the matter **must** [Auth:No Delegate] be referred to the relevant Group Head or Service Chief for resolution.

Determining the Requirement for PV Clearances

- 31. PV is the highest level of clearance issued by the Government. PV clearances are expensive, time consuming and highly intrusive to the applicant. The requirement to gain and hold a PV clearance is governed by employment in an intelligence agency, or the proven requirement to access:
 - a. CODEWORD material;

Note: Clearance requirements for CHARLIE, DELTA, ECHO and GAMMA compartments are contained in DSM Part 2:30 *Classification and Protection of Official Information*

- b. Special Cryptographic Access refer to DSM Part 2:53 Communications Security;
- c. operations that require a PV as a prerequisite for access;
- d. TOP SECRET ICT systems;
- e. specified assets and capabilities; and
- f. specified intelligence collection and exploitation methods and techniques.
- 32. It is recommended that all PV requests are strictly assessed and vetted by commanders and managers. They should only be progressed if a clear requirement can be identified, and if a lower level clearance would not provide adequate access to the required information.
- 33. All applicants for a PV require sponsorship. The PV sponsor **must** [Auth:None] assess whether the position the applicant currently or will occupy meets the criteria above.
- 34. PV clearances **must** [Auth:None] be sponsored by one of the following authorities or their delegate:
 - a. Secretary of Defence;
 - b. Chief of the Defence Force (CDF);
 - Vice Chief of the Defence Force (VCDF) or delegate at the 2 Star / SES band 2 level within VCDF group;
 - d. Deputy Secretary Strategic Policy & Intelligence (DEPSEC SP & I);

- e. Director Australian Geospatial-Intelligence Organisation (AGO) for AGO personnel, nominated personnel supporting the GEOINT mission, or as defined by the Intelligence & Security Group Psychological Assessment Policy;
- f. Director Defence Intelligence Organisation (DIO) for DIO personnel, nominated personnel supporting the Intelligence Assessment mission, or as defined by the Intelligence & Security Group Psychological Assessment Policy;
- g. Director Australian Signals Directorate (ASD) for ASD personnel, nominated personnel supporting the SIGINT mission, or as defined by the Intelligence & Security Group Psychological Assessment Policy;
- h. Chief Joint Operations (CJOPS) for Headquarters Joint Operations Command (HQJOC) personnel and personnel deploying operationally;
- i. First Assistant Secretary Security and Vetting Service for DS&VS staff only;
- j. Chief of Navy for limited Navy personnel categories only; and
- k. Chief of Air Force for Air Force personnel, with the exception of those that require sponsorship under (d), (e), (f), (g) and (h) above.
- 35. Defence Intelligence Security (DIS) manages requests for PV sponsorship on behalf of DAGO, DDIO and DASD. DIS will consider the sponsorship of PV clearances for Defence and government personnel who directly support the GEOINT, Assessment, or SIGINT mission. If this is not the case, the commander or manager is to seek sponsorship for the clearance subject from one of the other listed sponsors in accordance with their command or line management structure.

Transfer of PV Sponsorship

36. The PV Sponsor **must** notify the AGSVA when a PV holder in their area of responsibility moves to another Group or Service, leaves Defence or no longer requires a PV clearance.

Note: A notification lead time may be required for transfers to AGO, DIO or ASD to facilitate any additional vetting requirements.

Example: If a RAAF PV sponsored employee was transferring to ASD, RAAF would advise DIS, as early as possible, of the intention to transfer sponsorship, triggering any additional vetting requirements to be initiated by ASD. On the satisfactory completion of any additional vetting requirements, ASD would undertake full sponsorship of the RAAF employee and, RAAF would notify AGSVA of the transfer of PV Sponsorship.

Example: If a AGO PV sponsored employee was transferring to another Group or Service, leaves Defence or no longer requires a PV clearance, AGO would notify AGSVA that the employee no longer requires an AGO sponsored clearance and AGSVA would cease the clearance. If a gaining agency requires the clearance to be reactivated, the gaining agency would submit a clearance request via the Security Officer dashboard. AGSVA then conducts the necessary checks prior to reactivating a clearance.

Reviewing Clearance Requirements

- 37. The ongoing maintenance of a security clearance costs the Government time and resources. Commanders and managers are responsible for the efficient and effective use of resources, therefore they **must** [Auth:None] review their DSAP to determine if the level of clearance is still warranted for each position in the following circumstances:
 - a. when the duties of the position change;

DSM Part 2:20 Page 7 of 26

- b. prior to commencing advertising or other recruitment actions for a vacant position;
- for clearances granted to permit access to secure areas, when the physical location of the position changes; and
- d. before the current occupant's security clearance is revalidated.

Note: AGSVA requires confirmation of the subjects continuing need to hold a clearance before commencing a revalidation.

38. It is recommended that DSAP positions be reviewed annually to confirm the holder of the position still requires the requisite clearance to perform the duties of the position.

Initiating or Modifying a Security Clearance

Privacy Considerations

- 39. Information collected during the security clearance process is subject to the *Privacy Act 1988* and *Freedom of Information Act 1982*. While security officers and commanders and managers may assist in security processes, they generally do not have a right to access a clearance subject's personal information supplied to AGSVA.
- 40. Consistent with requirements of the *Privacy Act 1988*, AGSVA may supply commanders and managers with limited personal information necessary to risk manage an employee's individual security circumstances. Commanders and managers in receipt of such information are required to comply with the provisions of the *Privacy Act 1988* when handling this information. In particular they **must not** [Auth:None] disclose such information to third parties who are not directly involved in the management of the employee's security circumstances. Advice should be sought from AGSVA prior to disclosing such information to third parties.
- 41. In accordance with the *Freedom of Information Act 1982*, clearance subjects and clearance holders may access information they have provided as part of the security clearance process by contacting AGSVA.

Requesting a New Clearance

- 42. Before initiating the clearance process, the respective commander or manager is responsible for ensuring that:
 - a. APS or ADF recruitment checks are complete and a letter of offer, subject to the person obtaining the required clearance, has been issued;
 - b. the individual is an Australian citizen;

Note: If a clearance subject is not an Australian citizen refer to the section on *Security Clearances* for Foreign Nationals below.

Note: If the clearance subject is a former member of the armed forces of the UK, US, Canada or NZ and has enlisted in the ADF under the government to government 'ADF lateral recruit' program and whose Australian citizenship is pending, the security clearance process can be initiated;

- c. the security clearance level of the position is current and appropriate to the duties of the position; and
- d. the individual does not already hold an appropriate security clearance.

Note: Clearances that are granted under a Citizenship or Uncheckable Background Eligibility Waiver are not automatically transferable between departments, positions within a department or duties within a position. In these cases, the waiver and risk assessment are to be reviewed.

DSM Part 2:20 Page 8 of 26

- 43. If the applicant advises that they hold a current clearance, the commander or manager **must** [Auth:None] confirm the level of clearance currently held by the individual. In the first instance, clearance details should be confirmed on PSAMS2 via the security officer. If difficulties are experienced confirming clearance details, contact AGSVA prior to initiating a new clearance request.
- 44. As soon as the requirement for a new or upgraded clearance is identified, the relevant commander or manager **must** [Auth:None] request a vetting pack be sent to the clearance subject.

Former Clearance Holders

45. If the clearance subject advises that they have previously held the appropriate level of security clearance, the sponsor may request that AGSVA determine if the clearance can be reactivated. AGSVA may seek further information from the subject or commander or manager in order to determine if a clearance can be reactivated.

Note: In general, recently active clearances can be recognised by AGSVA, eg, where a clearance has recently lapsed due to a short break in employment.

46. If AGSVA does not reactivate the clearance, the commander or manager **must** [Auth:None] request a new security clearance.

Exempt Agency Clearance Holders

47. A small number of Commonwealth agencies, other than AGSVA, is authorised to issue security clearances. These clearances are recognised by Defence. Confirmation and transfer of clearance is sought via AGSVA.

Note: Secrecy provisions apply to the identification of former and serving members of ASIO and ASIS and a number of other agencies. Publicly identifying holders of clearances granted by exempt agencies may constitute an offence under the relevant legislation.

Upgrade or Downgrade of a Security Clearance

- 48. If a clearance holder moves to a position requiring a higher level of security clearance, the commander or manager **must** [Auth:None] request a new security clearance.
- 49. If a clearance holder moves to a position at a lower security clearance level, or a non-DSAP role within the same organisation, then the losing commander or manager **must** [Auth:None] request a downgrade of the individual's security clearance to the applicable level.

Exclusion: ADF personnel management policy may require a minimum clearance to be maintained for ADF members in particular employment categories in order to meet readiness requirements. In these circumstances a higher level clearance may be maintained provided the member remains in the specified employment category.

50. If the employing area has any security concerns that lead to a clearance holder being moved to a position requiring a lower security clearance, or having duties temporarily or permanently reassigned, then the commander or manager **must** [Auth:None] notify AGSVA of the basis of the security concerns at the earliest opportunity. Where duties are reassigned as a result of security concerns the employing area **should** initiate a review for cause. Further information on reviewing the suitability of a clearance holder is contained in the section on *Managing Clearance Holders* below.

Failure by a Clearance Subject to Provide Required Vetting Information

51. Non-compliance with the clearance process may delay the granting of initial and upgrade clearances and, in some cases, prevent the revalidation of clearances. Defence and AGSVA take very seriously non-compliance with the security clearance process. Clearance subjects who fail to provide information within the

DSM Part 2:20 Page 9 of 26

stipulated timeframe without reasonable grounds may not be granted a clearance or have a current clearance revoked.

- 52. Compliance timelines are notified to the applicant in their clearance pack. A request for an extension of time to complete the pack may be sought from AGSVA by the clearance subject's commander or manager. The request is to outline the reasons the extension is sought.
- 53. Advice for applicants on what to do if information requested during the clearance process is unavailable can be sought directly from the AGSVA Client Service Centre.
- 54. If advised by AGSVA, commanders and managers **must** [Auth:None] notify an applicant in writing of the requirement to provide vetting information within stipulated timeframes and of the range of consequences of failing to provide that information.
- 55. Commanders and managers of staff who do not cooperate in the security clearance process **must** notify the relevant human resource or contract management area and follow instructions with regard to notifying applicants of the effect of non-compliance on their conditions of employment.

Clearance Subjects with Uncheckable Backgrounds

- 56. Under the PSPF, only clearance subjects with checkable backgrounds are eligible to be considered for an Australian security clearance unless their agency head, or delegate, waives this requirement through the granting of an Uncheckable Background Eligibility Waiver.
- 57. The PSPF places strict constraints on the information that the recipient of Eligibility Waivers may access. Refer to Annex A for further information on the content, operation and information access restrictions that apply to Eligibility Waivers.
- 58. Only AGSVA can decide that a clearance subject has an uncheckable background as this is dependant on issues such as the ability to contact former employers and whether countries in which the person has previously lived are able to provide AGSVA with relevant information.

Note: Uncheckable backgrounds can affect both foreign nationals and Australian citizens; for example, when Australian citizens have spent time abroad during the checking period.

- 59. An uncheckable background does not necessarily preclude consideration for Defence employment. However, clearance holders with an uncheckable background represent a higher risk to Defence and require the identification and acceptance of residual risk by a Group Head or Service Chief. The Uncheckable Background Eligibility Waiver is the mechanism used to accept and manage these risks.
- 60. If, during the vetting process, AGSVA determines that background checks can not be conducted on a clearance subject to the standard required by the PSPF, for all or part of the prescribed checking period, all vetting processes will cease. AGSVA will advise the clearance sponsor that the clearance subject has an uncheckable background, together with any known risks identified by the AGSVA to date, and will request an Uncheckable Background Eligibility Waiver if the clearance process is to proceed.

Note: AGSVA will not request an Uncheckable Background Eligibility Waiver if AGSVA has already identified any other concerns that would disqualify the subject for a security clearance at the level requested. If such concerns have already been identified the clearance will be denied or offered at a lower level.

61. On receipt of advice that a clearance subject has an uncheckable background, the clearance sponsor may decide to either cease the clearance process or continue the clearance process under a risk managed approach via an Uncheckable Background Eligibility Waiver. The decision on whether or not to proceed with a clearance is a business decision taken by the sponsoring area.

Note: The PSPF places a number of information access restrictions on recipients of eligibility waivers. These conditions may be difficult for the employing area to meet or make employment for some duties impractical. Refer to Annex A for further detail.

- 62. If the sponsor decides to cease the clearance process then the sponsor **must** [Auth:None] advise the ASGVA in writing of the decision. The clearance is then denied by the AGSVA on the basis of an uncheckable background.
- 63. If the sponsor decides to continue the clearance process they **must** [Auth:None] complete an Uncheckable Background Eligibility Waiver and submit it to the relevant Group Head or Service Chief for approval. If the clearance subject will require access to any codeword material, the endorsement of each compartment controller, including any external to Defence, **must** [Auth:None] also be obtained. If the waiver is approved, it **must** [Auth:None] be forwarded to AGSVA for consideration.

Note: As contractors cannot accept security risk on behalf of the Commonwealth, if an Uncheckable Background Eligibility Waiver is required for a Defence Industry Security Program (DISP) employee, the contract manager is responsible for seeking approval of the Eligibility Waiver from the relevant Group Head or Service Chief.

Note: It is recommended that the contract manager and company work closely together to develop the supporting business case, including the impact on contract performance, before an Uncheckable Background Eligibility Waiver is put to the relevant Group Head or Service Chief.

- 64. The endorsement of an Uncheckable Background Eligibility Waiver does not guarantee that a clearance subject will be granted a security clearance by AGSVA as subsequent disqualifying information may be identified after the vetting process is restarted. Further, AGSVA may, at its discretion, not continue with a security clearance if the Uncheckable Background Eligibility Waiver does not fully detail the risks to the national interest, appropriate mitigations and any residual risks.
- 65. Once the Uncheckable Background Eligibility Waiver has been accepted or rejected by AGSVA, follow-on administrative actions may be required of the clearance sponsor. These can include:
 - a. altering an employment offer to reflect restrictions advised by AGSVA;
 - withdrawing an offer of employment; or
 - c. redeploying the individual concerned to another position.

Note: Refer to the section on *Procedural Fairness* below before taking any administrative action. Advice should also be sought from the relevant human resources area.

66. Clearances granted to a holder with an Uncheckable Background Eligibility Waiver are not automatically transferable between departments, positions within a department or duties within a position.

Procedural Fairness

- 67. Before a delegate makes a decision that could negatively affect the clearance subject, procedural fairness requires that the applicant be told the case to be met, to the fullest extent possible consistent with national security, and be given an opportunity to respond.
- 68. Based on this principle, all subsequent administrative actions that flow from the AGSVA delegate's decision **must not** [Auth:SES Band 1/07] be undertaken until any appeals by the clearance subject are finalised.

Note: Administrative actions include terminating employment, permanent modification or reassignment of duties, withdrawing offers of employment etc.

Exclusion: DISP companies are not bound by the same employment framework as Defence, and are therefore excluded from this procedural fairness requirement. However, Australian law may

DSM Part 2:20 Page 11 of 26

confer protections on the clearance subject and avenues of legal redress, such as an unfair dismissal claim, should a subsequent appeal find in favour of the clearance subject. DISP companies should therefore seek legal advice before taking administrative actions prior to all appeals being finalised.

69. FAS S&VS and ASIO retain the right to temporarily reduce or remove access to classified material, at any time, if a significant security concern is identified during the security clearance process. Therefore commanders and managers **must** [Auth:None] comply with any direction from FAS S&VS or ASIO to limit or modify access to classified material during the clearance process pending a final decision.

Challenging a Security Clearance Decision

- 70. Under the PSPF, AGSVA is required to advise a clearance subject who has received an adverse clearance decision of the decision, the basis of the decision and offer the subject a reasonable opportunity to respond.
- 71. AGSVA assessment of a person's overall suitability to hold a security clearance may subsequently be appealed. When notifying an applicant of an adverse decision, AGSVA is required to advise the applicant of the available avenues of appeal.

Note: An ASIO security assessment may be appealed through the Administrative Appeals Tribunal. Further information on this process will be notified to the applicant by AGSVA if an adverse ASIO assessment is issued.

Security Clearances for Foreign Nationals

- 72. The PSPF requires that access to classified information by a foreign national **must** [Auth:None] only occur if:
 - access is granted under a Security of Information Agreement or Arrangement (SIA) where the foreign national holds an equivalent or higher current security clearance issued by the foreign government; or
 - b. the foreign national has been issued an Australian security clearance.
- 73. Consistent with the above, the circumstances in which a foreign national may be permitted access to classified Defence information and assets, include:
 - a. The foreign national is employed in an Australian military or business unit on secondment from New Zealand (NZ), the United States (US), the United Kingdom (UK) or Canada (CA), <u>and</u> their foreign security clearance is recognised by Australia under the terms of a Security of Information Agreement or Arrangement (SIA).
 - b. The foreign national holds an Australian security clearance that has been issued:
 - (1) following AGSVA acceptance of an approved Citizenship Eligibility Waiver;
 - (2) following AGSVA acceptance of an approved Citizenship Eligibility Waiver <u>and</u> recognition that the individual's current or former NZ, US, UK or CA issued security clearance meets the requirements of an Australian clearance, either in full or in part; or
 - (3) on the basis of provisional entry to the ADF under the government to government 'ADF lateral recruit' program and the individual has undertaken to become an Australian Citizen.
- 74. Each of these scenarios is discussed further in the balance of this section.

- 75. The PSPF places strict constraints on information that the recipient of an Eligibility Waiver may access. Refer to Annex A for further information on the content, operation and information access restrictions that apply to Eligibility Waivers.
- 76. In certain situations, where the foreign security clearance equates to Australia's PV clearance, AGSVA may require the clearance subject to provide consent for AGSVA to request the release of relevant personal details from their foreign clearance sponsor. AGSVA may request the assistance of the Defence PV sponsor to confirm details of the PV equivalent clearance held, through existing arrangements/liaison officers in place with their foreign allied agencies, prior to recognising the clearance. Notwithstanding any foreign PV equivalent clearance held, AGSVA may require a clearance subject to undertake additional Australian psychological testing in order to assess their suitability for employment.

Determining if an Australian Security Clearance is Required

- 77. Whether an Australian clearance is required can usually be determined by whether the foreign national's activities occur under a formal agreement (e.g. project or research) between Australia and the relevant nation(s).
- 78. If the proposed access by a foreign national is not covered by a SIA, the foreign national **must** [Auth:None] hold an Australian security clearance before they can be granted access to classified information or assets.

Seconded Foreign Nationals

- 79. Seconded foreign nationals from NZ, US, UK and CA have their foreign security clearance recognised by Australia under the relevant SIA for the duration of their secondment to Australia or an Australian unit on operation. A seconded foreign national from these countries does not require an Australian clearance if they hold a current clearance at the equivalent level from their parent nation.
- 80. A foreign national is considered seconded if they are authorised to act on behalf of the Australian Government or are assigned to an ADF Unit.
- 81. Notification of security clearances for seconded staff may occur via the following mechanisms:
 - for posting between intelligence agencies, notification occurs via the relevant intelligence agency agreements;
 - b. for long term secondments, the DS&VS International Visits Office confirms clearances as part of the visits notifications process;
 - c. for short term secondments between deployed operational units, CJOPS may appoint delegates to confirm clearances by signal or classified email between nominated ADF and Allied commands; or

Note: This process may also be used for exchanging security clearance details for exercise participants.

- d. for RAN Ships exchanging staff at sea, confirmation of clearance may be passed between units by signal or classified email.
- 82. Seconded foreign nationals may access Australian Government Access Only (AGAO) but **must not** [Auth:None] access AUSTEO material. Non-seconded foreign nationals, eg exercise participants who are acting on behalf of their own nation, are not acting on behalf of the Australian Government and therefore **must not** [Auth:None] access AGAO or AUSTEO material.

Foreign National Contractors and Security of Information Agreements or Arrangements

- 83. Unlike a seconded foreign national, a contractor is not authorised to act on behalf of the Australian Government. A foreign national contractor may be employed in Australia or overseas.
- 84. A foreign national contractor does not require an Australian security clearance if their terms of employment meet all provisions of a relevant SIA and they hold a current security clearance issued by their foreign government. Under these arrangements, any classified material accessed by the contractor occurs under the relevant SIA as a government to government exchange. Therefore access to AGAO or AUSTEO material **must not** [Auth:None] be granted as this material can not be passed to a foreign government. For further information, refer to DSM Part 2:35 Security Information Agreements and Arrangements.
- 85. Contract managers are advised that failure to correctly implement the terms of a SIA in the employing contract for a foreign national contractor will, under the PSPF, result in the contractor being unable to access any Australian Government classified information. Therefore contract managers **must** [Auth:None] cite the relevant provisions of the SIA in the contract.
- 86. Before access to Australian Government classified information is granted to any foreign national contractors:
 - a. the provisions of a relevant SIA **must** be sought from the DS&VS Defence Security Policy and International Agreements Directorate, including for citing in the contract; and
 - b. the foreign national contractors' clearances **must** [Auth:None] be confirmed via the DS&VS International Visits Office
- 87. If the requirements of this section cannot be met, the contractor **must** initiate an Australian security clearance with a Citizenship Eligibility Waiver.

Visiting Foreign Nationals

88. Foreign nationals who are undertaking a short term visit to Australia have their clearances notified via their government to the DS&VS International Visits Office. Foreign visitor's clearances can be confirmed by contacting DS&VS International Visits. Contact details and procedures are available on the DS&VS security portal.

Citizenship Eligibility Waivers

- 89. Under the PSPF, only Australian citizens are eligible to be considered for an Australian security clearance unless their agency head, or delegate, waives this requirement through the approval of a Citizenship Eligibility Waiver.
- 90. The PSPF places strict constraints on information that the recipient of an Eligibility Waiver may access. Refer to Annex A for further information on the content, operation and information access restrictions that apply to Eligibility Waivers. A recipient of a Citizenship Eligibility Waiver **must not** [Auth:None] be granted access to AUSTEO information.
- 91. Importantly, the granting of a Citizenship Eligibility Waiver for a security clearance is a separate consideration to waiving Australian citizenship as a condition of engagement in the APS in accordance with section 22(8) of the *Public Service Act 1999*. Notwithstanding, this delegation **must** [Auth:None] be exercised prior to requesting AGSVA conduct or recognise a security clearance for a potential APS employee. The authority to waive Australian citizenship as a condition of engagement can be exercised by those delegates published in the 'Schedule of Public Service Delegations'.

Note: Final employment remains conditional on receiving an Australian security clearance from AGSVA.

DSM Part 2:20 Page 14 of 26

- 92. The PSPF also requires that the decisions to waive citizenship for employment in the APS and to waive citizenship for a security clearance are not to be exercised by the same delegate, unless that delegate is the Secretary. Therefore a delegate, other than the Secretary, who waives citizenship as a condition of engagement to the APS **must not** [Auth:None] authorise a Citizenship Eligibility Waiver for the purpose of a security clearance for the same individual.
- 93. Reasons for waiving the citizenship eligibility requirement for a security clearance may include:
 - a. the person is critical to Defence outcomes (including Defence industry in its role as a Defence capability enabler) and the risks to Defence can be mitigated and/or managed;
 - b. the role cannot be redesigned so that access to classified information or assets is restricted to existing employees with the appropriate clearance;
 - c. the role cannot be performed by an Australian citizen and there is no conflict of interest or other concern in relation to the person's country of allegiance and the role being undertaken;
 - d. the foreign national is a permanent resident of Australia who is eligible for citizenship and is actively seeking citizenship at the time of application and the citizenship process will be concluded in a reasonable period;

Note: Special arrangements apply for ADF recruits. See then section on *Clearances for ADF recruits who are not Australian citizens* below.

e. the foreign national is contracted directly to Defence to supply services in an overseas location and is not covered by a SIA.

Note: The Department of Foreign Affairs and Trade (DFAT) grants and administers security clearances for all locally engaged staff employed at Australian missions overseas.

94. AGSVA requires a Citizenship Eligibility Waiver to be completed for all civilian clearance subjects before it can commence the processing of an Australian clearance for a foreign national.

Note: An Uncheckable Background Eligibility Waiver may also be required if AGSVA determines the clearance subject has an uncheckable background.

Note: Refer to Annex A for further information on the content and operation of Eligibility Waivers.

- 95. Before commencing the development of a Citizenship Eligibility Waiver, the clearance sponsor **must** [Auth:None] consult AGSVA to determine if AGSVA is aware of any pre-existing concerns regarding the clearance subject. Pre-existing concerns can arise as a result of previous applications for an Australian security clearance. And, for a position located in Australia, the clearance sponsor is to ensure that the clearance subject has received the appropriate visa and is eligible to work in Australia.
- 96. All Citizenship Eligibility Waivers for civilian clearance subjects **must** [Auth:None] be approved by the relevant Group Head or Service Chief. The clearance sponsor is responsible for staffing the Citizenship Eligibility Waiver and providing it to AGSVA. If the clearance subject will require access to any codeword material the endorsement of each compartment controller, including any external to Defence, **must** [Auth:None] also be obtained.
- 97. Defence recognises that in some circumstances contractors may require a non-Australian citizen to hold a security clearance in order to perform specialist duties, either in Australia or overseas. As contractors can not accept security risk on behalf of the Commonwealth, sponsorship for an Australian security clearance that is subject to an Eligibility Waiver **must** [Auth:None] be negotiated via the relevant contract manager. The contract manager is responsible for seeking approval of the Citizenship Eligibility Waiver from the relevant Group Head or Service Chief.

Note: It is recommended that the contract manager and company work closely together to develop the supporting business case, including the impact on contract performance, before a Citizenship Eligibility Waiver is put to the relevant Group Head or Service Chief.

- 98. The approval of a Citizenship Eligibility Waiver does not guarantee that a clearance subject will be granted a security clearance by AGSVA. Notwithstanding the Citizenship Eligibility Waiver, AGSVA may decline the request for clearance if there is no prospect of a clearance being granted. AGSVA may, at its discretion, not accept the request for security clearance if the Citizenship Eligibility Waiver does not fully detail the risks to the national interest, mitigations and any residual risks.
- 99. Once the Citizenship Eligibility Waiver has been accepted or rejected by AGSVA, follow-on administrative actions may be required by the clearance sponsor. These can include:
 - a. altering an employment offer to reflect restrictions advised by AGSVA;
 - b. withdrawing an offer or employment; or
 - c. redeploying the person to another position.
- 100. Clearances granted to a holder with a Citizenship Eligibility Waiver are not automatically transferable between departments, positions within a department or duties within a position.

Recognising US, UK, CA and NZ Clearances when granting an Australian Clearance for Civilians

- 101. Subject to AGSVA accepting a Citizenship Eligibility Waiver, a clearance subject who holds or formerly held a clearance issued by the US, UK, CA or NZ is eligible to have their foreign clearance recognised as meeting the requirements (in full or in part) for an Australian clearance. If an Australian clearance is granted subsequent aftercare and reviews will be conducted by AGSVA.
- 102. This arrangement essentially functions as a transfer of security clearance, whereby an Australian security clearance, equivalent to or less than the recruit's foreign clearance, is issued. The actual level of clearance will depend on the level of the DSAP nominated by the recruiting Service or Group. Additional checks, including Uncheckable Background Eligibility Waivers, will be undertaken if the clearance requested is higher than the equivalent foreign issued clearance.
- 103. The PSPF places strict constraints on the information that the recipient of Eligibility Waivers may access. Refer to Annex A for further information on the content, operation and information access restrictions that apply to Eligibility Waivers.
- 104. To enable recognition of a US, UK, CA or NZ security clearance, the following conditions **must** [Auth:None] be met:
 - a. the clearance is current, or has lapsed or was cancelled for administrative reasons (e.g. such as leaving the service of that foreign government) within the six months prior to the proposed date of employment;
 - b. AGSVA can properly confirm the details of such foreign clearances via allied agencies;

Note: If AGSVA is unable to adequately confirm the foreign security clearance to its satisfaction, then a foreign clearance cannot be used to grant the Australian clearance.

- no issues of a security nature have been identified either by the foreign government or AGSVA;
 and
- d. AGSVA administrative requirements and timeframes are met by both the recruit and the recruiting organisation.

DSM Part 2:20 Page 16 of 26

- 105. In order for AGSVA to process a security clearance containing foreign recognition requests the following procedures and timeframes apply:
 - a. the recruiting or sponsoring Service or Group **must** request a personnel security clearance from the AGSVA and clearly identify the clearance subject as a <u>'foreign civilian recruit'</u>;
 - b. the request **must** [Auth:None] provide details of the recruit's US, UK, CA or NZ security clearance, including level, the agency it was issued by and any other identifying information, and the proposed commencement date for employment;
 - c. the request **must** [Auth:SES 1/O7] be submitted to AGSVA at least 90 days prior to the proposed date of commencement, except in exceptional circumstances as certified by at least a SES Band 1/O7 officer:
 - d. the recruiting or sponsoring element **must** [Auth:None] provide AGSVA with a copy of the recruit's application to join Defence or the DISP member company;
 - e. the application **must** [Auth:None] include copies of all related documents the recruit provided as part of the recruitment process;
 - f. in the case of direct recruits to Defence, the recruitment process **must not** [Auth:None] be finalised before AGSVA grants an Australian clearance; and
 - **Note:** All offers of employment remain subject to AGSVA granting a clearance.
 - g. in the case of recruits of DISP member companies, the recruit **must not** [Auth:None] be engaged in any classified work associated with a Defence contract that requires a clearance, before AGSVA grants an Australian clearance.
- 106. A failure to comply with these requirements will likely result in delays in processing the application and may prevent AGSVA from recognising a foreign clearance.

Clearances for ADF Recruits who are not Australian Citizens

- 107. In accordance with DI(G) PERS 33-1 *Citizenship requirements for entry to and service in the Australian Defence Force*, foreign nationals may be provisionally enlisted into the ADF despite not holding Australian citizenship. In accordance with Section 23 of the *Australian Citizenship Act 2007*, these individuals are eligible to apply for Australian citizenship after completing at least 90 days relevant Defence service in the permanent force or, in the case of Reservists, six months relevant Defence service. These recruits sign an undertaking to apply for Australian citizenship as soon as they are eligible to do so; if they do not, their ADF service may be terminated.
- 108. A Citizenship Eligibility Waiver for security clearance purposes is not required for an ADF recruit who has undertaken to become an Australian citizen in accordance with DI(G) Pers 33-1.
- 109. A background eligibility waiver is not required:
 - a. for foreign nationals of US, CA, UK or NZ who served in their armed forces;
 - whose clearance is current, or has lapsed or was cancelled for administrative reasons (e.g. such as leaving the service of that foreign government) within the six months prior to the proposed date of enlistment; and
 - c. the applicant is applying for an Australian clearance at or below the equivalent level of clearance granted by their government.

Note: If the clearance requested is higher than that previously held, AGSVA will determine if a background eligibility waiver will be required based on the amount of information available from the government that issued the clearance.

Note: Foreign nationals, who are being laterally recruited to the ADF from the armed forces of countries other than US, CA, UK or NZ, may require a background eligibility waiver. This will be determined by AGSVA.

- 110. Access to AUSTEO information **must not** [Auth:None] be granted prior to the recruit gaining Australian Citizenship. However, access to AGAO is permissible prior to naturalisation.
- 111. If an ADF lateral recruit is eligible to have a foreign clearance recognised the following requirements are to be met:
 - a. the recruiting service **must** [Auth:None] request a personnel security clearance from AGSVA which clearly identifies the clearance subject as an 'ADF lateral recruit';
 - b. the request **must** [Auth:None] provide details of the recruit's US, UK, CA or NZ security clearance, including level, the agency it was issued by and any other identifying information, and the proposed enlistment date;
 - c. the request **must** [Auth:SES 1/ O7] be submitted to AGSVA at least 90 days prior to the proposed enlistment, except in exceptional circumstances as certified by at least an SES Band 1 / O7 officer;
 - d. the recruiting service **must** [Auth:SES 1/O7] provide AGSVA a copy of the recruit's formal application to join the ADF; and
 - e. the recruitment process **must not** [Auth:None] be finalised before formal advice on the recruit's security clearance is obtained from AGSVA.

Note: All offers of employment remain subject to AGSVA granting a clearance.

Managing Clearance Holders

Aftercare

- 112. Commanders and managers are responsible for the ongoing management of their security cleared personnel. This applies regardless of whether the clearance has been issued by AGSVA, an exempt agency or a foreign government.
- 113. Significant security concerns can develop after a security clearance has been issued. Therefore commanders and managers **must** [Auth:None] report any issues of security concern that they become aware of to AGSVA. This information is handled in the strictest confidence. If AGSVA is not the clearance issuer, it will liaise with the relevant agency that issued the clearance.
- 114. Commanders and managers **must** [Auth:None] report changes in employees' circumstances if they are unsure if the employee has notified those changes in circumstance to AGSVA or the clearance issuing agency
- 115. From time to time, AGSVA may direct specific aftercare conditions be undertaken by a clearance holder or their commanders and managers. If AGSVA issues aftercare conditions they **must** [Auth:None] be adhered to.
- 116. Security reporting responsibilities extend past the employment of an employee. This is particularly relevant where an employee has separated under adverse circumstances. All Defence employees are reminded that they are required to report to AGSVA any security concerns they hold about current or former

DSM Part 2:20 Page 18 of 26

clearance holders. This is particularly relevant if there is any indication that the person intends to reveal classified or other official information.

Aftercare for Foreign Nationals and Clearance Holders granted an Uncheckable Background Eligibility Waiver.

- 117. Commanders and managers need to be particularly vigilant in monitoring the attitude, behaviour and security performance of foreign nationals and newly naturalised individuals granted Australian clearances. This includes the prompt reporting to AGSVA of any change in the individual's attitude or behaviour, or any incidents that may be cause for security concern.
- 118. A clearance granted to a holder with a Citizenship or Uncheckable Background Eligibility Waiver is not automatically transferable between departments, positions within a department or duties within a position. The following aftercare provisions apply to these clearance holders:
 - a. The Citizenship or Uncheckable Background Eligibility Waiver, including the supporting risk assessment and treatment plan, **must** [Auth:None] be reassessed by the relevant Group Head or Service Chief and returned to AGSVA:
 - (1) before transferring to Defence, if the original waiver was issued by another agency;
 - (2) before the clearance holder changes positions or duties within a position;
 - (3) at least every two years; and
 - (4) at any other time as directed by AGSVA.
 - b. The clearance holder **must** [Auth: ASV] gain Australian citizenship as soon as they become eligible to do so and forward a copy of naturalisation certificate to AGSVA.

Note: Individuals who are eligible to become Australian citizens but decline to do so when offered, or delay taking action to become Australian citizens at the first available opportunity, will generally have their security clearance withdrawn except in exceptional circumstances as approved by ASV.

- 119. An individual who is granted an Australian security clearance but is not an Australian citizen **must not** [Auth:None] be given access to AUSTEO material.
- 120. Access to material carrying the AGAO caveat may be permitted subject to the need-to-know principle.
- 121. For an individual to be granted access to 'eyes only' material, they must [Auth:None]:
 - a. be a citizen of one of the countries listed; and
 - b. hold an appropriate clearance for that country.

Note: This limitation is removed on advice from AGSVA after proof of Australian citizenship has been provided.

122. Access to codeword material is subject to approval of the compartment controller, provided the compartment is not subject to an eyes only caveat that would otherwise exclude access.

Reviewing the Suitability of a Clearance Holder

123. From time to time situations may arise that bring into question the suitability of a clearance holder to continue to access classified information and assets. The process used by AGSVA to assess such information is known as a review for cause.

DSM Part 2:20 Page 19 of 26

- 124. A review for cause may be initiated whenever a security concern regarding a clearance holder arises. AGSVA may initiate a review for cause in response to information from:
 - a clearance holder's colleagues or supervisors or any other individual who has reason to believe that the security clearance holder's personal circumstances, attitudes or behaviour have changed;

Note: Administrative action may be taken against Defence employees if security concerns raised are found to be vexatious.

- b. the security clearance holder, as a result of a change of circumstances;
- c. the DS&VS Security Incident Centre, where security incident data indicates a pattern of security incidents that raise concern;
- Defence Investigative Authorities, where a specific investigation or inquiry indicates an area of concern; and
- e. ASIO, as a result of an investigation or pending reassessment of a clearance holder's ASIO security assessment.

Note: In these circumstances, AGSVA will advise the clearance holder's supervisor of any necessary action, including ongoing access permissions, under the *ASIO Act 1979*.

Note: The secrecy provisions of the *ASIO Act 1979* apply to ASIO investigations. While ASIO involvement in personnel security matters is a rare occurrence, failure to adhere to lawful instructions issued by ASIO, or revealing the existence of an ongoing investigation, may render Defence employees liable to prosecution under the *ASIO Act 1979*.

- 125. AGSVA may reject a request to conduct a review for cause if in its opinion the matter is insufficiently justified, not of sufficient security concern or is a performance management issue.
- 126. FAS S&VS, as Agency Security Adviser may, as a result of a security incident or investigation, direct a commander or manger to temporarily restrict or deny access to classified material pending the completion of a review for cause.

Note: In order to avoid conflicts of interest, DS&VS maintains separation between security matters and AGSVA delegates' vetting decisions. Any decision taken to limit access by FAS S&VS has no influence on the outcome of a review for cause undertaken by AGSVA.

127. Unless otherwise directed to deny access to classified material by FAS S&VS or ASIO, it is the commander or managers administrative decision whether to limit or deny access to classified material during a review for cause. It is recommended that any such decision is supported by a risk assessment.

Note: Any decision taken to limit access during the review for cause has no influence on the outcome of the review for cause.

Periodic Reviews

- 128. Unless other security factors arise, all security clearances are required to be reviewed at regular intervals. The interval depends on the level of the security clearance (see table below). AGSVA is responsible for maintaining and initiating security revalidations and, for PV holders, the annual security appraisal.
- 129. A revalidation is a periodic review conducted to ensure that an individual is still suitable to hold a security clearance at the granted level. The purpose of the revalidation is to confirm the need to maintain the current security clearance and assess the accuracy and currency of information about the individual.

Note: Periodic reviews were previously described as either a revalidation or re-evaluation.

DSM Part 2:20 Page 20 of 26

130. Former clearances issued under the Protective Security Manual will be upgraded to the new PSPF clearance level on review.

Table 2:20-2: Frequency of Review

PSPF Standards for the Frequency of Review				
	BASELINE VETTING	NEGATIVE VETTING LEVEL 1	NEGATIVE VETTING LEVEL 2	POSITIVE VETTING
Revalidation	15 years	10 years	5 years	5 - 7 years
Security Appraisal	N/A	N/A	N/A	Annually

When a Clearance Subject's Employment ceases

- 131. Commanders and managers are responsible for managing the separation process.
- 132. The commander or manager **must** [Auth:None]:
 - a. report to AGSVA any security concerns arising from the separation;

Note: Indicators of concern can include termination in adverse circumstances, disgruntlement in the work place, or failure to acknowledge post separation requirements to protect classified information etc.

- b. administer or organise debriefs for personnel who have had access to CODEWORD or other compartmented information;
- c. notify the compartment controller of the separation and withdraw sponsorship of any compartmented briefings;
- d. advise AGSVA that:
 - (1) an employee or contractor with a security clearance is separating/has separated;
 - (2) if transferring to another agency or contracted service provider, which agency or provider, if known;
- e. remind the separating employee of his or her continuing personal obligations under the *Crimes Act 1914* and other relevant legislation;
 - (1) request that the employee signs the Recognition of Continuing Obligation; and
 - (2) forward a copy of the Recognition of Continuing Obligation to AGVSA.
- 133. A separating employee cannot be compelled to sign any security documentation. If an employee elects not to sign debriefing material or a recognition of security obligation, then the commander or manager **must** [Auth:None] notify AGSVA as this may indicate a behaviour of security concern.

Roles and Responsibilities

Secretary of Defence

- 134. The Secretary is accountable to the Minister for the performance of the vetting function supplied by AGSVA to Defence and other non-exempt agencies.
- 135. As the Agency Head, the Secretary:
 - a. establishes the minimum suitability requirements for all APS personnel employed in Defence;
 - b. imposes conditions of employment on APS employees, which may include character checks and security clearances, in accordance with the *Public Service Act 1999* sections 22(6) and 22(7);
 - c. may require APS personnel in a particular category to be security cleared to a predetermined level; and
 - d. is authorised to waive the eligibility requirements for a person to qualify for a security clearance.
- 136. The Secretary has delegated his responsibilities at paragraphs:
 - a. 131b to delegates published in the 'Schedule of Public Service Delegations'; and
 - b. 131c and d to the respective Group Heads and Service Chiefs.

Chief of the Defence Force

- 137. As the Chief of the Defence Force, the CDF:
 - establishes the minimum suitability requirements for all ADF personnel employed in Defence;
 - b. may require ADF personnel in a particular category to be security cleared to a predetermined level.

First Assistant Secretary Security and Vetting Service

138. FAS S&VS is responsible to the Secretary for ensuring that the Defence security clearance process and AGSVA vetting procedures are conducted in accordance with PSPF and IASF policy.

Assistant Secretary Vetting

- 139. ASV as the Head of AGSVA, may grant, deny, vary or revoke an Australian security clearance.
- 140. ASV may, with respect to clearances sponsored by Defence, recognise a foreign issued security clearance as meeting the requirements of an Australian security clearance in whole or in part, in accordance with relevant bi-lateral security instruments.

Note: Depending on the specific international security agreement, a recognised clearance may not be transferable to other agencies.

Group Heads and Service Chiefs

141. Group Heads and Service Chiefs are responsible for accepting and managing, through their chain of command, the security risk arising from the employment of all personnel and contractors within their chain of command. This includes accepting the security risk associated with employing personnel and contractors who have been granted a Citizenship or Uncheckable Background Eligibility Waiver because they do not meet the minimum PSPF eligibility requirements for a security clearance.

Commanders and Managers

- 142. Commanders and managers are responsible for the management of clearance subjects and clearance holders. Security officers assist commanders and managers in the administration of the supporting processes and act as a single point of contact with AGSVA.
- 143. Commanders and managers are responsible for:
 - identifying positions that require access to classified information and assets, or that otherwise require a clearance to provide a level of assurance as to the occupant's suitability to perform the particular role;
 - b. ensuring that there are an adequate number of personnel with clearances to meet their business continuity needs;
 - c. sponsoring security clearances or, in the case of PV clearances, gaining sponsorship from an authority listed in this DSM part (see paragraph 34);
 - d. initiating requests for new clearances and upgrades in a timely manner to permit processing within the agreed benchmark timelines detailed in the AGSVA service charter;
 - e. preparing Citizenship and Uncheckable Background Eligibility Waivers for their Group Head or Service Chief's approval; and
 - f. administering the security aftercare of their personnel, including:
 - (1) complying with any aftercare and clearance directions issued by AGSVA;
 - (2) briefing clearance holders on their security responsibilities, including the need to advise the AGSVA of any changes in their personal circumstances;
 - (3) managing individuals, granted a clearance subject to an Eligibility Waiver, in accordance with the provisions of the accompanying risk assessment;
 - (4) monitoring personnel behaviour and attitudes towards security;
 - (5) ensuring personnel participate in security awareness and training programs;
 - (6) reporting any security concerns to AGSVA; and
 - (7) reporting any changes in their staff's personal circumstances, which they have become aware of, to AGSVA.

Security Officers

144. Security officers assist their commander or manager to undertake their security management responsibilities. They act as a single point of contact with AGSVA on clearance matters. This includes:

DSM Part 2:20 Page 23 of 26

- initiating the security clearance process when directed by a commander or manager;
- b. confirming clearances held with AGSVA when directed by a commander or manager;
- c. bringing to the commander or manager's attention any clearance subjects who have not provided information to AGSVA within the requested timeframes to allow follow-up administrative action: and
- where appropriate, assisting clearance subjects in completing the requirements of the security clearance process.
- 145. While security officers assist a commander or manager with the clearance process and carry out administrative functions on their behalf, the responsibility for managing security clearances remains with the relevant commander or manager unless formally delegated.

Clearance Subjects

146. It is important that clearance subjects understand their responsibilities in relation to obtaining and maintaining a personnel security clearance. Clearance subjects' responsibilities are published on the AGSVA intranet site.

Clearance Holders

147. It is important that once granted a security clearance, Defence personnel and external service providers meet their ongoing responsibilities as clearance holders. See the AGSVA intranet site for responsibilities, including reporting of any change of circumstances.

Positive Vetting Sponsors

- 148. The PV sponsor is responsible for:
 - a. confirming that the position and the incoming individual of the position has a need to hold a PV in order to undertake their official duties;
 - notifying AGSVA when a PV holder no longer occupies a PV DSAP within their area of responsibility; and
 - c. maintaining a list of PV DSAP within their area of responsibility.

Positive Vetting Clearance Holders

- 149. PV clearance holders may be subject to additional requirements. PV holders will be informed of any additional requirements:
 - a. by AGSVA when the clearance is issued;
 - through IASF policy;
 - c. via intelligence agency training programs; and
 - d. as notified from time to time by their PV sponsor.

DSM Part 2:20 Page 24 of 26

Key Definitions

- 150. **Australian Government Security Vetting Agency**. AGSVA is a branch of DS&VS that provides independent security clearance vetting services and advice to non-exempt government agencies, including Defence, in accordance with the PSPF.
- 151. **Security clearance.** An administrative determination by a competent authority that an individual is eligible and suitable, from a security standpoint, to access security classified information and assets.
- 152. Clearance subject. An individual, whose suitability to hold a clearance, is being assessed.
- 153. **Clearance holder.** An individual, who has been assessed as suitable and has been granted a security clearance.
- 154. **Clearance sponsor.** A commander or manager, or for PV clearances, the PV sponsor, who sponsors an individual to undergo a security clearance for a position within their organisation.
- 155. **Designated Security Assessment Position.** A DSAP is defined in the *Crimes Act 1914* as 'a position in a Commonwealth authority which the head of the authority has determined to be a designated security assessment position whose duties are likely to involve access to national security information classified as secret or top secret'.
- **156.** Eligibility Waiver. A form of dispensation used to manage the residual risk to Defence when engaging a clearance holder who does not meet either the citizenship or minimum background checking requirements for a security clearance as specified in the PSPF. Within Defence, Eligibility Waivers are managed using the DSM dispensation process.
- **157. Uncheckable Background.** An assessment issued by AGSVA that a clearance subject's background can not be checked to the standard required by the PSPF for some or all of the relevant checking period.
- 158. **Vetting.** Checking and assessment procedures undertaken to develop an informed evaluation of a clearance subject's suitability to hold a security clearance of a specified level.
- 159. **'Need-to-know' principle.** The principle that the availability of official information should be limited to those who need to use or access the information to do their work.
- 160. **PV sponsor**. A Defence employee who occupies a position that is authorised to sponsor an individual to undergo a PV security clearance.

Further Definitions

161. Further definitions for common DSM terms can be found in the Glossary.

Annexes and Attachments		
Annex A	Accepting and Managing Risks Associated with Foreign Nationals and Clearance Subjects with Uncheckable Backgrounds	

Defence Security and Vetting Service Intelligent security for an insecure world



Defence Security and Vetting Service Intelligent security for an insecure world

Defence Security Manual

DSM Part	2:30 Classificati	ion and Protect	ion of Official Ir	nformation	
Version	8	Publication date	13 May 2016	Amendment list	26
Optimised for	Screen; Print; Scree	n Reader			
Releasable to	Defence, Defence Ir	ndustry			
Compliance Requirements		und by security policinally with the mandal evant contract provise 1982, the Public Scients in the DSM and Id / should not. Coority, if applicable, hassociated risk throwe process which mend' and 'may' are ut to be approved or dompliance with a serunagement principle	cy contained in the latory requirements of sion or legislation in ervice Act 1999, and d ISM are identified impliance with these has considered the jugh the granting of eets the intent of the ised to denote a serocumented.	DSM and Information the DSM and ISM cluding, but not limited the <i>Crimes Act 19</i> through the use of exequirements is majustification for non-a dispensation, or he DSM. Insible security practice ought to be information.	on Security Manual I may result in ted to; the <i>Defence</i> 114. the terms must / andatory unless compliance and has accepted a
Copyright	© Commonwealth of	f Australia 2010			
	This work is copyright no part may be reproduced Department of Deferoaddressed to Deferoads.	oduced by any proc nce. Requests and i	ess without prior wr inquiries concerning	itten permission from reproduction and r	m the

Defending Australia and its National Interests www.defence.gov.au



Introduction

- 1. The security of information is critical to the integrity of Defence's mission. If Defence does not protect its information from unauthorised access, its ability to function in support of the Government will be undermined. The Australian Government Security Classification System (AGSCS) allows Defence to share and exchange information with confidence by ensuring a common recognition of confidentiality requirements and the consistent application of protective security measures.
- 2. The purpose of Defence Security Manual (DSM) Part 2:30 *Classification and Protection of Official Information* is to detail security policy for the classification and protection of official information.

Policy

- 3. Originators of Defence information will assess that information, through a process of security classification, to determine the impact of access by, or disclosure to, unauthorised entities including individuals, groups or organisations.
- 4. The criteria and process that Defence uses to assess and classify information will be consistent with the AGSCS. This assessment will complement a broader assessment of Business Impact Levels (BILs) described in DSM Part 2:7 *Business Impact Levels*.
- 5. The authorisation of an entity to access information will be determined by a number of factors including; legislative requirements, need-to-know, security clearance and briefings (if applicable), information release decisions, probity and ethics, and temporary access decisions.
- 6. Suitable controls will be applied to information to ensure that it is protected from unauthorised access or disclosure.

Process

Classifying and Protectively Marking Official Information

Unofficial or Non-Work Related Information

7. The marking UNOFFICIAL may be assigned to information that Defence employees have generated in their private capacity under reasonable use of Defence resource provisions. The application of this marking assists Defence to ensure that this information is not included in official records such as archives. Policy related to personal use of Defence ICT resources is located within the System of Defence Instructions (SODI) in document CIS 6–1–001 Appropriate and inappropriate use of Information and Communications Technology Resources.

Note: Defence employees cannot expect that Defence will apply any specific protective measures to information marked UNOFFICIAL.

8. The UNOFFICIAL marking **must not** [Auth:None] be applied to official government information.

Official Information

- 9. There are two types of official information:
 - a. information that does not need increased security; and
 - b. information that needs increased security to protect its confidentiality.

DSM Part 2:30 Page 2 of 21

- 10. Official information can include public sector information sanctioned for public access or circulation, such as websites.
- 11. Australian Government employees **must** have agency authorisation to release any information to members of the public.
- 12. Authorisation **must** be managed in accordance with:
 - a. DSM Part 2:30 Classification and Protection of Official Information Annex E Release of Official Information; and
 - b. DSM Part 2:54 Internet Content.
- 13. When personal information is involved, any release is required to comply with the *Privacy Act 1988 (Cth)*.
- 14. Official information requiring increased protection is to be marked with the appropriate AGSCS protective marking.
- 15. The AGSCS establishes three types of protective markings: security classifications, Dissemination Limiting Markers (DLM) and caveats.

Note: This DSM part details all security classifications and DLM. It does not cover all applicable caveats, including codewords. Functional areas dealing with information that requires the application of caveats, including codewords, are provided with these protective markings on a need-to-know basis.

- 16. When generating official information, Defence personnel and external service providers **must** [Auth:None]:
 - a. assess the potential damage that could be caused by the compromise of the information;
 - b. identify any legal, regulatory or Cabinet requirements that apply to the information (eg, requirements arising from the *Privacy Act 1988*); and
 - c. assign any required protective marking(s) to the information.
- 17. A flowchart that shows how to select the appropriate protective marking(s) is located at Annex A. The format and manner in which protective markings and accompanying warnings notations are to appear on various forms of material is provided at Annex B.
- 18. In order to promote interoperability within the Australian Government, Defence personnel and external service providers **must not** [Auth:None] use protective markings that are not specified in the DSM.
- 19. It is recommended that the duration and level of a protective marking is limited via the inclusion of declassification instructions with a document. Instructions may be time limited to declassify content on a particular date or after a specific event, however they **must** [Auth:None] include the new marking. This ensures that information may be released to the widest audience at the earliest opportunity.
- 20. Under the AGSCS, official information assessed as not needing additional protection may either remain unmarked or be marked UNCLASSIFIED. It is recommended that the UNCLASSIFIED marking be applied, in lieu of leaving the information unmarked, as this indicates that the information has been formally assessed as UNCLASSIFIED.
- 21. Classification requirements for individual topics or projects may be communicated to Defence employees and external service providers via mechanisms such as Defence Instructions and Security Classification and Categorisation Guides (SCCG).

DSM Part 2:30 Page 3 of 21

Unclassified Official Information

- 22. Official information that does not meet the criteria for the application of a security classification is UNCLASSIFIED official information.
- 23. Both UNCLASSIFIED and classified information may require additional protections offered by the application of a DLM, the criteria for applying a DLM is at paragraph 34.

Preventing Over-Classification

- 24. Information is only to be protectively marked when the results of compromise warrant the expense of increased protection or there is a legislative or regulatory basis for the information to be protected. It is important that information not requiring protection remains UNCLASSIFIED.
- 25. Inappropriate over-classification has many seriously harmful effects, including:
 - a. public access to government information becomes unnecessarily limited;
 - b. unnecessary, administrative arrangements are set up that remain in force for the life of the document, including repository arrangements for records transferred to the National Archives of Australia, imposing an unnecessary cost on the Government;
 - c. the volume of security classified information becomes too large for an agency to protect adequately; and
 - security classification and associated security procedures are brought into disrepute if the
 protective marking is unwarranted, leading to protective markings in general being devalued or
 ignored.
- 26. For these reasons, the Australian Government expects that Defence personnel and external service providers will only protectively mark information and preserve that marking when there is a clear and justifiable need to do so.
- 27. Official information **must not** [Auth:None] be protectively marked in order to:
 - a. hide violations of law, inefficiency or administrative error;
 - b. prevent embarrassment to an individual, organisation or agency;
 - c. restrain competition; or
 - d. prevent or delay the release of information that does not need protection in the public interest.

AGSCS Security Classifications

- 28. The AGSCS has four levels of security classification. These classifications reflect the consequences of the compromise of information, as follows:
 - a. TOP SECRET requires the highest degree of protection as compromise could cause:
 - (1) exceptionally grave damage to national security; or
 - (2) exceptionally grave damage to the national interest more broadly.
 - b. **SECRET** is used where compromise could cause:

DSM Part 2:30 Page 4 of 21

- serious damage to national security;
- (2) serious damage to the national interest more broadly; or
- (3) serious damage to organisations or individuals.
- c. **CONFIDENTIAL** is used where compromise could cause:
 - damage to national security;
 - (2) significant damage to the national interest more broadly; or
 - (3) significant damage to organisation or individuals.
- d. **PROTECTED** is used where compromise could cause
 - (1) minor damage to national security;
 - (2) damage to the national interest more broadly; or
 - (3) damage to organisations or individuals.

Note: For examples of the impacts associated with each classification, refer to DSM Part 2:7 *Business Impact Levels* and its annexes.

Note: The initial release of the AGSCS included **PROTECTED** as a classification. However its definition did not include national security criteria and was not to be used to mark information requiring protection purely on national security grounds. However Version 2 of the AGSCS (released across government on 1 November 2014) changed this intention and PROTECTED can now be used to mark information requiring protection on national security grounds.

29. Some of Defence's international partners are required to treat Australian **PROTECTED** information as **CONFIDENTIAL**. The use of this classification may result interoperability issues. A document may contain information covered by more than one classification. Where this occurs, the compilation of classified information **must** [Auth:None] be assessed against the criteria above and the appropriate classification assigned to the document. This classification must [Auth:None] be at least as high as the most highly classified information or paragraph within the document.

Former Security Classifications

- 30. Some security classifications have been phased out and replaced with AGSCS equivalents; the following paragraphs detail grandfathering arrangements.
- 31. Since 31 July 2014, the former security classification HIGHLY PROTECTED cannot be used on active Defence records. Records reused since this date **must** [Auth:Sec] be remarked SECRET. Records and documents that are inactive or archived do not require remarking unless they are reused. Inactive and archived records are protected as for SECRET material.
- 32. Since 31 July 2014, the former security classification of RESTRICTED cannot be used on active Defence records. Records reused since this date **must** [Auth:Sec] be remarked using the DLM 'For Official Use Only' (FOUO). Records and documents that are inactive or archived do not require remarking unless they are reused. Inactive and archived records are protected as for FOUO material.
- 33. The remarking of documents from former classifications to AGSCS equivalents does not require the permission of the document's originator. However any caveats such as codeword or release markings can not be modified under these provisions.

DSM Part 2:30 Page 5 of 21

AGSCS Dissemination Limiting Markers

- 34. AGSCS DLM are protective markings that are assigned to information where disclosure may be limited or prohibited by legislation, or where the information may otherwise require special handling. DLM include:
 - a. FOUO;
 - b. Sensitive;
 - c. Sensitive: Personal;
 - d. Sensitive: Legal; and
 - e. Sensitive: Cabinet.
- 35. It is recommended that all information marked with a DLM carry a warning notation that indicates the specific nature of the DLM. For commercially sensitive information, health information or information marked with the Sensitive DLM, the inclusion of a warning notation is raised to a mandatory requirement. Details for these categories and their mandatory warning notations are included in the description of each DLM below.
- 36. Where a warning notation is used with a DLM it **must** [Auth:None] be included in the document's cover sheet (where a cover sheet is used). For email, the warning notation is included at the top of the email. In other situations, it is to be included as the first line of text or in the footer.

Note: The inclusion of warning notations in message metadata is not mandatory for automated ICT system to system communications that are not intended for end users.

- 37. To restrict wide and unnecessary dissemination of protectively marked information, it is recommended that limited distribution lists be used when distributing DLM marked information. The subject line of the message, minute or email can also be used to indicate the requirement for limited distribution.
- 38. A document may contain information covered by more than one DLM. Where this occurs the document **must** [Auth:None] be marked with all applicable DLM and warning notations.

Exclusion: Special requirements for FOUO exist, refer to FOUO information below.

- 39. Due to legacy ICT issues, email systems permit only one DLM to be selected for placement in the email subject line. Where more than one DLM applies to email they **must** [Auth:None] be included at the top of the email body. The most restrictive DLM should be applied in the subject line.
- 40. When importing email into Objective, only the first DLM will be automatically identified. Any DLM in the email body **must** [Auth:None] be added to Objective metadata manually in order to meet archiving and protective marking requirements.
- 41. With the exception of 'Sensitive: Cabinet' (which attracts a minimum classification of PROTECTED) DLM may be applied to UNCLASSIFIED information, ie, with information that does not warrant a security classification of PROTECTED or above. In this instance the preferred method of marking is for DLM to be used alone in the classification header and footer.

Example: A document is marked as 'Sensitive: Legal' not as UNCLASSIFIED 'Sensitive: Legal'.

Note: FOUO can only be used with UNCLASSIFIED information but is marked as FOUO not as UNCLASSIFIED FOUO see below.

42. **For Official Use Only.** FOUO is used on unclassified information only, where its compromise may cause limited damage to national security, Australian Government agencies, commercial entities or members of the public.

DSM Part 2:30 Page 6 of 21

- 43. As indicated by its definition, FOUO replaces:
 - a. the former security classification of RESTRICTED, which was previously applied to information that "may cause limited damage to national security";
 - b. the former marking of 'Commercial-in-Confidence', which was previously applied to information that 'may cause limited damage to ... commercial entities'; and
 - c. a range of former 'X-in-Confidence' markers including 'Audit-in-Confidence', 'Security-in-Confidence' and 'Committee-in-Confidence'.

Exclusion: If the information marked 'Audit-in-Confidence' or 'Security-in-Confidence' contains personal information it must be marked with 'Sensitive: Personal'.

44. FOUO can not be used in conjunction with classified information.

Example: A single paragraph in a document is marked either FOUO or PROTECTED, it can not be marked PROTECTED FOUO.

- 45. When marking documents that contain FOUO information and other content, the following applies:
 - a. If the document contains no information classified PROTECTED or above then there is no requirement to include the UNCLASSIFIED marking in the classification header and footer, the preferred notation is to use FOUO alone. Writing it as UNCLASSIFIED FOUO is superfluous as FOUO information can only be used with information that is unclassified.

Example: The document is marked FOUO not UNCLASSIFIED FOUO.

b. If the document contains a mix of security classified information at PROTECTED and above, then there is no requirement to include FOUO in the classification header and footer. The inclusion of FOUO is superfluous because the handling requirements of classified documents exceed those of DLM marked documents.

Example: A document containing a mix of SECRET, FOUO and 'Sensitive: Legal' will be marked as 'SECRET Sensitive: Legal'.

46. Where FOUO is used to identify commercially sensitive information, a warning notation that alerts the recipient to the commercial sensitivities **must** be included in the document and commence with the statement: 'This document contains commercially sensitive information'.

Note: The commercial warning notation can be applied in addition to any protective marking, FOUO and above. Where UNCLASSIFIED commercial information is not sensitive enough to warrant a warning notation, it is recommended originators consider using a distribution list.

47. The warning notation on commercially sensitive information may be generic:

Example: 'This document contains commercially sensitive information. The disclosure and use of this information may be subject to additional constraints.'

48. Where additional information is available, the use of a specific warning is recommended.

Example: 'This document contains commercially sensitive information supplied by company y related to tendering for project x. The disclosure and use of this information is restricted to staff conducting project x tender evaluations'.

- 49. See Annex B, Appendix 1 for an example of how commercially sensitive information is to be marked.
- 50. **Sensitive.** The Sensitive DLM **must** [Auth:None] be applied to any unclassified or classified information:

DSM Part 2:30 Page 7 of 21

- a. where the secrecy provisions of legislation may apply;
- b. where disclosure may be limited or prohibited under legislation; or
- c. which may fall under the category of an 'exempt document' under the *Freedom of Information Act 1982, Part IV, Section 38.*
- 51. The originator **must** [Auth:None] apply a warning notation that identifies the legislative basis on which the Sensitive DLM has been applied and any special handling requirements, either in the footer or as a cover page. If the legislative basis can not be identified, the Sensitive DLM **must not** [Auth:None] be used. Following is a non-Defence example of a warning notation that could be applied with the Sensitive DLM:

Example: 'Sensitive: This information is 'protected information' as described in Section 56 of the *Australian Prudential Regulation Authority Act 1998* and may only be accessed by APRA officers'.

- 52. Within Defence, the responsibility for determining the application of any specific legislative provisions rests with the information originator. Any subsequent reuse of that information then carries the DLM as well as the warning notation assigned by the originator.
- 53. Defence employees are advised that the use or release of sensitive information for purposes other than provided for in relevant enabling legislation may be in breach of Australian law and may render Defence or the employee liable to sanction including prosecution under the relevant legislation. If in any doubt, contact the originator of the information to obtain further instructions.
- 54. **Sensitive: Personal.** The 'Sensitive: Personal' DLM **must** [Auth:None] be applied to any unclassified or classified information that:
 - a. is 'sensitive information' as interpreted under the Privacy Act 1988, Part II, Section 6; or
 - b. may fall under the category of 'documents affecting personal privacy' under the *Freedom of Information Act 1982, Part IV, Section 47F 'Public interest conditional exemptions personal privacy'*.
- 55. While wider in scope, the 'Sensitive: Personal' DLM replaces the former markings of 'Medical-in-Confidence' and 'Psychology-in-Confidence'.
- 56. Where 'Sensitive: Personal' is used to identify sensitive health information, a warning notation of 'Health Information' **must** be included below the DLM in the document to alert recipients of the requirement to handle and store the information in accordance with DI(G) PERS 16-20 *Privacy of Health Information in Defence*. See Annex B, Appendix 2.
- 57. All 'Sensitive: Personal' information, whether or not it is also publicly available, **must** [Auth:None] be handled in accordance with the Information Privacy Principles (IPP) in the *Privacy Act 1988*.

Exclusion: The Australian Geospatial-Intelligence Organisation (AGO), the Australian Signals Directorate (ASD) and the Defence Intelligence Organisation (DIO) are exempt agencies under the *Privacy Act 1988*. Exclusions apply to the operation of these agencies and the intelligence product that they produce in respect to the *Privacy Act 1988*.

- 58. **Sensitive:** Legal. The 'Sensitive: Legal' DLM must [Auth:None] be applied to any unclassified or classified information that may be subject to legal professional privilege as provided by the *Freedom of Information Act 1982, Part IV, Division 2, Section 42.*
- 59. A statutory definition of 'legal professional privilege' (also referred to as 'client legal privilege') is outlined in the *Evidence Act 1995, Part 3.10, Division 1* as it applies to evidence being led in Commonwealth proceedings. Other jurisdictions have similar statutory definitions. Legal professional privilege also exists in common law.

DSM Part 2:30 Page 8 of 21

- 60. The 'Sensitive: Legal' DLM replaces the former marking 'Legal-in-Confidence'.
- 61. **Sensitive: Cabinet.** The 'Sensitive: Cabinet' DLM **must** [Auth:None] be applied, together with a minimum security classification of PROTECTED, to any information which may fall under the category of 'Cabinet documents' as defined in the *Freedom of Information Act 1982, Part IV, Section 34* or the Cabinet Handbook. This includes:
 - a. any document including, but not limited to business lists, minutes, submissions, memoranda and matters without submission that is or has been submitted, or proposed to be submitted to Cabinet:
 - b. official records of Cabinet;
 - c. any other information that would reveal:
 - (1) the deliberations or decisions of Cabinet; or
 - (2) matters submitted, or proposed to be submitted to Cabinet.
- 62. 'Sensitive: Cabinet' documents are 'Accountable Material' and **must** [Auth:None] be handled as 'Accountable Material' in accordance with the Cabinet Handbook, which is issued by the Department of the Prime Minister and Cabinet. These documents do not require the application of the caveat 'Accountable Material' to the document. For further guidance refer to the Cabinet Handbook.
- 63. More general Cabinet-related communications such as those with broad reference to Cabinet deliberations **must** be marked PROTECTED (as a minimum) and 'Sensitive: Cabinet' but can be sent either on the DRN or the Defence Secret Network (DSN) depending on the accompanying classification.

Example: An email stating 'we need to discuss policy X in order to produce a Cabinet submission for the meeting of day X' is considered Cabinet-related business and can be communicated on Defence systems with a minimum classification of PROTECTED.

64. The 'Sensitive: Cabinet' DLM replaces the former marking of Cabinet-in-Confidence.

Former X-in-Confidence Markings

- 65. Under the PSPF, all X-in-Confidence markings have been phased out and replaced with equivalent AGSCS protective markings. The following paragraphs detail grandfathering arrangements for these markings.
- 66. The former X-in-Confidence markings cannot be used on active Defence records after 31 July 2014. Records that are reused after this date **must** [Auth:Sec] be remarked with their equivalent AGSCS protective marking.
- 67. Records and documents that are inactive or archived do not require remarking unless they are reused. Inactive and archived records are protected in accordance with any assigned classification, or in the case of UNCLASSIFIED information as per DLM marked material.
- 68. X-in-Confidence material **must** [Auth:None] be remarked in accordance with Table 2:30-1.
- 69. Former X-in-Confidence markings that are not included in Table 2:30-1 **must** [Auth:None] be assessed against the AGSCS DLM criteria and have the appropriate DLM applied.
- 70. Remarking of documents from former X-in-Confidence markings to the equivalent AGSCS DLM does not require the permission of the originator. However any caveats such as CODEWORD or release markings can not be modified under these provisions.

DSM Part 2:30 Page 9 of 21

Former Marking	AGSCS Dissemination Limiting Marker (DLM)
Commercial-in-Confidence	For Official Use Only
Audit-in-Confidence	
Security-in-Confidence	
Committee-in-Confidence	
Cabinet-in-Confidence	Sensitive:Cabinet
Legal-in-Confidence	Sensitive:Legal
Medical-in-Confidence.	Sensitive:Personal
Psychology-in-Confidence	
Client-in-Confidence	
Staff-in-Confidence	
Honours-in-Confidence	
Audit-in-Confidence*	
Security-in-Confidence*	
* Only when personal information is collected	

Table 2:30-1: Mapping of former X-in-Confidence Markings to AGSCS Equivalents

AGSCS Security Caveats

- 71. Security classified information may bear a security caveat in addition to a security classification. The caveat is a warning that the information has special requirements in addition to those indicated by the protective marking.
- 72. Caveats are not classifications in their own right. They **must** [Auth:None] only be used with classifications of PROTECTED or above.
- 73. The different categories of security caveat are:
 - a. codewords (including source codewords and compartmented information);
 - b. releasability indicators:
 - (1) Eyes Only (including Australian Eyes Only (AUSTEO));
 - (2) Australian Government Access Only (AGAO)
 - (3) RELEASABLE TO (REL);
 - c. special handling; and
 - d. Accountable Material.
- 74. There are specific limitations on the production and storage of information bearing security caveats on ICT systems. System users **must** [Auth:None] only create, process or store information on systems which have been accredited to process such caveats. System Standard Operating Procedures (SOP), formerly referred to as 'ISSPP', detail the classifications and caveats that can be processed on each accredited

DSM Part 2:30 Page 10 of 21

system. Users are to refer to a system's SOP if there is any doubt whether the caveat can be processed or stored on the system.

Codewords¹

- 75. A codeword signifies a special need-to-know category of information and can be assigned to operations, information or material. A codeword, which is used to identify the source of certain information without revealing it to those who do not have a need-to-know, is known as a source codeword. Formal information compartments can be assigned one or more codewords.
- 76. **Compartmented information.** Compartment briefings referred to as CHARLIE, DELTA, ECHO and GAMMA are required to access certain codeword information. These briefings can only be provided to individuals who hold the required clearance as detailed in Table 2:30-2. For further information on security clearances see DSM Part 2:20 *Personnel Security Clearance Process*.

Briefing	Minimum security clearance and briefing held
C (CHARLIE)	Negative Vetting Level 1
D (DELTA)	Negative Vetting Level 2
E (ECHO)	Positive Vetting and Delta briefed
G (GAMMA)	Positive Vetting and Delta briefed

Table 2.30-2: Security Clearance Requirements for Compartment Briefings

- 77. Information covered by the DELTA, ECHO and GAMMA compartments is Sensitive Compartmented Information (SCI). The CHARLIE compartment is managed by Defence for Defence personnel only, on behalf of the compartment controller.
- 78. Guidance and requirements for handling information from the Defence intelligence agencies can be obtained from the Defence Intelligence Security website on the DSN or from the nearest Communications Intelligence Security Officer (COMSO). Further information and requirements associated with intelligence information including SCI, is available in the *Australian Government Sensitive Material Security Management Protocol* on the DSN DS&VS intranet site.

Special Access Program

- 79. Additional requirements that apply to the handling of information relating to the Defence Special Access Program are in DI(G) Admin 62-1 *Defence Special Access Programs Policy and Management.*
- 80. Unauthorised access to compartmented information by people who do not hold the briefing for that compartment constitutes a major security incident. Requirements for responding to security incidents are detailed in DSM Part 2:12 Security Incidents and Investigations. If you are exposed to a codeword that you are not currently authorised to access or do not recognise, then report it as a security incident and seek advice from your security officer immediately. Early reporting assists in preventing further distribution of such information.
- 81. Defence personnel and external service providers **must** [Auth:None] receive permission from the originator if compartmented information needs to be held outside the originator's facility or an accredited Sensitive Compartment Information Facility (SCIF).

DSM Part 2:30 Page 11 of 21

.

¹ Paragraphs 75 – 78 are redacted from the public version of this DSM part.

- 82. Permission from the originator to file the documents in a specific location **must** be recorded. If granted, personnel are to contact the ASD Records Management area to request a Special Series File. ASD is responsible for all Defence records management functions for Special Series files or SCI records including file requests, musters, sentencing, storage, and disposal.
- 83. All SCI material and material in the Charlie compartment **must** [Auth:None] be stored in the Special Series File managed by ASD. The information **must not** [Auth:None]:
 - a. be stored or processed on the Defence Restricted Network (including Objective);
 - b. be stored or processed on the DSN (including Objective);
 - c. be held in any department corporate file other than a Special Series File; or
 - d. be transferred to central registries or to the national archives.
- 84. When no longer required, all Special Series Files **must** be returned to ASD.

Note: Special provisions for the custody of intelligence information are made in the *Archives Act* Section 29(8). Further information can be found in the *Defence Records Management Policy Manual* (POLMAN 3).

Releaseability Indicators

- 85. Releaseability indicators are AGSCS caveats which permit or limit the release of information to specified nations or coalitions of nations.
- 86. The DRN is not accredited to store, process or communicate information bearing releasability indicators. In order to ensure that Defence remains compliant with various requirements of the ISM, information bearing these caveats **must not** [Auth:None] be produced or stored on the DRN.
- 87. Eyes Only and RELEASABLE TO (often abbreviated to 'REL') caveats indicate that access to information is restricted to specific nationalities or coalitions of nations, for example:
 - a. Australian Eyes Only, which is abbreviated to AUSTEO;
 - b. Australian and United States Eyes Only, which is abbreviated to AUS/USA Eyes Only; and
 - RELEASABLE TO, is abbreviated to REL;
 - d. REL AU/NATO indicates that material is releasable to Australia and NATO.

Note: The EO and REL caveats carry the same requirements; however the format varies depending on the information system in use and matters of interoperability between nations.

- 88. Information marked 'Eyes Only', 'RELEASABLE TO', 'REL:' REL TO:' **must not** [Auth:None] be passed to or accessed by foreign nationals whose nation is not listed in the caveat. It may be possible to have the caveat changed by the originator for all or part of the information. However, the caveat **must not** [Auth:None] be removed or changed without the written permission of the information originator.
- 89. For interoperability purposes, this material when produced by Defence is to be marked with the Australian releasability indicator (eg, 'AUS' or 'AU'). This is to prevent the situation of a foreign government not being able to return the information to Australia because it was not marked as being releasable to Australia.
- 90. **Australian Eyes Only.** The use of the AUSTEO caveat is to be strictly limited and **must** [Auth:None] be approved by an SES Band 1 / O7 officer or higher.

DSM Part 2:30 Page 12 of 21

91. Access to information marked with the AUSTEO caveat **must** [Auth:None] only be passed to appropriately cleared Australian citizens.

Note: Australian citizens who hold dual citizenship with another country and have been granted an Australian clearance have had their allegiance and loyalty to Australia assessed during the security clearance process. They are therefore eligible to access AUSTEO information.

- 92. Foreign nationals **must not** [Auth:None] be allowed access to AUSTEO information, even if they have an Australian security clearance granted under a citizenship eligibility waiver.
- 93. It may be possible to have the AUSTEO caveat changed by the originator for all or part of the information. However, the caveat **must not** [Auth:None] be removed or changed without the written permission of the originator.
- 94. **Australian Government Access Only** (AGAO). Information with the AGAO caveat **must not** [Auth:None] be released to a foreign government, foreign company or any foreign entity, including foreign contractors with a foreign security clearance.
- 95. AGAO differs from AUSTEO in that it may be released to US, UK, CA and NZ nationals that are integrated in, or working on behalf of, the Australian Government and have a legitimate need-to-know in the conduct of duties.
- 96. AGAO access **must** [Auth:None] be limited to people with a need-to-know, an appropriate level security clearance (for the accompanying classification), and who are either:
 - a. Australian Government employees or external service providers who are Australian citizens (such as members of the Defence Industry Security Program);
 - b. US, UK, CA or NZ nationals who have been granted an Australian security clearance on the basis of a citizenship eligibility waiver.

Note: Limitations apply to the extent of information access that can be granted under a citizenship eligibility waiver. See DSM Part 2:20 *Personnel Security Clearance Processes* for further information on the operation of these restrictions.

- c. US, UK, CA or NZ nationals who are integrated as officers of the Australian Government (Integrated Officers), whether located in Australia or Overseas.
 - (1) An Australian security clearance with citizenship eligibility waiver is not required; however they must [Auth:None] hold a current equivalent level clearance issued by their government.

Example: A US citizen who is seconded by the US government to work in an Australian project office located in the US is eligible for AGAO access.

Example: A foreign contractor with a recognised US issued clearance in the same project office is not eligible for AGAO access and would require an Australian clearance issued on the basis of a citizenship eligibility waiver in order to access AGAO. They can however access REL AU/US information.

Example: A member of the NZ Defence Force with a NZ SECRET clearance seconded to an ADF unit is eligible for AGAO access but can not access REL AU/US material.

- 97. AGAO information **must not** [Auth:None] be made accessible to US, UK, CA or NZ nationals accessing Defence networks from coalition gateways. In this circumstance these nationals are working on behalf of their own government and are not entitled to access AGAO.
- 98. With the exception of those covered by exchange arrangements within the Defence intelligence agencies, foreign nationals granted approval to access AGAO information **must** sign a *Certificate of*

DSM Part 2:30 Page 13 of 21

Assurance for Access to Australian Government Access Only (AGAO) information by United States, United Kingdom, Canadian or New Zealand nationals. A template of this certificate is located on the Defence Security Portal.

Special Handling Caveat

- 99. A special-handling caveat is a collection of various indicators such as operation codewords, instructions to use particular communications channels and 'EXCLUSIVE FOR (either a person or a position title)'. This caveat is usually used only within particular 'need-to-know' compartments.
- 100. Where information is marked 'EXCLUSIVE FOR (a person)' it is not position based and **must** [Auth:None] only be accessed by the person named in the instruction. Permission **must** [Auth:None] be sought from the originator before granting access to any other persons.

Accountable Material

- 101. If strict control over other classified information is required, it can be deemed Accountable Material by the originator.
- 102. Cabinet documents, TOP SECRET information and codeword material **must** [Auth:None] always be treated as 'Accountable Material'.

Exclusion: Handling exemptions exist for source codeword and some other Accountable Material when being handled within an originating intelligence agency's premises. Intelligence Agency staff are to refer to their agency's document handling procedures for further information on the operation of exclusions to this policy within their agency.

- 103. Accountable Material must [Auth:None]:
 - a. be marked with ACCOUNTABLE MATERIAL in bold print on the front cover of the material.

Exclusion: Application of the marking is not required for Cabinet documents, TOP SECRET information and CODEWORD material.

- b. carry a reference and individual copy number each page is accountable by numbering (eg, page 3 of 10) and placing the document copy number on each page;
- c. carry a warning such as 'not to be copied without the prior approval of the originator';
- d. be passed by hand or 'safe hand' transfer and be receipted; and
- e. be registered in a separate register that contains a record of all persons granted access to each accountable document. The central register is separate from the movement record which forms part of the document or file.
- 104. Refer to Annex C for information on managing accountable non-cryptographic publications.

Altering Protective Markings

105. Protective markings (security classifications, DLM, and caveats) **must not** [Auth:None] be remarked (ie, downgraded, removed or modified) without the written permission of the originator of the information. Any modification of a protective marking without the originator's authority **must** [Auth:None] be immediately reported as a major security incident.

Exclusion: Where the originator has included declassification instructions within a document further permission to remark the document is not required provided the instructions are met.

DSM Part 2:30 Page 14 of 21

Exclusion: Remarking of documents from former markings to their AGSCS equivalents does not require the permission of the originator. However any caveats such as codeword or release markings can not be modified under these provisions.

106. Further information for reviewing and altering classifications is provided at Annex D.

Protecting Official Information

107. Defence personnel and external service providers **must** ensure that official information is protected from unauthorised access as indicated by the protective markings.

Note: The combined effect of sections 70 and 79 of the *Crimes Act 1914* and section 91.1 of the *Criminal Code 1995* is that the unauthorised disclosure of information held by the Australian Government is subject to the sanction of criminal law.

- 108. This applies to information in any form, including oral, written, electronic, documentary, visual, briefings, material and equipment. Requirements for access, handling and storage of official information are listed, or referred to, below.
- 109. **Document handling training.** All Defence personnel and external service providers who access official information as part of their duties, **must** complete DS&VS document handling training at the appropriate level. There are two available courses:
 - a. the Classified Document Handling course is for Defence personnel and external service providers who have access to material marked CONFIDENTIAL or above.
 - b. the Basic Document Handling course is for Defence personnel and external service providers who have access to material marked PROTECTED and below.
- 110. Defence personnel and external service providers who completed document handling training prior to June 2014 **must** complete an updated version of the applicable course.

Note: In June 2014, DS&VS released updated document handling training based on the AGSCS. Personnel who completed document handling prior to this need to ensure that they undertake the updated training.

Note: Courses published prior to June 2014 can not be used as evidence to support competency or proficiency in current document handling procedures.

- 111. Defence personnel and external service providers who have completed the Basic Document Handling course **must** also complete the Classified Document Handling course if:
 - a. a change in their clearance and/or duties means that they will handle material marked CONFIDENTIAL or above; or
 - b. they are granted access to material marked CONFIDENTIAL or above through temporary access provisions.
- 112. **Security clearance**. Defence personnel and external service providers **must** ensure that access to official information is limited to those who have the level of security clearance required. For further information see DSM Part 2:20 *Personnel Security Clearance Process*.
- 113. **Need-to-know principle**. Defence personnel and external service providers **must** ensure that access to official information is limited to those who need to know the information for their official duties. This is called the need-to-know principle.

Exclusion: Unclassified information that has been formally approved for public release is not subject to the need to know principle.

DSM Part 2:30 Page 15 of 21

- 114. **Release of official information.** Requirements for the release of official information (including to other Australian Government agencies, to industry, under Freedom of Information requests, for court proceedings and to Parliamentary Committees) are provided in Annex E.
- 115. **Foreign Release.** Requirements for the release of classified information to foreign governments are provided in DSM Part 2:32 *Foreign Release of Official Information*.
- 116. **Physical transfer of official information**. Requirements for the removal and physical transfer of classified information are provided in detail in DSM Part 2:33 *Physical Transfer of Classified Information and Security-Protected Assets*.
- 117. **Electronic transmission of official information**. Requirements for the electronic transmission of classified information are provided in the ISM.
- 118. **Clear desk and screen.** Personnel are responsible for the security of official information under their control. During absences from their workplace, Defence personnel and external service providers **must** ensure that official information that is protectively marked is not left unattended and is secured appropriately in order to prevent access by those without a need-to-know. This is known as the clear desk and screen policy.
- 119. **Loss.** Any loss of classified information is a security incident. The requirements for reporting and investigating security incidents are provided in DSM Part 2:12 *Security Incidents and Investigations*.
 - **Note:** Early reporting in accordance with DSM Part 2:12 *Security Incidents and Investigations* may prevent further compromise and minimise the extent of damage of the security incident.
- 120. **Registration**. Requirements for the registration of official information held by Defence are provided in Annex F.
- 121. **Filing**. Requirements for the filing of official information are provided in Annex G, the *Archives Act* 1983, and the Defence Records Management Policy Manual.
- 122. **Copying and reproduction**. Requirements for the copying or reproduction of official information are provided in Annex H.
- 123. Disposal. Requirements for the disposal and destruction of classified material are provided in Annex I.
- 124. Off-site Work. Requirements for off-site work are provided in DSM Part 2:31 Off-site Work.
- 125. **Accountable non-cryptographic publications**. Instructions on managing accountable non-cryptographic publications can be found in annex C.
- 126. **Physical access and storage**. Requirements for the physical access and storage of official information and assets are provided in DSM Part 2:60 *Physical Security*.
- 127. **Close of day checks**. At the close of business each day, personnel are to take precautions to ensure that official information, especially protectively marked information, is protected from unauthorised access. It is recommended that security officers devise a workplace lock-up procedure which may include, but not be limited to the following:
 - a. logging off all systems and, if required, switching the machine off;
 - b. ensuring there is no security classified information left out in the workplace;
 - ensuring that laptops and other electronic media storing security classified information are secured;

DSM Part 2:30 Page 16 of 21

- d. ensuring there is no security classified information in waste-paper bins;
- e. ensuring that whiteboards and other displays do not show any security classified information (special care needs to be taken with electronic whiteboards);
- f. ensuring vaults and containers are locked;
- g. ensuring windows and doors are locked; and
- h. ensuring that keys to containers are secure.
- 128. It is also recommended that security officers put in place an appropriate system for checking the workplace at close of business (or the end of shifts) to ensure that security classified information is secured.
- 129. **Aggregated information.** Certain compilations of information may require the application of higher or additional security controls than individual documents or pieces of information within the compilation. This is because the business impact from the compromise of confidentiality, loss of integrity or unavailability of the aggregated information would cause greater damage than that of individual documents, see DSM Part 2:7 *Business Impact Levels* for further information.

Roles and Responsibilities

Group Heads and Service Chiefs

- 130. Group Heads and Service Chiefs are responsible for:
 - a. the implementation and maintenance of information security procedures within the areas under their control and within Defence in general;
 - b. ensuring the specification and maintenance of adequate security measures for information systems and their data; and
 - c. ensuring procedures conform to the minimum standards detailed in this DSM part.

First Assistant Secretary Security and Vetting Service and the Service Security Authorities

131. The First Assistant Secretary Security and Vetting Service (FAS S&VS) and the Service Security Authorities (SSA) are responsible for the provision of advice regarding the classification and protection of official information. The SSA perform this function for their respective Services.

Commanders and Managers

- 132. Commanders and managers are responsible for:
 - a. the security of information under their direct control;
 - ensuring that official information is marked with the required protective marking;
 - ensuring that employees hold an appropriate security clearance and comply with the appropriate protective security procedures for handling official information;
 - d. determining which of their staff have a 'need-to-know' and will require access to official information;

DSM Part 2:30 Page 17 of 21

- e. providing a secure environment that is appropriate to the security classification of official information held, processed or received by their unit or business unit; and
- f. compliance with this DSM part.

Defence Personnel and External Service Providers

- 133. All Defence personnel and external service providers are responsible for:
 - a. classifying official information they generate in the course of their duties; and
 - protecting official information that is not eligible for public release in accordance with the assigned protective marking.

Security Officers

134. Security officers are responsible for assisting the relevant commander or manager with administrative actions that enable compliance with this DSM part. They are the first point of contact for security concerns and queries by employees and provide security advice and assistance to commanders and managers, employees and others who have access to official information.

Key Definitions

- 135. **Official information.** Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and external service providers, that includes:
 - a. documents and papers;
 - b. data;
 - software or systems and networks on which the information is stored, processed or communicated;
 - d. intellectual information (knowledge) acquired by individuals; and
 - e. physical items from which information regarding design, components or use could be derived.
- 136. **Unofficial information.** Non-work related information generated by Defence employees under reasonable use of Defence resource provisions, typically contained in email, faxes etc.
- 137. **Originator.** The entity that created the official information or on whose behalf the official information was created. An originator can be:
 - a. a military or business unit within Defence;
 - an Australian Government department or agency;
 - a foreign government; or
 - a person who has been authorised and has received appropriate training to conduct declassification of intelligence information within specified intelligence compartments on behalf of the intelligence compartment controller.
- 138. **Classification process.** The process by which the confidentiality requirements of official information are assessed and the appropriate protective markings applied.

DSM Part 2:30 Page 18 of 21

- 139. **Protective marking.** A marking given to official information that is sensitive or security classified to indicate the level of protective measures that are to be applied during use, storage, transmission, transfer and disposal so as to reduce the risk of unauthorised disclosure. There are three types of protective markings:
 - a. security classifications;
 - b. dissemination limiting markers; and
 - security caveats.
- 140. **Security classification.** A type of protective marking assigned to security classified information that indicates the consequence of unauthorised disclosure and convey to users the level of protection needed during use, storage, transmission, transfer and disposal.
- 141. National Interest. A matter which has or could have an impact on Australia, including:
 - national security;
 - b. international relations:
 - c. law and governance, including:
 - (1) inter state/territory relations;
 - (2) law enforcement operations where compromise could hamper or prevent national crime prevention strategies or endanger personal safety;
 - d. economic wellbeing; and
 - e. heritage or culture.
- 142. **National security information.** National security information is any official resource (including assets) that records information about or is associated with Australia's:
 - a. protection from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and the protection of Australia's territorial and border integrity from serious threats; or
 - b. Defence capability.
- 143. **Dissemination limiting marker.** A protective marking assigned to information which requires special handling due to legal, regulatory, privacy or Cabinet requirements or other sensitivities.
- 144. **Security caveat.** A protective marking applied to security classified information indicating that special protective requirements apply in addition to those associated with its security classification.
- 145. **Public release.** Unlimited public access or circulation of official information, for example by way of Defence publications or websites. The need-to-know principle does not apply once the information enters the public domain.
- 146. File. Either:
 - a. an organised unit of documents, accumulated during current use and kept together because they deal with the same subject, activity or transaction; or

DSM Part 2:30 Page 19 of 21

- b. in electronic archives and records, two or more data records dealing with the same subject, activity or transaction that are treated as a unit.
- 147. **Record.** Defined by the *Archives Act 1983* as a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of:
 - a. any information or matter that it contains or that can be obtained from it; or
 - b. its connection with any event, person, circumstance or thing.
- 148. **Commonwealth record.** Defined by the *Archives Act 1983* as a record that:
 - a. is the property of the Commonwealth or a Commonwealth institution; or
 - b. is deemed to be a Commonwealth record by virtue of the *Archives Act 1983*, but does not include a record that is exempt material or is a register or guide maintained in accordance with Part VIII of the *Archives Act 1983*.

Further Definitions

149. Further definitions for common DSM terms can be found in the Glossary.

Annexes and Attachments		
Annex A	Selecting an Appropriate Protective Marking	
Annex B	Applying Protective Markings to Official Information	
Annex C	Managing Accountable Non-Cryptographic Publications	
Annex D	Reviewing and Altering Protective Markings	
Annex E	Release of Official Information	
Annex F	Registration of Protectively Marked Information	
Annex G	Official Information Filing and File Census	
Annex H	Copying and Reproduction of Protectively Marked Information	
Annex I	Disposal and Destruction of Protectively Marked Information and Assets	

Defence Security and Vetting Service Intelligent security for an insecure world



EXECUTIVE SERIES

RULES OF ENGAGEMENT

ADDP 06.1









AUSTRALIAN DEFENCE DOCTRINE PUBLICATION

Edition 3



ADDP 06.1

RULES OF ENGAGEMENT

Australian Defence Doctrine Publication (ADDP) 06.1—*Rules of Engagement* edition 3 is issued for use by the Australian Defence Force and is effective forthwith. This publication supersedes ADDP 06.1 edition 2.

The fall of

Angus J Campbell, AO, DSC General Chief of the Defence Force

Department of Defence CANBERRA ACT 2600

6 August 2019



CHAPTER 1

RULES OF ENGAGEMENT

INTRODUCTION

- 1.1 **Definition.** Rules of engagement (ROE) are Chief of the Defence Force (CDF) directives issued to the Australian Defence Force (ADF), in consultation with the Australian Government, which regulate the use of force and activities connected to the use of force. The document by which CDF promulgates ROE is a ROE authorisation (ROEAUTH).
- 1.2 ROE align with Government objectives. ROE do not inhibit or replace the command function; they are a part of it. The purpose of ROE is to regulate the application of military force consistent with Government policies and legal obligations.
- 1.3 ROE do not:
- a. provide a substitute for strategy or tactics
- b. describe specific doctrine, tactics and procedures
- c. address safety-related issues or weapon states.
- 1.4 ROE operate together with other operational documents regulating the mission (such as operation orders) and the use of force, such as targeting directives, orders for opening fire, orders for the use of force, and special instructions. All operational documents must be consistent with ROE; operational documents may be more restrictive than ROE, but never more permissive.
- 1.5 CDF is the authority for issuing, amending and cancelling ROE. Subordinate commanders may further restrict the use of force, but may never authorise a more permissive use of force than that authorised by the ROE.
- 1.6 All military force is regulated by ROE.
- 1.7 The application of ADF ROE to forces embedded into the ADF from other nations will depend on the specific arrangements in place between Australia and the contributing nation.

FUNDAMENTALS

- 1.8 ROE are drafted as a series of permissions. If an action relating to the use of force is not authorised in the ROE, commanders have no authority to carry out that action. Commanders must seek clarification if the authorised ROE are considered unclear, inappropriate or inadequate to cover the military situation.
- 1.9 ROE are a command directive. Key to the proper interpretation of ROE is an understanding of command intent and how that is expressed through the rules.
- 1.10 ROE are to be consistent with the law, and can provide restrictions and constraints in addition to legal requirements. ROE are interpreted and applied in accordance with the law.

Types of rules of engagement

- 1.11 ROE are issued for operations across the full spectrum of military force, from armed conflict through to peacetime operations. There are two broad categories of ROE:
- a. **Standing rules of engagement.** These ROE govern the use of force by the ADF outside of armed conflict and in the absence of operation-specific ROE.
- b. **Operation-specific rules of engagement.** Where planned operations involve ADF force elements, specific ROE are likely to be issued. The ROEAUTH includes the precise scope of application of these ROE. There may be an overlap between the application of standing ROE and operation-specific ROE.
- 1.12 These broad categories of ROE can be modified or amplified in the following ways:
- a. **Multinational force rules of engagement**. Multinational force (MNF) ROE can exist where agreed on between participating nations. CDF may issue direction and guidance that supplements the MNF ROE. When issued, operation-specific ADF ROE have precedence over MNF ROE for ADF members. In some circumstances this will mean the MNF ROE continue to apply to ADF members but they must also comply with any more restrictive rules in the ADF ROE. In other circumstances it will mean that only ADF ROE applies to ADF members and the MNF ROE do not apply.
- b. **Extant rules of engagement**. Extant ROE are those authorised for use and currently active.
- c. **Dormant rules of engagement**. When CDF authorises ROE for a particular operation, dormant ROE may also be issued for implementation either on receipt of a particular code word or in the event of a specified set of circumstances. Dormant ROE may also be issued to advise subordinate commanders of ROE that are likely to be authorised for a subsequent phase of an operation or a given set of events. They allow for forward planning and should provide the commander with the flexibility to counter actions by an adversary when circumstances are changing too rapidly to accommodate the normal ROE approval process. Once activated, dormant ROE form part of the extant ROE.
- d. **Exercise rules of engagement**. Exercise ROE may be issued for the purposes of training, and applies only to activities that are part of the planned exercise. Exercise ROE do not govern the actual use of force. For exercises conducted in peacetime in Australia, the ROE that will govern use of force, should a real-life incident occur, will be the standing ROE.

Formulating and reviewing rules of engagement

1.13 Many factors influence the formulation of ROE. The relative significance of these factors will vary according to the circumstances. Chapter 2 discusses the key overlapping factors in more detail.

1.14 Once formulated, Headquarters Joint Operations Command (or other theatre command headquarters) passes the proposed draft ROE to Military Strategic Commitments (MSC), where consultation will occur, as necessary, with subordinate commands and other government departments. Head Military Strategic Commitments (HMSC) then passes the draft ROE to CDF, who may notify the Minister for Defence. CDF issues the ROE via a ROEAUTH (Chapter 3) to the Chief of Joint Operations (CJOPS) or appropriate theatre commander, who is responsible for further promulgation of the ROE to force elements. On receipt, commanders have an obligation to review the ROE to ensure that they remain consistent with the prevailing circumstances. Commanders should seek clarification if the ROE are considered unclear, inappropriate or inadequate to cover the military situation.

Relationship of rules of engagement to the law

- 1.15 ROE provide authoritative direction on the use of force. ROE are drafted to be consistent with the law, must be interpreted and applied in accordance with the law, but are not themselves law. ROE do not re-state all of the law that is applicable to a military operation.
- 1.16 ROE can provide limitations in addition to legal requirements. These limitations may be imposed for operational and policy reasons.

Contravention of rules of engagement

- 1.17 ROE are orders for the purposes of the *Defence Force Discipline Act 1982*. ROE staff procedures and training are designed to minimise the likelihood of a breach of ROE by ADF force elements. Nevertheless, breaches of ROE may arise through error, accident or misadventure, or potentially in rare cases, through deliberate acts. In the event of an ADF member breaching ROE, the adverse consequences of such breaches are minimised by:
- a. reporting the breach up the chain of command by the quickest means possible
- b. informing lateral and subordinate commands, where the consequences are likely to affect them
- c. implementing remedial measures to avoid a recurrence
- d. if required, subjecting the breach to formal investigation; which may lead to disciplinary, criminal and/or administrative action
- e. considering public information aspects.

CHAPTER 2

KEY FACTORS INFLUENCING RULES OF ENGAGEMENT

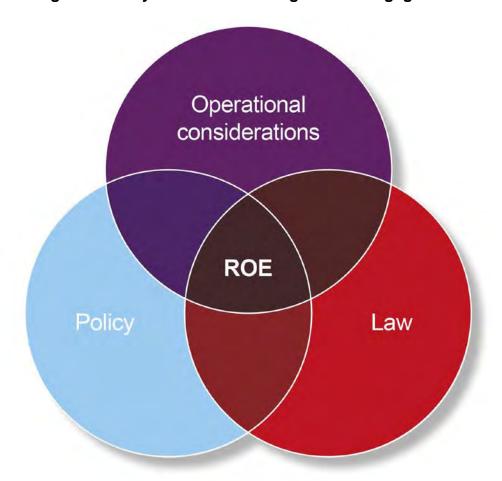
Executive summary

- There are three key factors that influence rules of engagement: law, policy and operational considerations.
- The relative significance of each factor will vary depending upon the nature of the operation.

KEY FACTORS

- 2.1 Many factors influence the formulation of rules of engagement (ROE); the relative significance of these factors will vary according to the circumstances. The three key overlapping factors are:
- a. law
- b. policy
- c. operational considerations.

Figure 2.1: Key factors influencing rules of engagement



Law

- 2.2 ROE must comply with Australian domestic law and be consistent with Australia's international legal obligations.
- 2.3 Foreign domestic law can also influence ROE when the ADF deploys to a host nation in support of, or under an agreement (such as a status of forces agreement) with, the host nation. For example, it may influence the imposition of restrictions on the carriage of weapons by the ADF within the host nation.
- 2.4 ROE may authorise the full range of actions permissible by law, or limit them based on policy or operational considerations. ROE do not restate all of the applicable law for an operation; they are drafted on the basis that ADF members have been trained on relevant law, know how to apply it and have access to legal advice.