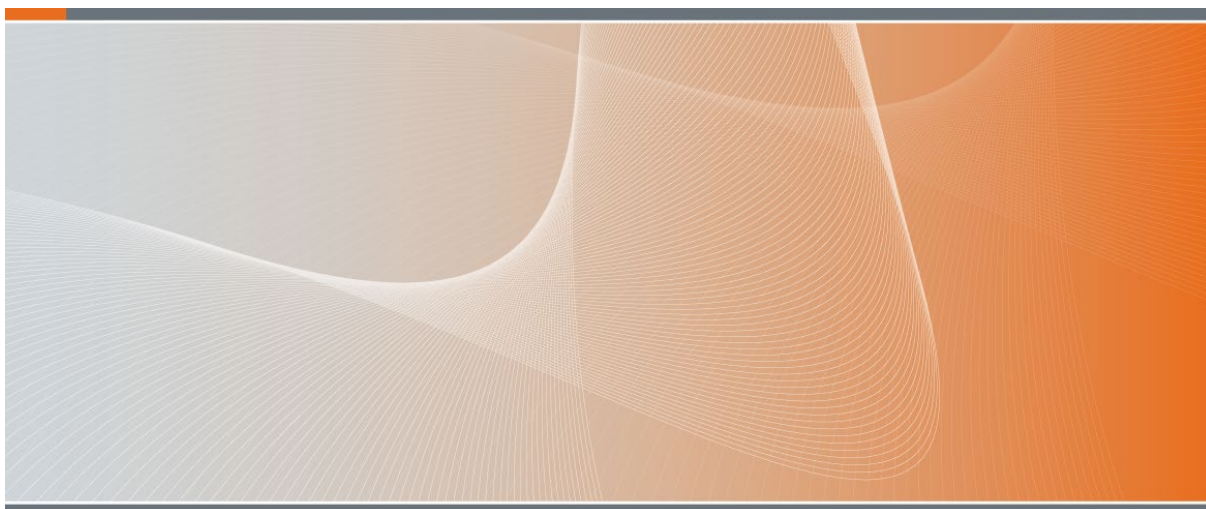




Australian Government
Department of Defence

DEFENCE SECURITY PRINCIPLES FRAMEWORK



A handwritten signature in black ink, appearing to read 'Kylie Scholten'.

Kylie Scholten
Chief Security Officer
First Assistant Secretary
Defence Security and Vetting Service
Policy Owner (Security)

Department of Defence
CANBERRA ACT 2600

31 July 2020

Defence Security Principles Framework

Governance and Executive Guidance

Approvals

1. The Defence Security Principles Framework (DSPF) has been endorsed by the Secretary of Defence as the Accountable Authority for Defence.
2. This document and the related DSPF Principles and Controls have been issued by the **Chief Security Officer** with the authority of the Associate Secretary on 2 July 2018.

Note: The First Assistant Secretary Security and Vetting Service (FAS S&VS) is the Chief Security Officer for Defence.

Purpose

3. The DSPF aligns Defence with the Commonwealth's Protective Security Policy Framework (PSPF). Under the PSPF, all agencies must develop their own protective security policies and procedures.

Objective

4. The DSPF is a principles-based framework intended to support a progressive protective security culture that understands and manages risk, leading to robust security outcomes. This approach:
 - Allows all parts of Defence to manage security within their operational context and constraints. This recognises the best security decisions are made in accordance with agreed principles, with a desired outcome in mind.
 - Ensures the most appropriate people are setting security requirements. Those who know their business are best placed to set security standards and requirements for that aspect of Defence business.
 - Sets clear processes and accountabilities, which underpin assurance of Defence protective security arrangements.

Scope and applicability

5. This document, and all documents that belong to the DSPF (DSPF documents), are administrative policy framework documents. They apply to all Defence personnel.
6. The terms of a relevant contract may extend the application of DSPF documents to persons engaged under a contract.

7. The Secretary and the Chief of the Defence Force (CDF) require Defence personnel to comply with provisions in DSPF documents unless the particular circumstances warrant departure from the provisions.
8. Some provisions in framework documents may support Defence personnel to comply with obligations that exist in:
- Applicable laws;
 - The Defence Enterprise Agreement;
 - Directives and determinations issued under the *Public Service Act 1999* or the *Defence Act 1903* or the *Defence Enterprise Agreement*; or
 - Defence Instructions.
9. Defence personnel must not depart from the provisions in framework documents in a way that would result in any breach of those obligations.
10. When considering a possible departure from DSPF documents, the Secretary and the CDF require Defence personnel to:
- Consider whether the proposed departure would be inconsistent with:
 - Applicable laws;
 - The *Defence Enterprise Agreement*;
 - Directives and determinations issued under the *Public Service Act 1999* or the *Defence Act 1903* or the *Defence Enterprise Agreement*; or
 - *Defence Instruction – Administrative policy* and other extant Defence Instructions.
- If yes, the departure is not permitted;
- Consider whether a proposed departure is reasonable and justified in the circumstances and will produce a better outcome for Defence.
 - Consult their supervisor, wherever practicable, about a proposed departure – a properly informed decision also involves consulting the policy owner.
 - Be responsible and accountable for the consequences of departing from, or not adhering to, the content of DSPF documents including where such departure or non-adherence results in a breach of applicable laws or leads to adverse outcomes for Defence.

11. Defence personnel may be subject to performance management, administrative action or, in some circumstances, disciplinary action where their decision to depart from provisions in DSPF documents involves serious errors of judgement.
12. Failure to adhere to administrative policy may result in a breach of legislation or other legal requirement and sanctions under that legislation may apply.
13. Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include in the terms of a contract the requirement to comply with the provisions of DSPF documents and, if so, include such terms.
14. Failure by persons engaged under a contract to comply with the requirements of this policy – where compliance is a term of the contract – may result in a breach of contract.

DSPF Document management and availability

15. DSPF documents belong to the administration and governance policy domain in the administrative policy framework. The **Chief Security Officer**, as FAS S&VS, is the accountable officer for security.
16. The DSPF is a flexible policy framework. DSPF documents will be reviewed and updated as necessary from 02 July 2018.
17. Authoritative DSPF documents are only available from the interactive DSPF site on the Defence Protected Network (DPN). A non-interactive version is also available from the DPN Defence manuals site and the [Defence Online Services Domain](#). The currency of DSPF documents cannot be guaranteed if sourced from other locations.
18. The security advice function, including queries on the DSPF, is provided in the first instance through 1800DEFENCE. Additional information can be found on the on the DPN.

The structure of the DSPF

19. Building on the PSPF and Information Security Manual (ISM), the DSPF provides governance, principles, policy, process and guidance to enable and empower Defence personnel to make security decisions in accordance with risk.

20. The DSPF has three Defence-specific levels of protective security management:

DSPF Whole of Government	Directive on Security of Government Business
	Protective Security Principles
	Protective Security Outcomes
	Protective Security Core Requirements and Policies
	Protective Security Protocols
Defence	DSPF Governance and Executive Guidance
	DSPF Principles and Expected Outcomes
	DSPF Enterprise-wide Controls

See DSPF Roles and Responsibilities diagram

21. The Defence-specific guidance will be provided through a suite of documents that will reference the PSPF. The DSPF is the authoritative source for enterprise security policy in Defence.

22. The three tiers of Defence Guidance are:

- *DSPF Governance and Executive Guidance*: This document establishes and explains the DSPF framework.
- *DSPF Principles and Expected Outcomes*: These documents provide security principles and expected outcomes across the Defence Enterprise (including references to any guidance, policies, or laws relevant to understanding/applying the principle or achievement of the expected outcome).
- *DSPF Enterprise-wide Controls*: Where necessary, these documents provide additional controls, processes and instructions relating to the interpretation and the application of *DSPF Principles and Expected Outcomes* relating to specific, complex or unconventional circumstances. They may also be used to manage circumstances where a degree of commonality across security management would be preferable and beneficial. It is neither expected, nor desirable, that all *DSPF Principles and Expected Outcomes* have accompanying *DSPF Enterprise-wide Controls*.

Understanding Principles and Expected Outcomes

23. *DSPF Principles and Expected Outcomes* follow a standard format. Each includes:

- The Principle: the high-level statement of intent (this is *what* we need to do);
- The Rationale: a statement explaining the importance of the principle (this is *why* we do it); and
- The Expected Outcomes: a statement of what needs to be achieved in order to meet the intent of the principle (this is Defence's desired *end* state).

24. *DSPF Principles and Expected Outcomes* documents do not include specific steps on how security outcomes should be achieved. Rather, they outline basic principles and desired outcomes that should guide our design and implementation of policy and controls to effectively manage security risks.

Constraints, Obligations and External Requirements

25. The DSPF has been designed around the concept of managed flexibility. This means that decision makers will have flexibility to adapt security solutions to their context. However, risk management decisions must also be shaped/influenced by relevant guidance, policies, or laws, such as:

- Legislation and regulation;
- Whole of government policy and expected outcomes;
- Decisions of relevant senior leadership, committees and boards;
- Australian and International standards; and
- International obligations and agreements.

26. Each *DSPF Principles and Expected Outcomes* document contains a "See also" section and an "Implementation Notes, Resources and Tools" section to provide applicable external implementation guidance.

Understanding DSPF Enterprise-wide Controls

27. Where additional guidance is needed to manage or mitigate a security risk beyond the general principle provided in the *DSPF Principles and Expected Outcomes* documents, it may be appropriate to develop a *DSPF Enterprise-wide Controls* document which provides controls, processes and instructions.

28. *DSPF Enterprise-wide Controls* are developed by **Control Owners**, an SES or ADF Star Rank Officer assigned accountability and authority to manage a specific defence security risk (refer paragraph 63).

29. *DSPF Enterprise-wide Controls* need to be sufficiently detailed to meet the security objective, but should not be so prescriptive as to produce a compliance based approach to security – except where there is a basis for a mandatory direction (refer paragraph 35).

30. **Control Owners** (refer paragraph 63) may set *DSPF Enterprise-wide Controls*. Subordinate security controls, processes and instructions may be Group or Service specific, collaborative or locational. These should be approved by the relevant **Control Owner**.

Security Controls Guidance

31. Subordinate security controls, processes and instructions need to be formally documented as they may be subject to review or audit. Security related decisions should be recorded in approved Defence records management systems accordance with Records Management Policy Manual and guided by Good Decision-Making in Defence.

Reviewing Controls, Processes and Instructions

32. *DSPF Enterprise-wide Controls*, and security decisions more broadly, may need to be reviewed; in line with continuous improvement and best practice. The requirement exists to review *DSPF Enterprise-wide Controls*, and consult stakeholders, to support and ensure effective security risk management practices:

- following a significant incident;
- following a change in environment or risk context; or
- as part of a scheduled program of review or audit.

Risk Management

33. Security risks should be resolved at the lowest possible level. All Defence personnel have an obligation to evaluate and treat risks. Serious residual risks, informed by a Security Risk Assessment, need to be escalated to the appropriate decision-maker for management. Business Impact Levels (BILs) should be used to assess the impact of the loss of information or assets.

34. Security risks are managed under the DSPF through:

- escalation of serious residual risks; and
- regular reporting.

Mandatory Provisions

35. Some provisions in the DSPF are mandatory. These are identified through the use of the word **must** and **must not** (bold type).

36. Any mandatory provision under the DSPF is to be approved by the **Chief Security Officer**. The **Chief Security Officer** is authorised to establish mandatory provisions under the *Defence Instruction – Administrative policy* and non-compliance is a reportable security incident.

37. Where it is determined that a departure from a mandatory provision is required, a dispensation may be sought from the relevant Control Owner. Dispensations can only be approved by the Control Owner.

Escalating and Accepting Risks

38. Where there is a risk to achieving the Expected Outcomes of a *DSPF Principles and Expected Outcomes* document, Defence personnel should manage or escalate this risk in accordance with sound risk management practices and the *Defence Instruction – Administrative policy*. Persons engaged under a contract cannot manage or escalate risks except through Defence personnel.

39. To enable sound risk management, **Control Owners** should set and make available general thresholds for escalation of serious risks, and specific thresholds on matters of special concern. These thresholds should help Defence personnel to decide which risks to escalate within their Group or Service and which need to be escalated to the **Control Owner**. The **Control Owner** also determines which risks need to be taken to the **Defence Security Committee (DSC)**, refer paragraph 61).

40. Escalation thresholds should determine the level (i.e. rank or position title) at which Defence personnel can manage risks at varying risk ratings (i.e. low to extreme risks).

41. With the exception of mandatory provisions, Defence personnel and persons engaged under a contract should regard DSPF Enterprise-wide Controls as guidance. Accepting the risk of departing from policy is to be guided by the escalation thresholds.

42. Where risk management results in a significant departure from Commonwealth policy (the PSPF or the ISM) this is to be reported via **Control Owners** to the **Chief Security Officer** or the **Chief Information Security Officer** for review of impact on obligations to the Commonwealth.

43. The preferred method for assessing risk is the Security Risk Assessment Guide (the SRA Guide). The preferred method of expressing risks and setting a threshold for escalation are the Guide's Risk Rating table and Consequence Descriptors.

44. Where a **Control Owner** already has a mature risk methodology in place they should utilise this, however they should ensure that relevant **Control Implementers** (refer paragraph 67) and **Control Officers** (refer paragraph 70) are aware of the requirement to use this methodology. The **Control Owner** should also map their methodology to the Guide's Risk Rating table.

Regular Reporting

45. The Secretary has an obligation to report annually to Government on Defence compliance with the PSPF. The Secretary is assisted by the **Chief Security Officer**, who provides an enterprise-wide view of Defence's security risk to the **DSC**.

46. The enterprise-wide security risk view is underpinned by assurance reporting from **Control Owners** (refer paragraph 63). **Control Owners** are required to provide an annual report to the **DSC** on each DSPF Principle and Expected Outcome they have responsibility for by completing the DSPF Reporting template. The purpose of this report is to:

- Provide general assurance to the **DSC** that a specific *DSPF Principle and Expected Outcome* is being implemented across Defence in a manner that manages the relevant security risks;
- Highlight any serious security incident or events; and
- Raise matters or serious risks of concern for **DSC** consideration.

47. In addition to an annual report, **Control Owners** should elevate serious residual security risks for action or acceptance by the **DSC** as they arise. Regular reports can then be used to review the management of serious residual risks.

48. DSPF reporting should be supported by an assurance framework established by each **Control Owner** with relevant **Control Implementers**. This exact nature of this framework will vary from one *DSPF Enterprise-wide Control* to another. **Control Implementers** will provide appropriate assurance to **Control Owners** and escalate risks in accordance with defined thresholds.

Training and Awareness

49. Security awareness training is an important element of any protective security regime. It supports the implementation of good policies, practices and procedures and helps to foster positive security attitudes.

50. To support a robust and positive security culture, Defence personnel and persons engaged under a contract are to undertake suitable security training through:

- Annual Security Mandatory Awareness on Campus; and
- The appropriate document handling course.

51. Further guidance regarding suitable security training can be obtained from the DS&VS Security Education intranet site.

Roles and Responsibilities

52. The Secretary is the Accountable Authority, in accordance with the [Public Governance, Performance and Accountability Act](#). This role is expected to meet the [four security outcomes](#) of the PSPF through the Attorney-General's on the Security of Government Business. To achieve this, the Secretary is to apply the PSPF, putting effective protective security programs into place that ensure:

- Defence's capacity to function;
- confidence in the department and the Australian Defence Force (ADF) by the public;
- the safeguarding of official information and security-protected assets; and
- the safety of Defence's personnel, persons engaged under a contract and clients.

See DSPF Roles and Responsibilities Diagram

53. The Secretary is the **Risk Owner** of Defence security and, in accordance with the PSPF, has designated:

- The Associate Secretary as the chair of the **Enterprise Business Committee** (EBC) and **DSC**. In this capacity, the Associate Secretary will escalate security issues through the two committees.
- The FAS S&VS as the **Chief Security Officer**, responsible for overseeing the development and implementation of the DSPF.
- The Director-General of the **Australian Signals Directorate** is the accreditation authority for TOP SECRET Special Compartment Information Facilities (SCIFs) and is the Communications Intelligence Security Authority for Defence.

Chief Security Officer

54. As the **Chief Security Officer** for Defence, FAS S&VS is delegated responsibility by the Secretary for Defence's security risk management.

55. In accordance with the PSPF, the **Chief Security Officer** is responsible for directing all areas of the Defence enterprise's security to protect Defence's people, information (including ICT) and assets.

56. This includes key oversight responsibilities outlined in the [*PSPF Paper 2 – Management Structures and Responsibilities*](#).

57. Defence-specific responsibilities include:

- Supporting and advising the Secretary and Chief of the Defence Force on security matters in Defence;
- Maintaining and overseeing the DSPF, specifically:
 - maintaining the *DSPF Governance and Executive Guidance*;
 - the DSPF Principles and Expected Outcomes, except for ICT Principles and Expected Outcomes, which are managed by the **Chief Information Security Officer**;
 - appointing **Control Owners**;
- Maintaining and overseeing clear security accountabilities and reporting structures through the DSPF;
- Appointing security advisers in Defence in accordance with PSPF requirements. This includes the appointment of a **Chief Information Security Officer**, in consultation with the Chief Information Officer;
- Reporting on the risk and effectiveness of *DSPF Enterprise-wide Controls* to the **DSC**;
- Producing Defence's annual PSPF report for Secretary approval;
- Promoting and fostering a positive security risk management culture within Defence; and
- Directing security training, threat information dissemination, security awareness programs, and incident reporting and investigations in Defence.

Chief Information Security Officer

58. The **Chief Security Officer** has designated the Chief Technology Officer, Chief Information Officer Group (CIOG), as the **Chief Information Security Officer** for Defence.

59. The **Chief Information Security Officer** is responsible for providing ICT security related whole of Defence strategic direction, reporting and advice to the **Chief Security Officer**.

60. This includes maintaining *DSPF Principles and Expected Outcomes* related to ICT security.

Defence Security Committee

61. The **DSC** is chaired by the Associate Secretary and reports to the Risk Owner via the **EBC**.
62. The **DSC** provides the primary oversight of the DSPF. **DSC** members:
- Provide security risk management strategic direction;
 - Address escalated residual security risks;
 - Consider **Control Owner** (refer paragraph 63) and enterprise-wide security risk reports; and
 - Seek to resolve any security related risks, problems or disagreements.

Control Owner

63. An SES or ADF Star Rank Officer assigned accountability and authority to manage a specific defence security risk. These will be derived from the *DSPF Principles and Expected Outcomes*. The relevant **Control Owner** in each instance may be a Group Head or Service Chief, or a more appropriate subordinate.
64. **Control Owners** will:
- Manage, monitor and report on the implementation across the Defence enterprise of any *DSPF Principles and Expected Outcomes*;
 - Set relevant *DSPF Enterprise-wide Controls*;
 - Approve subordinate security controls, processes or instructions for Group or Service specific, collaborative or locational purposes;
 - Define **Control Implementers** (refer paragraph 67) and establish any necessary horizontal accountability arrangements, including oversight of subordinate documents;
 - Build a framework and culture for the resolution of risks at the lowest possible level;
 - Act as Enterprise Subject-Matter Expert for relevant *DSPF Principles and Expected Outcomes*;
 - Provide appropriate assurance and reporting to the **DSC** and the **Chief Security Officer**;
 - Set and make available general thresholds for escalation of serious risks, and specific thresholds on matters of special concern; and

- Escalate risks that have a significant impact on the residual security risk to the **DSC** (in this sense a **Control Owner** is also a manager of residual risk).

65. **Control Owners** will be proposed to implement *DSPF Principles and Expected Outcomes* as required by the **Chief Security Officer** on the basis of:

- Formal organisational responsibility/accountability;
- Expertise; and
- Control of resources.

66. Where a **Control Owner** cannot be agreed the ownership will be referred to the **DSC** (refer paragraph 61).

Policy Owner and Publishing Authority

While **Control Owners** are responsible for the setting of any *DSPF Enterprise-wide Controls*, the **Chief Security Officer** is the Policy Owner and the DSPF publishing authority. **Control Owners** must meet DSPF Principles and Expected Outcomes when developing variations to their DSPF Enterprise-wide Control. Further guidance can be obtained from the Directorate of Administrative Policy and the Better Policy Handbook.

Control Implementer

67. Group Heads and Service Chiefs, or Commanders and Managers of specific business units, may be specifically delegated responsibility by the **Control Owners** to ensure the implementation and/or reporting against specific *DSPF Enterprise-wide Controls* to mitigate or manage security risks. They will generally be the managers or commanders with some specific responsibility for the implementation of the *DSPF Enterprise-wide Control*.

68. **Control Implementers** will:

- Implement *DSPF Enterprise-wide Controls* within their business unit;
- If required, develop subordinate security controls, processes or instructions that are Group/Service specific, Collaborative or Locational (such as Standard Operating Procedures);
- If required, exercise delegated authority as directed by the **Control Owner**;
- Provide reasonable assurance and reporting to **Control Owners**;
- Promote the resolution of risks at the lowest possible level; and
- Elevate significant security risk concerns with relevant **Control Owners**.

69. **Control Implementers** will be formally designated by **Control Owners**.

Control Officers

70. **Control Officers** encompass all staff and stakeholders in the Defence Enterprise. Defence personnel and persons engaged under a contract all have a duty to manage security risk in accordance with the DSPF.

71. Supervisors and custodians of information and assets are accountable for the appropriate implementation of *DSPF Enterprise-wide Controls* within their work places.

72. Where Defence personnel outsource a function, they cannot outsource the risk. Commanders and managers remain accountable (via the contract manager) for the protective security of their function and any official information and sensitive equipment made available to persons engaged under a contract.

Accountability and Relationships between Roles

Control Officers and **Control Implementers** can be accountable to **Control Owners** outside of their Group/Service (horizontal accountability). **Control Owners** can designate **Control Implementers** regardless of their Group or Service, and will set clear expected outcomes for Control Implementers to manage and improve security controls in accordance with security risk assessments.

Effective communication will be vital, as horizontal accountability is critical to effective enterprise security management. Where horizontal accountability raises risks or concerns, **Control Owners** should seek a mutually agreed outcome about the **Control Implementers** role. If an agreement cannot be reached the matter should be escalated to the **DSC**.

Executive Security Advisers

73. Each Group or Service is to appoint an **Executive Security Adviser (ESA)**. The **ESA** will:

- Support their senior management, **Control Owners** and **DSC** representatives to analyse their security environment and counter unacceptable risks;
- Act as their Group or Service point of contact for security matters;
- Support their Group or Service in maintaining an effective **Security Officer** structure; and
- Provide advice to their Group and Service **Security Officers**, **Control Implementers**, and **Control Officers**.

Security Officers

74. **Security Officers** are an important part of the Defence Security Community and contribute to the protection of Defence's people, information, assets in support of its capabilities and mission. The role of the **Security Officers** is critical to ensure the desired protective security culture is promoted and maintained across Defence.

75. Security Officers are required to provide DSPF advice and support to **Control Implementers**, **Control Officers**, and their Commanders and Managers on security matters, particularly on the implementation of *DSPF Enterprise-wide Controls*.

76. Commanders and Managers are to appoint **Security Officers** wherever sensitive or classified information and/or security protected assets are stored or handled. They should be appropriately trained (see the DS&VS Security Education intranet site for current Security Officer training requirements) and hold an appropriate security clearance.

77. Commanders and managers are not to appoint an external service provider as a **Security Officer**.

Contents

Governance and Executive Guidance

Principle 10

Assessing and Protecting Official Information

Control 10.1

Assessing and Protecting Official Information

Annex A to Assessing and Protecting Official Information – Selecting an Appropriate Protective Marking

Annex B to Assessing and Protecting Official Information – Applying Protective Markings to Official Information

Annex C to Assessing and Protecting Official Information – Reviewing and Altering Protective Markings

Annex D Assessing and Protecting Official Information – Release of Official Information

Annex E to Assessing and Protecting Official Information – Registration of Protectively Marked Information

Annex F to Assessing and Protecting Official Information – Official Information Filing and File Census

Annex G to Assessing and Protecting Official Information – Copying and Reproduction of Protectively Marked Information

Annex H to Assessing and Protecting Official Information – Disposal and Destruction of Protectively Marked Information and Assets

Annex I to Assessing and Protecting Official Information – Remarking Information Bearing Former Protective Markings

Annex J to Assessing and Protecting Official Information – Creating and Managing Information Compartments

Principle 11

Security for Projects

Control 11.1

Security for Projects

Principle 12

Security for Capability Planning

Principle 13

Communications Security (COMSEC)

Control 13.1

Communications Security (COMSEC)

Principle 14

Audio-visual Security

Control 14.1

Audio-visual Security

Annex A to Audio-visual Security – Construction and Acoustic Testing of Audio Secured Rooms

Principle 15

Foreign Release of Official Information

Control 15.1

Foreign Release of Official Information

Principle 16

Defence Industry Security Program

Control 16.1

Defence Industry Security Program

Annex A to Defence Industry Security Program – Privacy Notice

Annex B to Defence Industry Security Program – Suitability Matrix

Principle 17

Information Systems (Physical) Security

Control 17.1

Information Systems (Physical) Security

Principle 18

Information Systems (Personnel) Security

Control 18.1

Information Systems (Personnel) Security

Principle 19

Information Systems (Logical) Security

Control 19.1

Information Systems (Logical) Security

Principle 20

Information Systems Lifecycle Management

Control 20.1

Information Systems Lifecycle Management

Principle 21

Offshore and Cloud Based Computing

Control 21.1

Offshore and Cloud Based Computing

Principle 22

Mobility Device Security

Control 22.1

Mobility Device Security

Principle 23

ICT Certification and Accreditation

Control 23.1

ICT Certification and Accreditation

Annex A to ICT Certification and Accreditation – Certification and Accreditation Appointments

Annex B to ICT Certification and Accreditation – Defence Certification and Accreditation Process

Principle 24

Information Systems Security Incident Management

Control 24.1

Information Systems Security Incident Management

Principle 25

Information Systems Business Impact Levels and Aggregation

Control 25.1

Information Systems Business Impact Levels and Aggregation

Principle 26

Media Protection Security

Control 26.1

Media Protection Security

Principle 27

Information Systems Data Transfer Security

Control 27.1

Information Systems Data Transfer Security

Principle 28

Information Systems Log Management

Control 28.1

Information Systems Log Management

Principle 29

Information Systems Vulnerability and Patch Management

Control 29.1

Information Systems Vulnerability and Patch Management

Principle 30

Remote Access to Defence Systems

Control 30.1

Remote Access to Defence Systems

Principle 40

Personnel Security Clearance

Control 40.1

Personnel Security Clearance

Principle 41

Temporary Access to Classified Information and Assets

Control 41.1

Temporary Access to Classified Information and Assets

Principle 42

Identity Security

Control 42.1

Protected Identities

Annex A to Protected Identities – Process for Granting Honours and Awards

Principle 44

Overseas Travel

Control 44.1

Overseas Travel

Annex A to Overseas Travel – Overseas Travel Briefing and Debriefing Guides

Annex B to Overseas Travel – Travelling with Portable Electronic Devices and Media

Principle 45

Contact Reporting

Principle 46

Counterintelligence

Principle 70
Working Offsite**Control 70.1**
Working Offsite**Principle 71**
Physical Transfer of Information and Assets**Control 71.1**
Physical Transfer of Information and Assets

Annex A to Physical Transfer of Information and Assets -Transport of Bulk Assets

Annex B to Physical Transfer of Information and Assets – Developing a Movement Security Plan

Principle 72
Physical Security**Control 72.1**
Physical Security

Annex A to Physical Security – Security Containers, Vaults, and Safes

Annex B to Physical Security – Policy Transition from Security Rated Areas to Physical Security Zones

Principle 73
Physical Security Certification and Accreditation**Control 73.1**
Physical Security Certification and Accreditation**Principle 74**
Access Control**Control 74.1** Physical Access Control

Annex A to Physical Access Control - Defence Common Access Card Types

Annex B to Physical Access Control - Defence Common Access Card Types - Visual

Annex C to Physical Access Control - Transitional Arrangements for Certain Types of Defence Common Access Cards

Principle 75
Contracted Security Guards**Control 75.1**
Contracted Security Guards

Principle 76

Identification, Search and Seizure Regime

Control 76.1

Identification, Search and Seizure

Annex A to Identification, Search and Seizure Regime – Other Non-Statutory Search Regimes

Annex B to Identification, Search and Seizure Regime – Offences and Penalties

Annex C to Identification, Search and Seizure Regime – Defence Access Control Points

Annex D to Identification, Search and Seizure Regime – Training and Qualification Requirements

Annex E to Identification, Search and Seizure Regime – Summary of Defence Security Officials' Powers

Annex F to Identification, Search and Seizure Regime – Defence Security Official Identity Card Delegations

Appendix 1 to Annex F of Identification, Search and Seizure Regime – Defence Security Official Identity Card Delegations

Annex G to Identification, Search and Seizure Regime – Special Search Provisions for Declared Explosive Ordnance Depots

Principle 77

Security Incidents and Investigations

Control 77.1

Security Incidents and Investigations

Annex A to Security Incidents and Investigations – Special Reporting Requirements

Annex B to Security Incidents and Investigations - Security Incident Impact Levels

Principle 78

Weapons Security

Control 78.1

Weapons Security

Annex A – Storage Requirements for Weapons

Appendix 1 to Annex A – Ceasing Periodic Checks During an Extended Reduced Activity Period

Annex B – Storage and Management of Privately Owned Weapons and Ammunition

Annex C – Armouries

Annex D – Transporting Defence Weapons

Annex E – Security Requirements for Display and Demonstration of Weapons

Appendix 1 to Annex E – Mounting Procedures for Small and Trophy Weapons

Principle 79

Explosive Ordnance Security

Control 79.1

Explosive Ordnance Security

Annex A to Explosive Ordnance Security – Storage of Explosive Ordnance

Appendix 1 to Annex A of Explosive Ordnance Security – Ceasing Periodic Checks during an Extended Reduced Activity Period

Annex B to Explosive Ordnance Security – Transport Procedures for Explosive Ordnance

Annex C to Explosive Ordnance Security – Security Requirements for Control of Inert Explosive Ordnance

Appendix 1 to Annex C of Explosive Ordnance Security – Security Requirements for Display and Demonstration of Inert Explosive Ordnance

Annex D to Explosive Ordnance Security – Storage and Management of Privately Owned Explosive Ordnance

Principle 80

Radioactive Sources

Principle 81

Escorting Security Protected or Classified Assets

Control 81.1

Escorting Security Protected or Classified Assets

Annex A – Escorting Requirements for Explosive Ordnance External Service Providers

Principle 82

Procurement

Annex A to Procurement – Transition Period

Principle 83

SAFEBASE Security Alert Level System

Control 83.1

SAFEBASE Security Alert Level System

Principle 84

Fuel Security



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Assessing and Protecting Official Information

General Principle

1. Defence will protect Official Information in accordance with the expectations of the originator of the information. Where Defence is the originator of information, it will classify that information, according to the impact of access by, or disclosure to, unauthorised individuals, groups or organisations.

Rationale

2. The security of information is critical to the integrity of Defence's mission. If Defence does not protect its own information and information received from external parties from unauthorised access, its ability to function in support of the Government will be undermined.

3. The security classification system 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.

Expected Outcomes

4. The criteria and processes that Defence uses to assess and classify information are consistent with the requirements set out in the Protective Security Policy Framework. This security classification assessment will be informed by a broader assessment of Business Impact Levels (BILs) on each occasion.

5. Suitable controls are applied to Official Information to ensure that it is protected from unauthorised access or disclosure.

6. Defence protects foreign government information received under a General Security Agreement (GSA) or Defence-specific Security of Information Agreement or Arrangement (SIA) in accordance with the relevant terms.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Assessing and Protecting Official Information
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 10
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 10.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Sensitive and classified information; and Access to information. <u>Legislation:</u> Freedom of Information Act 1982 (Cth) Privacy Act 1988 (Cth)
See also DSPF Principle(s)	Information Systems (Physical) Security Information Systems (Personnel) Security Personnel Security Clearance Overseas Travel Working Offsite Physical Transfer of Information and Assets
Implementation Notes, Resources and Tools	Business Impact Levels FAQ, tools and guide

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 May 2019	FAS S&VS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Assessing and Protecting Official Information

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. AS SPS has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Introduction

3. This DSPF Control provides guidance on assessing and protecting of Official Information in Defence. The DS&VS Information Security intranet page is a useful resource on how to apply Protective Markings in Defence.
4. Additional guidance for specific activities can be found in the Annexes of this DSPF Control.

5. To ensure Defence personnel and persons engaged under a contract are meeting the Expected Outcomes of this policy (Refer to DSPF Principle 10 – *Assessing and Protecting Official Information*), the following mandatory provisions apply:
- a. Official Information requiring increased protection must be clearly marked with the appropriate Protective Marking in compliance with the Australian Government Protective Security Policy Framework (PSPF).
 - b. Altering the Protective Marking on Official Information must not be done without Originator approval.
 - c. Official Information **must** be protected with suitable controls commensurate with its level of sensitivity and/or classification.
 - d. Official Information **must** only be released to, and accessed by, those who need-to-know the information for their official duties.
 - e. Classified information **must** only be released to, and accessed by, those who have the appropriate level of security clearance required and with a need-to-know.
 - f. Caveated information **must** only be accessed and handled in accordance with the relevant caveat controls in this DSPF Control.
 - g. Official Information **must not** be protectively marked in order to:
 - (1) hide violations of law, inefficiency or administrative error.
 - (2) prevent embarrassment to an individual, organisation or agency.
 - (3) restrain competition.
 - (4) prevent or delay the release of information that does not need protection in the public interest.
 - h. All Defence personnel **must** have agency authorisation to release any Official Information to members of the public. For further information, refer to Annex D of this DSPF Control.
 - i. Documents and Files containing information covered by more than one classification **must** be classified to the highest level of information contained within.
 - j. Classified information must be appropriately recorded in accordance with the [Archives Act 1983](#) and the Records Management Policy Manual (RECMAN). Refer to Annex F of this DSPF Control.

- k. All information classified TOP SECRET, and accountable material, held by Defence must be registered. Refer to Annex E of this DSPF Control.
- l. All information classified SECRET and above, and accountable material, held by Defence Industry Security Program members must be registered. Refer to Annex E of this DSPF Control.
- m. Disposal of sensitive and classified information **must** be in accordance with Defence Records Management Policy Manual (RECMAN) and by methods appropriate for the level of classification in accordance with Whole of Australian Government requirements. Refer to Annex H of this DSPF Control.
- n. Classified information **must** be transferred by secure means commensurate with its level of classification (i.e. by SAFEHAND). Refer to DSPF Principle 71 – *Physical Transfer of Information and Assets*.

Protecting Official Information

6. Official Information is any information received, developed or collected by, or on behalf of, the Australian Government, by Defence personnel and person's engaged under a contract in their professional capacity and may include:

- a. documents and paper;
- b. data;
- c. software or systems and networks on which the information is stored;
- d. intellectual information (knowledge) acquired by individuals; and
- e. physical items from which information regarding design, components or use could be derived.

7. Official Information encompasses sensitive and security classified information.

8. Defence personnel and persons engaged under a contract must take appropriate steps to ensure that Official Information is protected from compromise or unauthorised access in accordance with the information's Protective Marking.

Note: The unauthorised disclosure of Official Information may be subject to the sanction of criminal law under **Part 5.6 of the Criminal Code 1995 (Cth)**.

9. This applies to information in any form, including oral, written, electronic, documentary, visual, briefings, material and equipment.

Assessing Official Information

10. Defence personnel and persons engaged under a contract, as the originators of that information, are to determine the sensitivity of Official Information by assessing the damage that the compromise of, or unauthorised access to, that information or asset would likely cause to Defence and/or the Australian Government. This is called assessing the Business Impact Level (BIL)(see Table 1).

11. The BIL allows an originator to determine if Official Information requires a routine level of protection, is sensitive or requires a security classification.

Note: The responsibility as the originator belongs to the functional position from which the information was originally prepared, not necessarily the individual who prepared the document.

Table 1: Business Impact Levels

BIL	1 (Low)	2 (Low-Medium)	3 (High)	4 (Extreme)	5 (Catastrophic)
Protective Marking	OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
Compromise of information confidentiality would be expected to cause:	No or insignificant damage. This is the majority of routine information.	Limited damage to an individual, organisation or government generally if compromised.	Damage to the national interest, organisations or individuals.	Serious damage to the national interest, organisations or individuals.	Exceptionally grave damage to the national interest, organisations or individuals.

12. Guidance on how to assess the BIL of Official Information in accordance with Table 1 and how to apply the corresponding Protective Marking can be found in Annexes A and B of this DSPF Control.

13. It is important for Official Information to be protectively marked at the lowest level allowed through the assessed BIL. The appropriate use of Protective Markings enables Defence to engage internally and externally with as broad an audience as necessary and subject to the need-to-know principle. The misuse of Protective Markings, including the over-protection of Official Information, inhibits information sharing and collaboration.

Limiting Access to Official Information

14. **Security clearance.** Defence personnel and persons engaged under a contract **must** ensure that access to classified Information is limited to those who have the appropriate level of security clearance required. For further information refer to DSPF Principle 40 – *Personnel Security Clearance*.

15. **Need-to-know principle.** Defence personnel and persons engaged under a contract **must** ensure that access to Official Information is limited to those who need to know the information for their official duties.

***Exclusion:** Official Information that has been formally approved for Public release is not subject to the need-to-know principle.*

Managing Official Information in Your Business Area

16. **Clear desk.** Personnel are responsible for the security of Official Information under their control. During absences from their workplace, Defence personnel and persons engaged under a contract are to 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.

17. **Session and Screen Locking.** During any absence from their work station, Defence Personnel and person/s engaged under a contract are to ensure their work station screen is locked to ensure unauthorised access to Defence ICT systems and Official Information is deterred.

18. **Close of day checks.** At the close of business each day, personnel are to take precautions to ensure that Official Information, especially sensitive or classified information, is protected from unauthorised access. It is recommended that Security Officers develop a workplace lock-up procedure which may include, but not be limited to the following:

- a. Ensuring no sensitive or security classified information is left unattended on a desk (that is, it is stored appropriately).
- b. Logging off all systems and, if required, switching the machine off.
- c. Ensuring desk are clear of documents to avoid sensitive or classified information being left out in the workplace.
- d. Ensuring that laptops and other electronic media storing security classified information are secured.
- e. Ensuring Official Information has been disposed of appropriately, including checking waste-paper bins.
- f. Ensuring that whiteboards and other displays do not show any security classified information.
- g. Ensuring vaults and containers are locked.
- h. Ensuring windows and doors are locked.
- i. Ensuring that container keys are secured.

- j. Keys are not left in doors and drawers (at the end of the day or for an extended period of time).
- 19. It is also recommended that Commanders and Managers put in place an appropriate system for checking the workplace at close of business (or the end of shifts) to ensure that Official Information is secured appropriately.
- 20. Offsite Work. Requirements for offsite work are provided in DSPF Principle 70 – *Working Offsite* and Control 70.1 – *Working Offsite*.

Applying Protective Markings to Official Information

- 21. The Protective Marking of Official Information informs the level of protection afforded to it. Defence-specific guidance on applying Protective Markings to Official Information can be found in Annexes A and B of this DSPF Control.
- 22. The Protective Marking 'UNOFFICIAL' may be assigned to information that Defence personnel and persons engaged under a contract have generated in their private capacity under reasonable use of Defence resource provisions.

Example: Thomas sends an 'UNOFFICIAL' email to his co-workers inviting them to an after-work gathering to celebrate his birthday.

Allison sends an 'UNOFFICIAL' email to her partner asking them to pick up a carton of milk on the way home from work.

Official Information

- 23. 23. Official Information that is not sensitive and has a BIL rating of Low (1) should have the following Protective Marking:

- a. 'OFFICIAL'.

Sensitive Information and Dissemination Limiting Marker

- 24. Official Information that is determined to be sensitive, but not classified, and has a BIL rating of Low-Medium (2) should have the following Protective Marking to restrict its dissemination:

- a. 'OFFICIAL: Sensitive'.

Security Classified Information

- 25. Official Information that is determined to be sensitive and has a BIL rating of High (3), Extreme (4) or Catastrophic (5) is classified information and should have a Security Classification as a Protective Marking.

- 26. Security Classifications are:

- a. 'PROTECTED';

- b. 'SECRET'; and
- c. 'TOP SECRET'.

27. A document may contain information covered by more than one Protective Marking. Where this occurs, the compilation of Official Information is to be assessed against the criteria above and the appropriate classification assigned to the document. This Protective Marking is to be at least as high as the most sensitive or classified information or paragraph within the document.

Information Management Markers (IMMs)

28. An IMM is assigned to information where disclosure may be limited or prohibited by legislation, or where the information may otherwise require special handling. IMMs include:

- a. legislative secrecy – for information that is subject to one or more legislative secrecy provisions;
- b. personal privacy – for information that is personal information as defined in the *Privacy Act 1988*; and
- c. legal privilege – for information that is subject to legal professional privilege.

Security Caveats

29. Security Caveats are additional Protective Markings applied to Official Information to warn of special protections that are to be applied to the information in addition to the security classification.

30. Some security caveats used in Defence are:

- a. special handling instructions;
- b. releasability caveats; and
- c. Codewords.

31. **Special handling instructions**, including 'Cabinet' and 'Exclusive for...' are caveats that are applied to Official Information requiring specific precautions that are to be taken.

- a. '**Cabinet**'. Cabinet documents are defined in the Cabinet Handbook and the *Freedom of Information Act 1982*. Official Information that includes Cabinet material, as defined in the Cabinet Handbook, must be marked with the 'Cabinet' caveat and be classified 'PROTECTED' or higher.

- b. **‘Exclusive for ...’**. Indicates the information must be accessed only by the named recipient, and permission must be sought from the Originator before granting access to any other persons. This special handling instruction can only be used on Official Information classified ‘PROTECTED’ or higher.
32. **Releasability Indicators**, including ‘Australian Eyes Only’ (‘AUSTEO’) and ‘Australian Government Access Only’ (‘AGAO’), are caveats which permit or limit the release of Official Information to individuals based on citizenship or position.
33. The Defence Protected Network (DPN) 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 [Information Security Manual](#) (ISM) and the PSPF, information bearing these caveats is not to be produced or stored on the DPN.
34. **‘Releasable to ...’ (‘Rel ...’)**. The ‘Rel ...’ caveat identifies Official Information with access limited to citizens of those countries listed in the Protective Marking. Access to ‘Rel ...’ caveated information must be limited to citizens of the countries listed in accordance with the conditions under a Security of Information Agreement or Arrangement or a General Security Agreement.
35. DSPF Control 15.1 – *Foreign Release of Official Information* provides more detail on the foreign release process, and the use of the ‘Rel ...’ caveat under a Security of Information Agreement or Arrangement or a General Security Agreement

Note: *If Defence-originated information is not subject to another releasability caveat, it is to be treated as approved by the originator for release to FVEY governments with the protective marking ‘Rel AUS/CAN/NZL/UK/USA’.*

36. **‘Australian Government Access Only’ (‘AGAO’)**. Access to ‘AGAO’ caveated information must only be released to people who are either:
- Australian Government, Defence personnel or persons engaged under a contract who are Australian citizens (such as members of the Defence Industry Security Program);
 - United States, United Kingdom, Canadian or New Zealand nationals who are integrated or embedded as officers of the Australian Government (Integrated Officers), whether located in Australia or Overseas, and who hold a current equivalent level clearance issued by their government; or

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.]*

- c. United States, United Kingdom, Canadian or New Zealand citizens 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 DSPF Principle 40 – Personnel Security Clearance for further information on the operation of these restrictions.

Example: A foreign person engaged under a contract with a recognised US issued clearance working in an Australian Project Office is not eligible for 'AGAO' access normally and would require an Australian clearance issued on the basis of a citizenship eligibility waiver in order to access 'AGAO' caveated information.

37. Information with the 'AGAO' caveat **must not** be released to a foreign government, foreign company or any foreign entity, including foreign persons engaged under a contract with a foreign security clearance outside of the circumstances highlighted in paragraph 35.

38. 'AGAO' caveated information is not to be made accessible to United States, United Kingdom, Canadian or New Zealand nationals accessing Defence networks from coalition gateways. In this circumstance, these individuals are working on behalf of their own government and are not entitled to access 'AGAO' caveated information.

39. With the exception of those covered by exchange arrangements within the Defence intelligence agencies, foreign nationals granted approval to access 'AGAO' caveated information are required to sign a Certificate of Assurance for Access to Australian Government Access Only (AGAO) information by United States, United Kingdom, Canadian or New Zealand nationals.

40. **'Australian Eyes Only' ('AUSTEO').** The use of the 'AUSTEO' caveat is to be strictly limited and must only be released to 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' caveated information.

Receiving Classified Information with Old and New Security Classification Protective Markers

41. Defence ICT systems can receive and send emails with the old and new security classification system Protective Markings as of 31 July 2020.

42. Table 2 should be used when determining security classification Protective Markings equivalencies for handling, storing, discussing and transmission of classified information between the current Defence Protective Markings and the revised security classification system Protective Markings under the PSPF.

Table 2: Security Classification Protective Markings Equivalency

Before 1 October 2020 (Now)		From 1 October 2020 (what's changing)
TOP SECRET	Security Classifications	TOP SECRET
SECRET	Security Classifications	SECRET
CONFIDENTIAL	Security Classifications	Discontinued
PROTECTED	Security Classifications	PROTECTED
Sensitive: Cabinet	DLM → Caveat	Cabinet (Caveats can only be applied to security classified information, i.e. PROTECTED or above)
Sensitive Sensitive: Personal Sensitive: Legal	DLM → Information management marker	Apply classification or OFFICIAL: Sensitive and optional information management markers: – Legislative secrecy – Personal privacy – Legal privilege
For Official Use Only	DLM → DLM	OFFICIAL: Sensitive
UNCLASSIFIED	Non-classification markings	OFFICIAL
UNOFFICIAL	Non-classification markings	UNOFFICIAL

43. **Special Access Program.** Additional requirements that apply to the handling of information relating to the Defence Special Access Program are in the Special Access Program Manual (available on the DSN).

44. There are specific limitations on the production and storage of information bearing security caveats on ICT systems. System users **must** only create, process or store information on systems which have been accredited to process such caveats.

Altering Protective Markings

45. Protective Markings **must not** be remarked (i.e. 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 is to be immediately reported as a major security incident in accordance with DSPF Principle 77 – *Security Incidents and Investigations*.

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.

Exclusion: *Remarking of documents from former markings to their revised PSPF equivalents does not require the permission of the Originator. Refer to Annex I of this DSPF Control. However any caveats such as CODEWORD or release markings cannot be modified under these provisions.*

46. Further information for reviewing and altering classifications is provided at Annex C of this DSPF Control.

Transfer of Official Information

47. **Physical transfer of Official Information.** Requirements for the removal and physical transfer of classified information are provided in detail in DSPF Principle 71 – *Physical Transfer of Information and Assets*.

48. **Electronic transmission of Official Information.** Requirements for the electronic transmission of classified information are provided in the [ISM](#) and DSPF Principle 27 – *Information Systems Data Transfer Security*.

Appropriate Storage and Archive Requirements

49. **Physical access and storage.** Requirements for the physical access and storage of Official Information and assets are provided in DSPF Principle 72 – *Physical Security*.

50. **Registration.** Requirements for the registration of Official Information held by Defence are provided in Annex E of this DSPF Control.

51. **Filing.** Requirements for the filing of Official Information are provided in Annex F of this DSPF part, the [Archives Act 1983](#), and the Records Management Policy Manual (RECMAN).

52. **Loss.** Any loss of classified information is a security incident. The requirements for reporting and investigating security incidents are provided in DSPF Principle 77 – *Security Incidents and Investigations*.

Note: *Early reporting in accordance with DSPF Principle 77 – Security Incidents and Investigations may prevent further compromise and minimise the extent of damage of the security incident.*

53. **Copying and reproduction.** Requirements for the copying or reproduction of Official Information are provided in Annex G of this DSPF Control.

54. **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, refer Business Impact Levels for further information.

ASD Compartment Information Storage and Handling Requirements

55. Defence personnel and persons engaged under a contract are to receive permission from the Originator if ASD-managed compartmented information needs to be held outside the Originator's facility or an accredited Sensitive Compartment Information Facility (SCIF).

56. Any permission from the Originator to file the documents in a specific location is to be recorded by the security officer in the area's security register. If granted, the ASD Records Management area is to be contacted to request a Special Series File. ASD is responsible for all Defence records management functions for Special Series Files or Sensitive Compartment Information (SCI) Records including file requests, musters, sentencing, storage, and disposal.

57. All SCI material is to be stored in the Special Series File managed by ASD. The information is not to:

- a. be stored or processed on the DPN (including Objective);
- b. be stored or processed on the Defence Secret Network (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.

58. When no longer required, all Special Series Files are to be returned to ASD.

59. Special provisions for the custody of intelligence information are made in the [Archives Act 1983](#) Section 29(8). Further information can be found in the Records Management Policy Manual (RECMAN).

Protecting Foreign Information

60. Defence personnel and persons engaged under a contract must handle foreign government information with a level of protection no less stringent than is provided by the Originator.

61. In many cases, the Australian government has provided an assurance to safeguard this information under the terms of a Security of Information Agreement or Arrangement (SIA) or a General Security Agreement (GSA). For example, foreign government information **must** be compartmentalised to ensure it is protect from unauthorised third party access.

62. Defence personnel and persons engaged under a contract **must** protect foreign government information in accordance with all relevant SIAs and GSAs. A complete list of Defence's SIAs is available on the Defence Security & Vetting Service (DS&VS) site on the Defence Secret Network (DSN).

Note: A list of 'OFFICIAL' SIAs is available on the DPN]

63. For more information on SIAs and GSAs, contact 1800DEFENCE.

64. In many cases, Project Security Instructions (PSI) apply to project-specific foreign information. Defence personnel and persons engaged under a contract are to protect foreign information in accordance with all relevant PSI as long as they do not contradict the relevant SIA or GSA.

Key Definitions

65. **Accountable material.** Accountable material is information that requires the strictest control over its access and movement including TOP SECRET security classified information and some types of caveated information such as Cabinet.

66. **Official Information.** Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and persons engaged under a contract that includes:

- a. documents and paper;
- b. data;
- c. software or systems and networks on which the information is stored,
- d. intellectual information (knowledge) acquired by individuals; and
- e. physical items from which information regarding design, components or use could be derived.

67. **Unofficial Information.** Non-work related information generated by Defence personnel and persons engaged under a contract under reasonable use of Defence resource provisions, typically contained in email, faxes etc.

68. **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;
- b. an Australian government department or agency;
- c. a foreign government; or

- d. 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.

69. **Classification Process.** The process by which the confidentiality requirements of Official information are assessed and the appropriate Protective Markings applied.

70. **Protective Marking.** A marking given to Unofficial and Official Information 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. Protective Markings used in Defence are:

- a. 'UNOFFICIAL';
- b. 'OFFICIAL';
- c. 'OFFICIAL: Sensitive';
- d. 'PROTECTED';
- e. 'SECRET'; and
- f. 'TOP SECRET'.

71. **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. Security Classifications used in Defence are:

- a. 'PROTECTED';
- b. 'SECRET'; and
- c. 'TOP SECRET'.

72. **National Interest.** A matter which has or could have an impact on Australia, including:

- a. national security;
- b. international relations;
- c. law and governance, including:
 - (1) interstate/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.

73. **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.

74. **Information Management Marker (IMM).** A way to identify information that has non-security related restrictions on access and use due to legal, legislative or privacy sensitivities. Information Management Markers are not Protective Markings. IMMs used in Defence are:

- a. 'Personal Privacy';
- b. 'Legal Privilege'; and
- c. 'Legislative Secrecy'.

75. **Security Caveat.** Applied to security classified information indicating that special protective requirements apply in addition to those associated with its Security Classification. Security Caveats used in Defence include:

- a. Special handling instructions:
 - (1) 'Cabinet'; and
 - (2) 'Exclusive for ...'.
- b. Releasability indicators:
 - (1) 'Australian Eyes Only' ('AUSTEO');
 - (2) 'Australian Government Access Only' ('AGAO'); and
 - (3) 'Releasable to...' ('Rel ...').

76. **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.

77. **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
- 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.

78. **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.

79. **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

80. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – Selecting an Appropriate Protective Marking

Annex B – Applying Protective Markings to Official Information

Annex C – Reviewing and Altering Protective Markings

Annex D – Release of Official Information

Annex E – Registration of Protectively Marked Information

Annex F – Official Information Filing and File Census

Annex G – Copying and Reproduction of Protectively Marked Information

Annex H – Disposal and Destruction of Protectively Marked Information and Assets

Annex I – Remarking Information Bearing Former Security Classifications

Annex J – Creating and Managing Information Compartments

Document administration

Identification

DSPF Control	Assessing and Protecting Official Information
Control Owner	AS SPS
DSPF Number	Control 10.1
Version	4
Publication date	28 August 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Assessing and Protecting Official Information
Related DSPF Control(s)	Information Systems (Physical) Security Information Systems (Personnel) Security Personnel Security Clearance Overseas Travel Working Offsite Physical Transfer of Information and Assets

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy; restructure to present information of most use up front.
4	28 August 2020	AS SPS	Update of mandatory statements regarding the need-to-know principle, security clearances, and the AUSTEO caveat



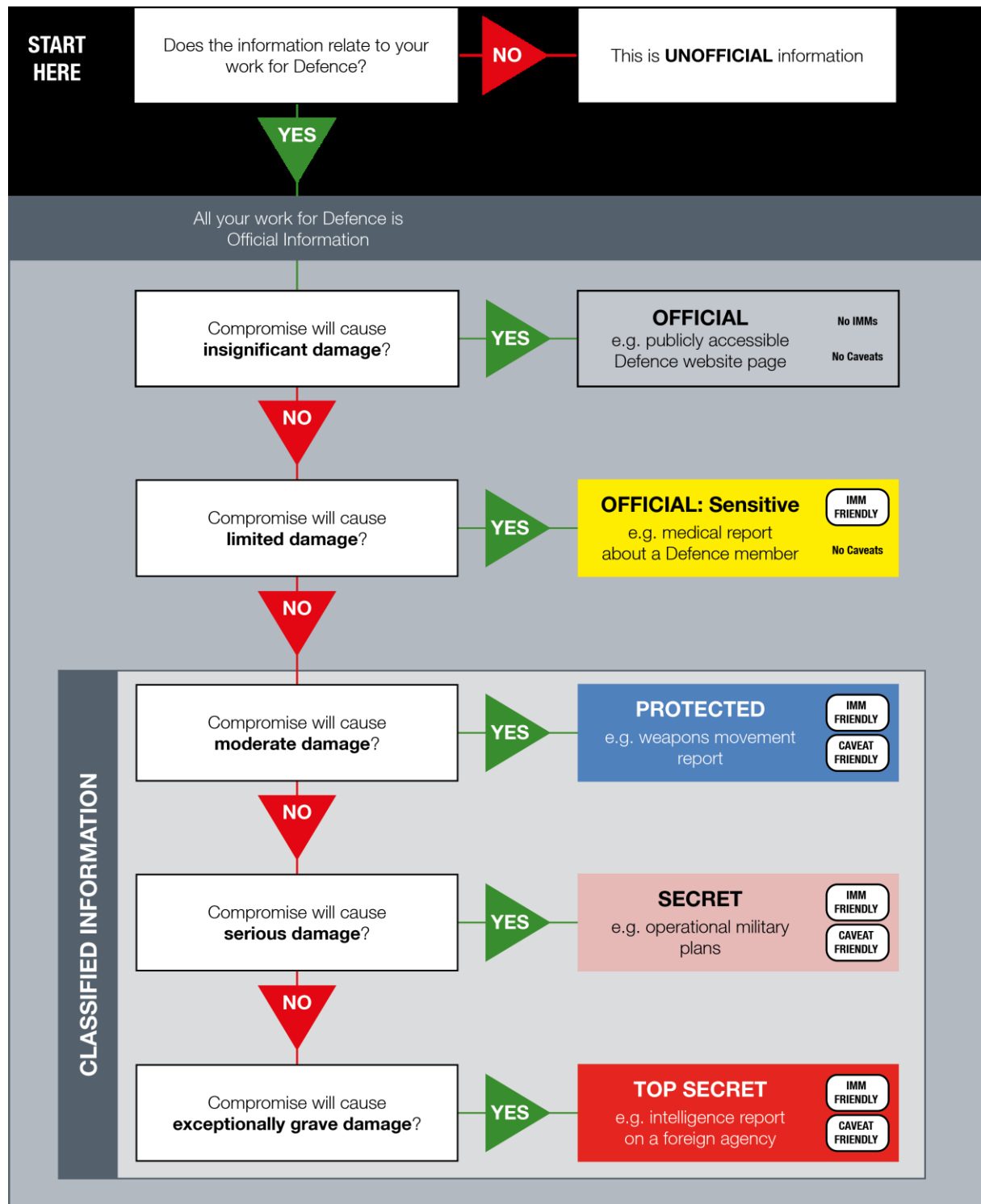
Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Assessing and Protecting Official Information – Selecting an Appropriate Protective Marking

1. The flow chart on the following page outlines the steps involved in selecting the most appropriate Protective Marking for a document.

Figure 1: Protective Marking selection



Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Selecting an Appropriate Protective Marking
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update of text and infographic to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Assessing and Protecting Official Information – Applying Protective Markings to Official Information

1. Where a Protective Marking is required it must be clearly marked. In the context of verbal briefings or discussions, it is recommended that the level of the brief or discussion be clearly stated.

Applying Protective Markings to Documents

2. Protective Markings are required to be in capitals, in bold text and of a minimum height of 5mm at the top and bottom of each page. It is recommended that the protective markings are in red.

3. If an existing document requires its Protective Marking to be over-stamped, it is recommended that the over-stamping be in red.

Applying Paragraph Markings

4. It is recommended that individual paragraphs of a document be protectively marked. Where paragraph markings are used, all paragraphs in the document are required to be marked, so as to avoid a situation where it cannot be determined if a paragraph was intentionally left unmarked in the classification process.

5. The order of precedence or hierarchy for protective markings is:

- a. classification (or the OFFICIAL: Sensitive dissemination limiting marker (DLM));
- b. foreign government information markings (if any);
- c. caveats or other special handling instructions (if any); then
- d. Information Management Markers (IMM) (if any).

6. The paragraph marking is to appear in a consistent position on each paragraph throughout the document. It is recommended that it is placed in brackets at the beginning of each paragraph. The protective marking can be written in full or abbreviated. Classifications, Information Management Markers (IMM) and special handling caveats are abbreviated as follows:

- a. 'OFFICIAL' – (O);
- b. 'OFFICIAL: Sensitive' – (O:S);
- c. 'Legal privilege' (Legal);
- d. 'Personal secrecy' (Pers);
- e. 'Legislative secrecy' (Leg);
- f. 'Cabinet' (Cab);
- g. 'PROTECTED' (P);
- h. 'SECRET' (S); and
- i. 'TOP SECRET' (TS).

7. A paragraph marking key is to be used on all paragraphs in a paragraph marked document.

Translating New Security Classification Protective Markings

8. During the transition period to the new security classification system, Defence will be able to receive classified information from other federal government departments and agencies that are already using the new security classification system. While the appropriate selective marking for this information will already have been identified by the originator, there will be circumstances in which Defence will be required to identify a Protective Marking different to that selected by the originator.

9. In this case, the equivalencies identified in Table 2 of Control 10.1 – *Assessing and Protecting Official Information* must be used to determine what Protective Marking is appropriate.

Example: *Emails received with the Protective Marking of 'UNCLASSIFIED' will need to be handled by Defence as 'OFFICIAL'.*

Protectively Marking Document Titles

10. It is recommended that the title of a document be marked no higher than 'OFFICIAL' to ensure ease of reference.

11. If the title needs to be classified, the relevant Protective Marking is to appear abbreviated in brackets after the last word of the title.

12. To enable unclassified reference to a document with a classified title, it is recommended the originator apply either an unclassified abbreviated title or reference number and date.

Printed Graphic Material

13. For maps, drawings and other printed graphic material the Protective Marking is to be printed or stamped near the map scale or drawing numbers as well as printed at the top and bottom centre of the document. If the material is to be folded, the marking is to remain visible after folding.

Protectively Marking Annexes, Appendices and Covering Documents

14. Sometimes the annex or appendix to a document requires a different protective marking from the document itself. If the annex or appendix has a higher protective marking or classification than the principal document, the document's front cover is to indicate that the document and the annex or appendix as a whole cover a higher classification.

Example: 'SECRET-covering-TOP SECRET'

Example: 'OFFICIAL-covering-PROTECTED'

15. If a summary or covering letter to a document does not require any Protective Marking, or has a lower Protective Marking than the document to which it is attached, the summary may remain 'OFFICIAL'. However, it is to indicate that it covers a document of a higher Protective Marking.

Example: 'OFFICIAL-covering-SECRET'

16. Documents with covers, such as books, pamphlets and reports, are to show the Protective Marking on the front cover, title page and rear cover. Any binding or fastening of pages cannot obscure the Protective Marking.

Aggregation

17. Large compilations of Official Information, for example a collection of electronic records, 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, refer Table 1 of Control 10.1 – *Assessing and Protecting Official Information* for further information on Business Impact Levels.

Imagery

18. Photographs and film requiring protection and their storage envelopes or containers are to carry a conspicuous Protective Marking. Security classified imagery (including roll imagery, cine-film, video tape) requires further Protective Marking in the title and end sequences to ensure projection of the marking for at least five seconds for each. Photographic negatives are required to be marked to ensure the Protective Marking will be reproduced on all copies made from that negative. The copies are to be marked.

Presentations

19. Presentations containing Official Information are to bear Protective Markings. Each slide or screen is to be treated as an individual page, as with a paper based document, and marked accordingly. Dot points may be protectively marked in line with paragraph markings. It should also be noted that the speaker's notes in the slides may also contain Official Information and these are to be marked accordingly.

Audio

20. For audio presentations and recordings, the level of Protective Marking is to be clearly stated at the beginning and end. The tape or other media and its container is to be conspicuously labelled with the appropriate Protective Marking.

Microforms

21. All microforms such as aperture cards, microfiche and microfilm containing security classified matter are to show the appropriate Protective Marking at the top and bottom centre of each frame. Containers and envelopes are to bear the appropriate Protective Marking. The Protective Marking is to be visible without projection on both aperture cards and microfiche, and microfilm is to be prominently marked at the beginning and end of each roll.

Electronic Storage Media and ICT Equipment

22. Policy for the marking of electronic storage media and devices is contained in:

- a. DSPF Principle 22 – *Mobility Device Security*; and
- b. the [Information Security Manual \(ISM\)](#).

23. Cryptographic Controlled Items and some other High Assurance products have special labelling requirements in order to maintain tamper evidence. These are detailed in DSPF Principle 13 – *Communications Security (COMSEC)* and its references.

Document administration

Identification

DSPF Annex	Applying Protective Markings to Official Information
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex C to Assessing and Protecting Official Information – Reviewing and Altering Protective Markings

Reviewing a Protective Marking

1. It is recommended that protectively marked information be reviewed after an event such as:
 - a. the completion of an operation, program or project;
 - b. a security incident related to the information;
 - c. a file is withdrawn from use or returned to use; or
 - d. a muster is conducted.
2. All Defence personnel and persons engaged under a contract are encouraged to challenge any security classification they believe is insufficient, excessive or inaccurate by contacting the originator or the business unit responsible for the document or item carrying the classification. A reason for a challenge is to be provided along with a request for declassification or reclassification.

Altering a Protective Marking

3. Only the originator can authorise the alteration of the Protective Markings.

Note: The alteration of a protective marking means to change a protective marking's protection requirements. A change in a protective marking due to a change of Whole-of-Government classification guidelines (re-marking) is not in-scope for this definition. For information re-marking classified documents, see Annex I – Remarking Information Bearing Former Security Classifications

4. Where the originating military or business unit within Defence no longer exists, or if it no longer has the subject matter expertise to make such decisions, the responsibility for reviewing and, if required, altering a Protective Marking rests with the:
 - a. military or business unit that has assumed the functions and responsibilities of the original unit;

- b. Executive Security Adviser (ESA) if it is unclear who has assumed the responsibilities within a Group or Service; or
- c. First Assistant Secretary Security and Vetting Service (FAS S&VS) if an appropriate Group or Service cannot be identified as holding the functions and responsibilities of the original unit. The FAS S&VS may delegate this authority if required.

Note: *The responsibility as the originator belongs to the functional position from which the information was originally prepared, not necessarily the individual who prepared the document.*

5. For printed material, the Protective Marking is to be changed by crossing out the previous marking and clearly labelling or stamping the new marking. The originator is to then sign and date the front page and note the authority for the change. All copies of the reclassified information are to be amended in the same way. The alteration can be performed by the holders of the information after having received written authorisation from the originator. Form XC040 (Classified Document Register) is to also be amended when the Protective Marking is altered.
6. **Downgrading or Declassification of a document.** Form XC021 – *Downgrading or Declassification of Classified Documents* is to be used when downgrading or declassifying a document that is classified PROTECTED or higher. Users are to follow the instructions contained within Form XC021.
7. **Electronic Records.** The same principles apply when altering the Protective Markings of an electronic record. In this instance, the metadata is amended to reflect the new Protective Marking.
8. **Files.** The registry **must** be informed when a file needs reclassification due to the removal or addition of classified information. If classified information added is of a higher nature than the file, the file classification **must** be upgraded. The file cover is to be temporarily amended until such time the file is returned to the registry, where a change will be made to its Protective Markings.
9. **Removal.** Removal of any information from a file is to be completed in accordance with Defence Records Management Policy. For further information, refer to the Records Management Policy Manual (RECMAN).
10. **Archives.** The NAA or the Australian War Memorial in consultation with the Director of Classified Archival Records Review (DCARR) will review information in the open period that is the subject of a public access request under the [Archives Act 1983](#). The DCARR may also review protectively marked archival material as part of a proactive program in anticipation of public access requests under the *Archives Act 1983*. Refer to RECMAN for further information.

Note: The DCARR does not provide a general declassification service for Defence. Where a work group requires advice on the continuing sensitivity of a particular topic for a record that is more than 15 years old, DCARR may be able to assist.

Note: If the record is more than 15 years old, a person may be guilty of an offence under the Archives Act 1983, s26(1)(c) if the classification is altered without the permission of the NAA.

11. If the archival records are held by a service history unit, then that unit will be responsible for reviewing the information of their service only. Joint service records are to be reviewed in liaison with the relevant Service work groups.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Reviewing and Altering Protective Markings
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2018	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex D Assessing and Protecting Official Information – Release of Official Information

1. Official Information can include public sector information sanctioned for public access or circulation, such as websites.
2. The authorisation for the release of Official Information is to be managed in accordance with:
 - a. the Defence Web Estate Manual (WEBMAN) where information is being released on the internet; and
 - b. in compliance with the [Privacy Act 1988 \(Cth\)](#) when personal information is involved.

Other Australian Government Agencies

3. Official Information owned or originated by Defence can be released to other Australian Government agencies that are subject to the [Australian Government Protective Security Policy Framework](#) (PSPF), unless the originator has placed any limitations on its release to the contrary. If there is any doubt, the originator's approval is to be provided before the release can occur.

Foreign Governments and Officials

4. The release of Official Information to foreign governments, foreign individuals and other foreign entities is to be completed in accordance with DSPF Principle 15 – *Foreign Release of Official Information*.

Intra-Government Presentations

5. Presentations at which only appropriately cleared Australian Government employees and integrated officers are present do not constitute public release. The presenter is to:
 - a. confirm that the security clearances and nationalities of the audience are appropriate and covered by an SIA;

- b. confirm that the physical security and IT accreditation of the facility are appropriate;
- c. inform the audience of the classification level of the information being disclosed; and
- d. remind the audience of its obligation under the DSPF to protect the information.

Public Release

6. Public release of Official Information, including through a tender briefing, is to be done in accordance with the Defence Communication Manual, Chapter 2 – *Media Engagement and Public Comment*.

7. Where Official Information is intended for public release or publication, it may have confidentiality requirements before release (for example, Budget papers.) In these instances, when applying Protective Markings, the originator is to indicate when the information is to be released to the public and the Protective Markings removed.

Freedom of Information

8. The release of Official Information in response to a freedom of information request is to be completed in accordance with the [Freedom of Information Act 1982](#) (the FOI Act). For advice, contact the Freedom of Information Directorate.

Note: The FOI Act has exemptions from disclosure for Official Information affecting national security, Defence or international relations. It also has an exemption for information communicated in confidence by a foreign government. This includes information communicated pursuant to any agreement or other formal instrument on the reciprocal protection of classified information, such as Security of Information Agreements and Arrangements.

Release to Industry

9. Information protectively marked as 'OFFICIAL: Sensitive' or an IMM may be released to persons engaged under a contract subject to the need-to-know principle.

10. Industry accessing this information may require Defence Industry Security Program (DISP) membership. DISP membership for access to information at this level is not mandatory but may be required, subject to a security risk assessment. For further information refer to DSPF Principle 16 – *Defence Industry Security Program*.

11. Official Information that is classified 'PROTECTED' and above is only to be released to DISP members which have:

- a. staff cleared to the required level of access;

- b. accredited facilities to store the material; and
- c. (if electronic access is necessary), accredited ICT systems to process the material.

Exclusion: 'PROTECTED' material in hardcopy form may be released in limited quantities to non-DISP members and other individuals that do not hold a security clearance. Refer to DSPF Principle 41 – Temporary Access to Classified Information and Assets for release criteria that apply to access to 'PROTECTED' material without a BASELINE security clearance.

State, Territory and Local Governments

12. The release of Official Information to State, Territory and local government departments and agencies, or any agency not bound by the PSPF, must have the written approval of the owner or originator of the information who must hold a position at or above the EL2 / O-6 level. For further advice, contact the Defence Security and Vetting Service (DS&VS) Regional Office or the Executive Security Advisor.

Courts

13. Where documents sought under a court order are classified, the Subpoena Clerk in the Directorate of Litigation (DLIT) is to be contacted as soon as possible. The Subpoena Clerk will seek advice from a Legal Officer in the DLIT and consult DS&VS about the release of the documents.

Parliamentary Committees

14. All Defence involvement in Parliamentary Committees requires approval from the Minister for Defence. For further information refer to the Ministerial and Parliamentary Branch.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Release of Official Information
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex E to Assessing and Protecting Official Information – Registration of Protectively Marked Information

1. All information classified 'TOP SECRET', and accountable material, held by Defence must be registered. Information at other classifications held by Defence should be registered.
2. All information classified 'SECRET' and above, and accountable material, held by Defence Industry Security Program members must be registered. Information at other classifications held by Defence Industry Security Program members should be registered.
3. When manual methods are required for classified document recording, Form XC040 – Classified Document Register (Defence) (CDR) is to be used. Defence Industry Security Program (DISP) members use Form AC458 – Classified Document Register (Industry).

Note: CDRs are to be classified on their merits and not according to the security classification of the documents they record, unless the title of the document itself is security classified. In this instance, it is suggested that the originator create a separate 'OFFICIAL' reference title. With due care, the CDR should rarely need to be classified. Where the volume of correspondence justifies it, separate registers for each classification and inwards and outwards correspondence may be used.

4. The Objective application offers electronic registration and auditing features which are compliant with the [Archives Act 1983](#) and meet some of the registration requirements of the DSPF. The following instructions apply to the use of the Objective application:
 - a. Codeword information must not be stored in Objective on either the Defence Protected Network (DPN) or Defence Secret Network (DSN).
 - b. Where a classified document is created as an electronic document within Objective there is no requirement to register that document into a CDR. Classified documents created in Objective are not to be placed on hard copy files, instead they should be stored on Objective virtual or mixed mode file.

- c. When converting a physical record to a digital record it is necessary to ensure that the new digital record remains authentic, reliable, integral and usable. The integrity of the record is to remain protected, complete and unaltered by the digitisation process. When original source records are digitised they are to inherit the access, destruction or transfer arrangements applicable to the original physical record. For further information, refer to the Records Management Manual (RECMAN).
 - d. The preferred method of distributing documents is by sending an Objective link. When a document classified 'SECRET' or above is printed from Objective for manual distribution, the document is to include the Object ID.
 - e. A CDR entry is required to track dispatch and return receipt of the physical document via Form XC051 – *Dispatch Advice/Receipt for Classified Matter*. For further information on the requirements for the physical transfer of classified information refer to DSPF Principle 71 – *Physical Transfer of Information and Assets*.
5. 'TOP SECRET' information is to be registered in a separate Form XC040 or Form AC458 as applicable. It is recommended that access to 'TOP SECRET' registers is limited to individuals with a demonstrated need-to-know for the subject matter and for the extent of 'TOP SECRET' holdings of a particular military or business unit.
6. **Registration of hard copy draft or working papers.** Material that is accountable or classified 'TOP SECRET' must be registered in a CDR when:
- a. completed as a finished document; or
 - b. retained for more than seven days after creation, regardless of the stage of development.
7. Classified hard copy draft or working papers are to be:
- a. dated when created;
 - b. marked with their overall classification, and with the annotation 'Draft' or 'Working Paper'; and
 - c. destroyed when no longer needed.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Registration of Protectively Marked Information
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Defence Security Principles Framework (DSPF)

Annex F to Assessing and Protecting Official Information – Official Information Filing and File Census

1. Official Information is to be filed in accordance with the [Archives Act 1983](#) and the Records Management Policy Manual (RECMAN).
2. A file **must** carry, as a minimum, the Protective Marking of the highest level of security classified information it holds. When new information is added to the file, the file user is to ensure that the classification carried by the file is still appropriate. If the information to be added is at a higher classification than the file itself, the file user is to reclassify the file before attaching the new document.

Note: Active files that are protectively marked with former security classifications and X-in-Confidence markings are to be remarked with the equivalent current security classification Protective Markings. Refer to this DSPF Control for further information on equivalences.

3. Official Information that can be filed is to be placed on an appropriate file as soon as possible after its creation or receipt.

File Types

4. It is essential that the Protective Marking of the file be clearly and easily identifiable and easily distinguished from other Protective Markings. The standard colour file covers for security classified files are:
 - a. 'TOP SECRET' – red;
 - b. 'SECRET' – salmon/pink;
 - c. 'PROTECTED' – blue (formerly: green plus stripe pre-01 October 2018 PSPF revision); and
 - d. 'OFFICIAL: Sensitive' – yellow.

Active File Types with outdated Protective Markings

5. Files that carry former Protective Markings may continue to be used and active. The following applies:
 - a. Former 'CONFIDENTIAL' – green (Files should be closed to new documents, active information in the file should be reassessed, marked and stored appropriately);
 - b. Former 'RESTRICTED' and 'X-in-Confidence' file covers may continue to be used, over stamp the former protective marking with the new protective marking and remark the file in the appropriate records management system.

Filing Procedures

6. The normal filing procedures such as file reference and folio numbering can be used for security classified files to maintain a record of the information held on the file. It is also good practice to follow normal filing procedures such as recording the date and name of the person holding the file from time to time.
7. It is recommended all Defence files have a folio sheet placed in the inside front cover of the file. An example of a folio sheet is provided at Table 1 of this DSPF Annex.
8. If a folio sheet is used, it is recommended all files have the documents within the file folio numbered sequentially.

Table 1: Example of Folio Sheet

File Title:

File Number:

Folio	Date	Sender / Originator	Doc Type	Subject	Class	CDR

File Census

9. A file census of information classified 'PROTECTED', 'CONFIDENTIAL' (if active files remain), 'SECRET', or 'TOP SECRET', and accountable material is to be conducted at least every two years. At the discretion of the Commander or Manager, it is recommended that a file census occurs:

- a. annually, if substantial file holdings exist in the unit or facility;
- b. when the Security Officer or document custodian changes; and
- c. if a security incident or suspected compromise of a file occurs.

How to Conduct a File Census:

10. The Security Officer conducts or coordinates the census on behalf of the Commander or Manager. The local procedure for the census is recorded in the unit or facility Security Standing Orders.

11. All files are to have their documents checked against the folio sheet. Details of any missing documents are to be retrieved from the folio sheet and, if applicable, from the classified document register. Action to be taken as a result of missing documents is detailed in DSPF Principle 77 – *Security Incidents and Investigations*.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Official Information Filing and File Census
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex G to Assessing and Protecting Official Information – Copying and Reproduction of Protectively Marked Information

Copying and Reproduction

1. To help reduce the risk of compromise, copying and reproducing protectively marked Official Information is to be done only when it is necessary. Spare or spoilt copies of protectively marked Official Information are to be destroyed immediately. Refer to Annex H of this DSPF Control for further information on disposal and destruction methods. This destruction is defined as 'normal administrative practice' in terms of the [Archives Act 1983](#) and does not need specific permission from the National Archives of Australia.

Note: The scanning of documents into Objective for filing is an administrative procedure and does not constitute copying or reproduction. Refer to Annex F of this DSPF Control for further information on scanning documents into Objective.

2. For information classified 'SECRET' and above, Defence Industry are to record details of copies and reproductions in a Form AC458 classified Document Register (Defence) (CDR). In the case of 'TOP SECRET' and Accountable Material, each original document and reproduced copy is to be numbered. Any additional protective measures imposed by the originating authority are to be strictly observed. Persons authorising the copying of 'TOP SECRET' information are to record in the file bearing the original the details of the number of copies made and their distribution.

3. Accountable material **must not** be copied or reproduced by anyone other than the originator. If extra copies of such documents are required, additional copies are to be requested from the originator. Information must not be extracted from accountable material without the permission of the originator.

Exclusion: 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 agencies' document handling procedures for further information on the operation of exclusions to this policy within their agency.

Use of Multi-Function Devices

4. Most current Multi-Function Devices (MFD) incorporate data storage capabilities in the form of non-volatile memory such as hard disks or flash memory. Combined with communication and data transfer capabilities, MFD are effectively ICT systems.

5. Any entity providing MFD including photocopiers, printers, facsimile machines and similar devices, must treat these as part of the ICT system to which they are connected, with security addressed in accordance with DSPF Principle 20 Information Systems Lifecycle Management.

Example: A multi-function printer / photocopier device connected to the DRN is to be considered as part of the DRN and be managed from a security perspective in accordance with DSPF Principle 20 Information Systems Lifecycle Management.

6. Any MFD that are not connected to a larger ICT system or network must be treated as ICT systems in their own right, with security addressed in accordance with DSPF Principle 20 – *Information Systems Lifecycle Management*.

Note: A collection of independent MFD may be certified and accredited as a fleet and covered by a single set of security documentation.

7. Standard Operating Procedures (SOP) covering the use of MFD must be available to users.

8. MFD must be used in accordance with the applicable SOP.

Commercial Printing

9. If a commercial printing service is considered for the copying or reproduction of Official Information not intended for public release then it may be required to be a member of the Defence Industry Security Program (DISP), depending on the volume and type of information. For further information on considerations by Commanders or Managers in this regard refer to DSPF Principle 16 – *Defence Industry Security Program*.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Copying and Reproduction of Protectively Marked Information
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex H to Assessing and Protecting Official Information – Disposal and Destruction of Protectively Marked Information and Assets

1. Disposal of any Commonwealth record is to be done in accordance with the [Archives Act 1983](#) (the Act). Under the Act it is illegal to destroy Commonwealth records without the permission of the National Archives of Australia (NAA), or in accordance with a practice or procedure approved by the NAA, unless the destruction is required by law.

Note: For Defence policy refer to the Records Management Policy Manual (RECMAN).

Disposal and Destruction Procedures

2. When 'TOP SECRET' information and assets or accountable material need to be destroyed, the destruction must be conducted under the supervision of two persons who are security cleared to at least the classification of the information or asset being destroyed.

Recording Disposal and Destruction

3. Details of the disposal of all classified documents or assets recorded in the Classified Document Register (CDR) are to be clearly annotated alongside each individual document record and those carrying out the destruction are to sign the CDR or document register.

4. The originator of a copy-numbered classified document must be consulted prior to the destruction of such a document. If the originator approves destruction of the copy-numbered document, the destruction is to also be recorded by completing Form XC024 – Certificate of Destruction for Classified Material. The completed Form XC024 is then to be sent to the document originator.

5. For as long as any one document recorded in a given CDR is still in existence, the CDR is to be maintained. Following destruction of the final document recorded in a CDR, the CDR is to be retained for at least five years before being destroyed in accordance with RECMAN.

6. The book of Form XC051 – Dispatch Advice/Receipt for Classified Matter must be retained for at least five years after the last Form XC051 is returned. For information regarding CDR, refer to the DSPF Principle 71 – *Physical Transfer of Information and Assets*.

7. **Caveat – CABINET (Previously DLM Sensitive: Cabinet)** Information which bears the CABINET caveat is to be disposed of in accordance with the practices mandated by the Department of the Prime Minister and Cabinet. Refer to the [Cabinet Handbook](#).

8. **High grade cryptography and communications security.** High grade cryptography and communications security (COMSEC) material is to be handled in accordance with the DSPF and its authoritative sources.

9. **Electronic media.** Electronic media is sanitised/destroyed in accordance with the requirements of the Information Security Manual ([ISM](#)).

Shredders

10. Shredders used to destroy paper-based classified information are to be compliant with the requirements found in the current ASIO Security Equipment Guide (SEG)-01 *Class A and B Paper Shredders*.

11. Shredders used to destroy ICT media containing classified information are to be compliant with the requirements found in the current ASIO SEG-09 *Optical Media Shredders*.

Note: Commercial strip shredders are not suitable for the destruction of classified or sensitive information. The smaller the particle size the more secure the results.

Destructors

12. Destructors (disintegrators and hammermills) used to destroy both paper-based and ICT media containing classified information are to be compliant with the requirements found in the current ASIO SEG-18 *Destructors*.

Garbage and Recycling

13. Protectively marked information is not to be disposed of by garbage or unsecure recycling collection unless it has already been through one of the above approved destruction processes.

14. Garbage, whether it is placed in a garbage hopper or other area for collection or delivered directly to a garbage disposal service, is extremely vulnerable. Only information that is public domain information or has already undergone an approved destruction process, such as shredding, may be discarded in Defence general garbage.

15. Recycling or discarding intact documents does not serve the same purpose as document destruction and can only be used for public domain information disposal or when information has already undergone some form of appropriate destruction, such as shredding.

Contracted Disposal and Destruction

16. It may be considered necessary, after a comprehensive risk assessment, for the disposal of security classified waste to be undertaken by an authorised disposal company. Requirements can be found in ASIO Protective Security Circular 167 – External Destruction of Security Classified Information.

17. The destruction of 'TOP SECRET' or accountable information or assets is to occur within a Defence facility. The originator of the information may also apply special conditions to the destruction of some classified information which might prohibit the use of person/s engaged under a contract. Form XC024 – Certificate of Destruction for Classified Material, is to be sent to the originator upon destruction of the material.

18. Classified waste bags are used to temporarily store classified waste until a person/s engaged under a contract can carry out complete destruction. Classified waste bags must be stored according to the highest level of classification of their contents.

Destruction of Classified Information Overseas

19. Where possible, classified information or assets located overseas are to be transferred to an Australian controlled area, such as an Australian Embassy or High Commission, for destruction if appropriate transportation for the classified information or asset back to Australia cannot be arranged.

Note: Classified information and assets created or transferred overseas must be handled in accordance with DSPF Control 71.1 – Physical Transfer of Information and Assets.

Emergency Destruction Plan

20. Defence units are sometimes in sensitive areas where there is a risk of uninvited entry by unfriendly forces. In such cases, Commanders of Defence units in sensitive areas must develop an emergency destruction plan. The Commander should appoint a Security Officer, or an appropriate officer in the unit, to be responsible for keeping the emergency destruction plan current.

21. The emergency destruction plan is to:

- a. identify the order and method of destruction of all classified documents and information embedded in electronic systems; and

- b. ensure that the most highly classified and sensitive information or assets are destroyed first should the complete destruction of all classified information be necessary.
22. If Security Standing Orders are applicable to a unit on deployment, the plan is to be incorporated into those orders.
23. **Aircraft.** Contingent Commanders who have aircraft making flights over foreign territories must develop:
- a. a list of security classified information or assets carried on each type of aircraft; and
 - b. a plan detailing the order and method of destruction of each classified item.

Additional Requirements for Classified Assets

24. Classified assets must be destroyed so that:
- a. the security nature of the asset cannot be identified;
 - b. security classified performance details or data cannot be recovered;
 - c. components, if not totally destroyed, are no longer operational; and
 - d. the relationship of components to the overall asset cannot be identified.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Disposal and Destruction of Protectively Marked Information and Assets
Annex Version	4
Annex Publication date	29 September 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	29 September 2020	AS SPS	Update of Cabinet Handbook hyperlink



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex I to Assessing and Protecting Official Information – Remarking Information Bearing Former Protective Markings

1. The Attorney-General's Department updated the Protective Security Policy Framework (PSPF) in October 2018, and included a revised system of Protective Markings for classified information and assets. All non-corporate Commonwealth Agencies are required to transition to the revised system by 01 October 2020.

Legacy Protective Markings

2. There are legacy Protective Markings in circulation across the Australian Government that no longer reflect Government or Defence security policy. Defence personnel and persons engaged under a contract are required to handle, transfer, transmit and store Official Information with a legacy Protective Marker in accordance with their current equivalency as detailed in Table 1 of this Annex.

3. Protective Markers on published documents do not require marking, but should be handled in accordance with their current equivalent as detailed in Table 1.

4. Only active documents that have not yet been published require remarking, regardless of their level of approval. All new documents require the use of the new Protective Markers detailed in this Control.

5. The remarking of documents from legacy Protective Markers to the current Protective Markers does not require the permission of the document's originator. However any caveats such as CODEWORD or release markings cannot be modified under these provisions.

Table 1: Legacy Protective Markings and their current equivalency

Legacy Protective Marking	Date Ceased in Defence	Current Equivalent
'UNCLASSIFIED'	22 June 2020	'OFFICIAL'
'For Official Use Only'	22 June 2020	'OFFICIAL: Sensitive'
'CONFIDENTIAL'	22 June 2020	Discontinued; Follow requirements for 'SECRET'.
'Sensitive'	22 June 2020	'OFFICIAL: Sensitive' *There is no direct equivalent under the new Information Management Markers.
'Sensitive: Cabinet'	22 June 2020	'PROTECTED' or higher *'Cabinet' is now a caveat with specific handling instructions. It can only be used with a security classification.
'Sensitive: Personal'	22 June 2020	'Personal privacy' *Must be used with the Protective Marker of 'OFFICIAL: Sensitive' or higher.
'Sensitive: Legal'	22 June 2020	'Legal privilege' *Must be used with the Protective Marker of 'OFFICIAL: Sensitive' or higher.
'HIGHLY PROTECTED'	01 August 2012	'SECRET'
'RESTRICTED'	01 August 2012	'OFFICIAL: Sensitive'
'LEGAL-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Legal privilege'.
'CABINET-IN-CONFIDENCE'	01 August 2012	'PROTECTED' or higher with the caveat 'Cabinet'.
'COMMERCIAL-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive'
'AUDIT-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy' if it includes personal information.
'SECURITY-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy' if it includes personal information.
'COMMITTEE-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive'
'MEDICAL-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'

Legacy Protective Marking	Date Ceased in Defence	Current Equivalent
'PSYCHOLOGY-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'CLIENT-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'STAFF-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'HONOURS-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Remarking Information Bearing Former Security Classifications
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy Updated Protective Markings.



Defence Security Principles Framework (DSPF)

Annex J to Assessing and Protecting Official Information – Creating and Managing Information Compartments

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Creating and Managing Information Compartments
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Assessing and Protecting Official Information
DSPF Number	Control 10.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	31 May 2019	AS SPS	Created to consolidate classified content.
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy.



Defence Security Principles Framework (DSPF)

Security for Projects

General principle

1. Projects of a type referred to in the Expected Outcomes below, with an appropriate Steering Group (SG), need to incorporate security planning into project activities and all stages of the One Defence Capability System. Security is to be maintained throughout the planning and execution of all projects. Planning is to incorporate the expenditure required to deliver appropriate security measures.

Rationale

2. Projects and SGs carry significant security responsibilities. Failure to adequately protect official information and any capability that is acquired or supported, both during the project phase and on the introduction into service of any new capability, has security and financial consequences for Defence. Failure to consider and forecast security requirements throughout the capability's lifecycle, including assessing the security impacts on all Fundamental Inputs to Capability (FIC) elements, could lead to:

- a. project delays;
- b. increased security risks;
- c. security compromised capabilities;
- d. systematic security failings between Support Organisations and Project/Capability Managers; and
- e. increased costs due to remediation activities.

Expected outcomes

- 3. Security planning is undertaken for all projects that involve:
 - a. acquisitions conducted under the [Defence Integrated Investment Program](#);
 - b. the establishment, or major renovations, of the Defence estate or facilities infrastructure;

- c. collaborative engagements between industry or allies (e.g. joint ventures, outsourcing, or research and development.); or
 - d. some aspect(s) requiring consideration to be given to security matters.
4. Compliance with security policy is maintained during project planning and execution stages, and throughout all phases of the One Defence Capability System.

Note: Although projects are unlikely to run for the full duration of a capability's life cycle they should consider the security implications of as many phases of it as appropriate in the circumstances.

5. Adequate risk mitigation strategies are in place.
6. Security costs and accountabilities are included in the project design and delivery.
7. Project Security Risk is considered and managed through this Principle and Defence Security Principles Framework (DSPF) Control 11.1 – Security for Projects, alongside other risk under [Accountable Authority Instruction 1 - Managing Risk and Accountability](#). DSPF 4a, Governance and Executive Guidance also provides framing for Defence Security Risk management.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Functions Delivery (ASFD) through Branch Head (or equivalent)
High	Defence Security Committee (DSC) – through ASFD
Extreme	DSC – through ASFD

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Consideration may also be given to brief the Project Managers chain of command prior to elevating risks to ASFD.

Document administration

Identification

DSPF Principle	Security for Projects
Principle Owner	First Assistant Secretary Defence Security Division (FAS DS Division)
DSPF Number	Principle 11
Version	3
Publication date	1 September 2023
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 11.1
Control Owner	Assistant Secretary Functions Delivery (ASFD)

Related Information

Government Compliance	<u>PSPF Core Requirements:</u> Security Planning; Security governance for contracted service providers; and Eligibility and suitability of personnel. Legislation: Workplace Health and Safety Act 2011 (Cth) Standards: AS: 4811-2006: Employment screening
Read in conjunction with	Defence Security Principles Framework 4a, Governance and Executive Guidance Principles: 12 - Security for Capability Planning; 16 – Defence Industry Security; and 82 – Procurement. Capability Program Management Manual
See also DSPF Principle(s)	Principles: 10 – Classification and Protection of Official Information; 15 – Foreign Release of Official Information; 17 – Information Systems (Physical) Security; 18 – Information Systems (Personnel) Security; 19 – Information Systems (Logical) Security; 23 – ICT Certification and Accreditation 40 – Personnel Security Clearance; 41 – Temporary Access; and 71 – Physical Transfer of Official Information, Security Protected and Classified Assets.
Implementation Notes, Resources and Tools	Security Equipment Guides (SEGs) via the Security Toolkit. ASIO Tech Notes via the Security Toolkit. Security Equipment Evaluated Product List (SEEPL). This list contains products endorsed by the Security Construction and Equipment Committee (SCEC). Contact 1800DEFENCE or your Executive Security Adviser (ESA). The Defence Industry Security Program.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	1 September 2023	FAS DS	Amendments to update with the release of the Capability Program Management Manual, the One Defence Capability System, and administrative changes.



Defence Security Principles Framework (DSPF)

Security for Projects

Control Owner

1. The Assistant Secretary Functions Delivery (ASFD) is the Control Owner for this control under the Administration & Governance Domain of the administrative policy framework (which includes security). The Associate Secretary is the Accountable Officer for this domain. The First Assistant Secretary Defence Security Division (FAS DS Division) is the Policy Owner for security.
2. The ASFD is also the Policy Owner for Program Management under the Acquisition & Sustainment domain. The Deputy Secretary, Capability Acquisition & Sustainment Group (DEPSEC CASG) is the relevant Accountable Officer. The Executive Director Program Management is the Program Management Function Lead as defined in the [Capability Acquisition and Sustainment Group Business Framework](#).

Framework Escalation Thresholds

3. Security Risk Responsibility allocation does not override overall Risk Management Responsibilities as articulated in [Accountable Authority Instruction 1 - Managing Risk and Accountability](#).
4. The ASFD has set the following general threshold for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Functions Delivery (ASFD) through Branch Head (or equivalent)
High	Defence Security Committee (DSC) – through ASFD
Extreme	DSC – through ASFD

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel. Refer Annex A within for flow chart.

Consideration may also be given to brief the Project Managers chain of command prior to elevating risks to ASFD.

Controls

Project Security Planning

5. On appointment of an appropriate Steering Group (SG) under the One Defence Capability System, the Project security planning process is used to identify and document the relevant security authorities, standards, specifications, procedures and practices necessary to comply with Defence security policy during the Project. The Project security planning process should gather information from, and be a continuation of, any previous security planning.

6. This process is based on a risk management approach, and is maintained throughout the Project's life. A security plan for the Project is developed from the following process:

- a. for major capital Projects, security risk will be recorded in the Project's risk register in accordance with business processes for managing Project risk; or
- b. for smaller Projects, security risks can be recorded in a separate register.

7. The security planning processes are recommended for all other Defence capability proposals and Projects

Project Security Function

8. Projects are to consider the need for the appointment of a Project Security Officer.
9. In addition to a Project Security Officer, an appropriate SG is to be responsible for the Project security function for major capital Projects, infrastructure Projects involving new Defence facilities and major renovations to the Defence estate. This function should also be established for minor capital and collaborative Projects.
10. The composition of SG members will depend on the Project. Membership may comprise representation from:
 - a. the Project Owner / Project Sponsor;
 - b. the Executive Security Advisor (ESA);
 - c. Chief Information Officer Group (COMSEC and Defence Information Environment architects);
 - d. ICT and physical certification and accreditation authorities;
 - e. business process owners and those who share Project security risk;
 - f. the Service Delivery Division, Security and Estate Group particularly where there are extensive changes to the Defence estate;
 - g. the Base Support Manager or Senior Australian Defence Force Officer (SADFO) at bases that house related facilities and assets; and
 - h. contractor(s), when selected.
11. The Project security function should advise the SG Manager and Project Sponsor on security matters such as:
 - a. developing and approving Project Security Instructions (PSI) that meet stakeholders' needs;
 - b. coordinating concurrent security activities across multiple Projects and areas;
 - c. identifying security risks and treatments;
 - d. identifying security costs, including security costs and resources that will be required of areas outside Project managers control; and
 - e. engaging with accreditation authorities.

Project Planning

12. Project security costs are to be identified and resourced throughout all stages of the planning for and execution of a Project (refer to [Pages - Project Controls](#)). Security costs are to be identified for all Fundamental Inputs to Capability (FIC) throughout all stages of the [One Defence Capability System](#). Considering these costs early in Project planning allows for more accurate costing and scheduling of important Project security activity, including, but not limited to:

- a. Project Office and contractor security arrangements, including:
 - (1) gaining facility or [ICT system accreditation](#); and
 - (2) identifying the requirement for staff or external service providers to obtain personnel security clearances or DISP membership as appropriate (refer DSPF Principle 16 - *Defence Industry Security Program*); and
- b. asset and Capability security lifecycle costs, including:
 - (1) in service security costs such as additional security clearances, physical security infrastructure and enhanced guarding requirements on introduction to service; and
 - (2) disposal costs such as the destruction of security classified equipment or sanitisation of ICT resources prior to resale or disposal.

Project Security Reviews

13. Project security reviews are to be conducted throughout the Project. The purpose of a Project security review is to confirm that security documentation is current and that all security risks are identified and appropriately treated. Regardless of the size or complexity of a Project, the Project's security related documentation should be updated regularly so that it is relevant to the Project's activities.

14. For capital and intelligence Projects, the Integrated Project Manager should conduct Project security reviews at least annually, and to inform One Defence Capability System stages and processes including but not limited to:

- a. Decision making forums convened by appropriate Steering Groups;
- b. Health Checks;
- c. Independent Assurance and In-Depth reviews;
- d. Before Gate approvals;

- e. During the Risk Mitigation and Requirements Setting Phase if Capability risk mitigation activities are being held, for example, a major trial;
 - f. Prior to tender documentation being released;
 - g. On acceptance of the preferred solution, in order to identify any security implications of the preferred solution, including costing of security impacts, in preparation for contract negotiations;
 - h. During the Acquisition Phase, in order to ensure the implementation of agreed security measures by the Integrated Project Manager and external service providers;
 - i. Immediately prior to the transition into service, in order to ensure that Capability owners have adequate security in place to take delivery; or
 - j. Prior to disposal, to ensure the secure disposal of classified resources and the return of all official information and assets from external service providers.
15. For research and Projects other than major or minor capital Projects and intelligence Projects, the Project Managers:
- a. should conduct a Project security review of security risks and relevant Project documentation prior to Project approval in order to:
 - (1) confirm compliance with security policy;
 - (2) ensure adequate risk mitigation strategies are in place; and
 - (3) confirm that security costs have been included in the Project design and delivery.
 - b. should conduct Project security reviews at least annually after Project approval.

Note: It is recommended that Integrated Project Managers observe the schedule above at the equivalent phases of the Project.

Note: For smaller Projects not included above, a Project security review may entail the development of a series of exploratory questions to determine appropriate levels of security preparedness. Exploratory questions could include - is classified infrastructure required? Are there enough security cleared staff available? Does the Project have the room to store all of the documents it will be producing?

Security Activities by One Defence Capability System Phase

Strategy and Concepts Phase

16. A security risk assessment should be conducted during the development of the Gate 0 Business Case and be documented as part of the Integrated Project Management Plan in order to ensure that security costs are included in the design planning for the Project and the introduction into service of the planned Capability.

17. During this phase, the following security aspects should be addressed:

- a. classification of the existence of the Project;
- b. security of Project management activities;
- c. identification of the Project;
- d. who is involved;
- e. where and how the Project will be managed and/or developed;
- f. the requirement for secure communications Capability between Project stakeholders;
- g. schedule of security related activities such as accreditation of facilities and ICT systems; and
- h. the security of the Capability to be acquired, including transition into service, in-service support and disposal.

Note: This information may start out generically and be tailored as the Project moves towards later acquisition phases.

18. For all major and minor Projects, and based on a risk assessment, the Integrated Project Manager (or Project Sponsor or Project Director if no Project Manager has been appointed), should provide to the Defence Security Division (DS Division) the following security documents for approval:

- a. Project Identification Document (PID) - refer to the recommended format on the [Defence Security Portal](#);
- b. Security Classification and Categorisation Guide (SCCG) – refer to the recommended format in [DS Division Security Operations – Projects](#); and

Note: Projects acquiring assets with an existing Security Classification Guide provided by the vendor nation may incorporate it into the Australian SCCG as an annex. DS Division is to be consulted in this instance.

- c. Program/Project Security Instruction – The [PSI Template](#) should be completed for any projects with an Australian Resident project team overseas, or that operate under a Bilateral or Multinational Cooperative Defence Program or Project Arrangement. Security Standing Orders otherwise apply.

Note: These documents are to be provided to Project.Security@defence.gov.au at the earliest possible stage of the project

*The PID, PSI and SCCG may not be mature at this Phase of the One Defence Capability System. They **must**, however be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review.*

19. For Defence intelligence agencies' projects, the documents listed above should be approved by the Deputy Secretary Strategic Policy and Intelligence, the head of the relevant intelligence agency or its senior management committee.

20. Integrated Project Managers are to contact the DS Division for advice regarding projects with overseas components to ensure compliance with any international obligations.

21. Where the project has staff located overseas (such as when staff are part of a Resident project team), and based on a risk assessment, a separate PSI covering the overseas components should be produced using the template on the [Defence Security Portal](#).

22. Security classifications and [Business Impact Levels](#) (BILs) are applied to the systems, sub-systems, components and project information via the SCCG. The measures required to protect the information and assets are then identified and documented in the PSI.

23. Research projects, and projects other than capital and intelligence projects, are not required to submit any of the above documentation to DS Division; however, the Project Manager should develop a SCCG if the project involves:

- a. a significant scientific breakthrough with implications for national security;
- b. a designated high technology area of research; or
- c. commercial sensitivities, including:
 - (1) a development unique to Australia that might have marketing potential;
 - (2) individuals or organisations outside of Defence, such as academic or commercial research and development specialists; and
 - (3) a patent application.

24. Integrated Project Managers are responsible for the production of security documentation. The DS Division can provide assistance in their development.

Risk Mitigation and Requirements Setting Phase

25. During this phase the following security aspects are considered:

- a. trials and risk mitigation activities;
- b. tendering and tender response activities (including security requirements related to the release of project-specific official and classified information); and
- c. where multiple Capability solutions are being compared, security aspects are considered for each solution:
 - (1) solution specific risks, including Capability risks and any shared risks introduced by a proposed solution; and
 - (2) associated security costs.

26. Where a project involves trials and testing, a security plan covering these elements should be developed.

27. Where testing of equipment is conducted, the classification of information in relation to the performance of equipment should be reviewed after the activity has occurred. This is necessary as the actual performance of the activity may differ to that anticipated at the beginning of the project and could impact the classification level.

28. If changes are made during negotiations, the PID should be resubmitted to the DS Division before contract signature.

Note: The PID, PSI and SCCG **must** be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review, and forwarded to DS Div at project.security@defence.gov.au.

Acquisition Phase

29. DSPF Principle 82 - *Procurement* addresses many security issues that projects will encounter during the acquisition phase. Immediately prior to the transition into service phase, the scheduled security review should be conducted. The focus of this review is to ensure that Capability owners have adequate security in place to take delivery. It is important that SCCGs are reviewed prior to the introduction into service as this document will be used by the recipients of the Capability to determine security for the delivered solution.

30. During the transition into service phase, Integrated Project Managers are to monitor and review the security aspects of in-service support and, in conjunction with the Capability Users, regularly review SCCGs to ensure adequate protection measures remain in place.

Note: The PID, PSI and SCCG **must** be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review, and forwarded to DS Div at project.security@defence.gov.au.

In-Service and Disposal Phase

31. During the in-service phase, the project office will either assume responsibility for logistics security and maintenance security of the delivered Capability, or the project will be complete. Security procedures for the logistics security and maintenance security functions will require regular review to ensure that they remain effective.

32. Immediately prior to the disposal or project closure phase, the scheduled security review should be conducted. The focus of this review is to ensure that classified material, including both assets and information, is correctly disposed of. Issues to consider are:

- a. security-protected assets are transferred, sanitised or destroyed as appropriate;
- b. appropriate security arrangements, including disposal arrangements for security-protected assets and classified information, are accepted by the Capability Manager responsible for the in-service operation of the delivered Capability;
- c. the project's official and classified information is archived; and
- d. External service providers associated with the project have returned all official information to Defence or have destroyed it.

33. During disposal, the Project Manager will monitor the disposal and transfer of information and security protected assets.

34. During project closure, Integrated Project Managers should:

- a. review the project's security performance and provide a report to the DS Division, noting any outstanding security issues as well as any lessons learnt during the conduct of the Project; and
- b. confirm that in-service support agencies have appropriate security arrangements in place to enable compliance with applicable parts of the DSPF.

Note: The PID, PSI and SCCG **must** be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review, and forwarded to DS Div at project.security@defence.gov.au.

Roles and Responsibilities

First Assistant Secretary Defence Security Division

35. FAS DS Division is responsible for:
- a. providing protective security advice to Integrated Project Managers and Project Security Officers; and
 - b. approving PSIs to ensure that all project security requirements have been adequately considered and addressed in the circumstances that Security Standing Orders do not apply.

Capability Managers, Delivery Groups and Enabler Groups

36. Capability Managers, delivery and enabler Group Heads are responsible for the security of all projects managed by their respective Groups and Services and for the appointment of the Project Managers responsible for a project's security. This responsibility may be delegated by Capability Managers to Program Sponsors and by delivery and enabler Group Heads to Program Managers.

Chief Defence Scientist

37. The Chief Defence Scientist (CDS) is responsible for the development of security policies and procedures to be applied to protect the research programs and associated collaborative activities undertaken by Defence Science and Technology Group (DST Group).

Chief Information Officer

38. The Chief Information Officer (CIO) is, where appropriate, responsible for:
- a. providing ICT and Communications Security (COMSEC) advice to Project Managers and Project Security Officers; and
 - b. reviewing SCCGs and PSIs to ensure that all ICT security and COMSEC recommendations have been adequately considered and addressed.

Program Sponsor

39. The Program Sponsor is accountable to the Capability Manager for:
- a. the management of security within the Project, including setting and controlling the project security tolerances and reporting requirements; and
 - b. ensuring that the outcomes of all program activities are achieved and aligned with Defence strategic objectives.

Program Manager

40. The Program Manager is responsible for the management of security of all projects within their Program and is responsible for the appointment of an Integrated Project Manager.

Project Sponsor

41. The Project Sponsor is accountable to the Capability Manager through the Program Sponsor for the management of security within the Project and is to work in partnership with the Integrated Project Manager to ensure capability outcomes are delivered.

Integrated Project Manager

42. The Project Manager is responsible for:
- a. the security of all aspects of the project, including managing the security risk associated with the project;

Note: external service providers, including Defence Industry Security Program (DISP) members, cannot accept security risks on behalf of the Commonwealth. Therefore, if DISP members or other external service providers are engaged, the Project Manager, via their contract manager, retains responsibility for managing all outsourced risks.

- b. ensuring that protective security requirements are considered and budgeted for throughout the project, including the consideration of security requirements associated with the Capability to be delivered by the project prior to its introduction into service;

Note: where a project is acquiring assets or building infrastructure, the Project Manager is responsible for security requirements planning and any related expenditure throughout the entire lifecycle of the assets or building infrastructure.

- c. advising the DS Division of the nature of larger projects and anticipated security impacts to facilitate the provision of advice to Project Managers and Project Security Officers by DS Division;

- d. advising CIOG of the nature of larger projects (with significant ICT infrastructure or accreditation requirements), and description of the ICT and COMSEC aspects of the project so that CIOG may provide advice to Project Managers and Project Security Officers;
- e. appointing a Project Security Officer for large or sensitive projects;
- f. ensuring that facilities and ICT systems used by the project to store, process or communicate official or classified information or material are accredited prior to use in accordance with DSPF Principle 23 - *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*;
- g. ensuring that appropriate security classification guidance is available to all Defence personnel and persons engaged under a contract associated with the project. To ensure proper coordination of all security matters within a project, the Project Manager is to determine the relevant Group or Executive Security Adviser for the project;
- h. ensuring compliance with Defence security policy within their project; and
- i. reviewing all security documentation, appointments and arrangements to ensure the ongoing security of the project, prior to commencement of the project.

Project Security Officer

43. Project Security Officers may assist their Project Manager with the necessary administrative actions to enable compliance with this DSPF part. This may include providing the Integrated Project Manager with security advice and support related to:
- a. the development, maintenance and review of Project security documentation;
 - b. the determination of the Project's ICT and physical accreditation requirements, refer to DSPF Principle 23 - *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*; and
 - c. the need for secure communications Capability between Project stakeholders (for further information regarding the requirement for secure communications, refer to DSPF Principle 10 – *Assessing and Protecting Official Information*.)
44. For small Project teams, the Integrated Project Manager may fulfil the role of Project Security Officer.

Defence Special Access Programs Project Managers

45. Project Managers responsible for Defence Projects that include Special Access Program (SAP) activities are to maintain the special security requirements applicable to the SAP framework. [The Special Access Programs Manual](#) assigns responsibilities and prescribes security procedures for implementation and use in the management, administration and oversight of all Defence SAPs.

Key Definitions

46. **Project.** A unique, finite, multidisciplinary and organised endeavour to realise agreed FIC deliverables within pre-defined requirements and constraints.

47. **Project Manager.** The person who has responsibility to plan and deliver the Project, inclusive of all agreed FIC to the specified scope, schedule and budget.

***Note:** Reference to Integrated Project Managers refers to Project managers engaged in Projects conducted as part of the One Defence Capability System (ODCS) process.*

48. **Steering Group.** The organisational entity established within the primary delivery and enabler Group which performs Project functions as part of the One Defence Capability System process. It is comprised of representatives from all relevant stakeholders, and may be an Integrated Project Management Team.

49. **Project Sponsor.** The primary representative of the Capability Manager and the Program Sponsor liaising directly with the Integrated Project Manager. The Project Sponsor is accountable to the Capability Manager and Program Sponsor for delivery of the Product. The Project Sponsor sets direction for the Project and ensures that activities and outputs are consistent with the Capability needs and priorities of the Capability user.

50. **Program Manager.** The person appointed within the delivery and enabler Group to conduct program management functions in support of acquisition and sustainment activities.

51. **Program Sponsor.** The person accountable for ensuring that the outcomes of all program activities are achieved and that these outcomes remain aligned with Defence strategic objectives. The Program Sponsor is accountable to the Capability Manager for the management of Capability throughout the One Defence Capability System.

52. **Resident project teams.** Defence personnel and/or persons engaged under a contract based overseas with foreign prime contractors on Defence acquisition Projects.

53. **Capability.** 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. Capability is generated by FIC comprising organisation, personnel, collective

training, major systems, supplies, facilities, support, command and management, and industry.

54. **Project Identification Document (PID)**. A document that provides information about the Project or Project phase. A PID indicates the anticipated level of protectively marked information and/or assets to be protected, in-country and overseas industry involvement, and likely ICT connectivity requirements.

55. **Security Classification and Categorisation Guide (SCCG)**¹. A document that records the security classification and Business Impact Level (BIL) given to each element of a Project or asset.

56. **Program/Project Security Instruction (PSI)**. A document that outlines how whole of Government and Defence program/Project security measures will be applied to the Project.

57. **Special Access Program (SAP)**. A high security, Capability protection framework that imposes need-to-know and access controls beyond those normally provided for access to PROTECTED, SECRET, or TOP SECRET information. The level of controls is based on the criticality of the program to the Defence mission and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.

Further Definitions

58. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Annexes and Attachments

Annex A: Project Security Risk Escalation Thresholds Flow Chart

¹ SCCGs were previously known as Security Classification Grading Documents (SCGD).

Document administration

Identification

DSPF Control	Security for Projects
Control Owner	Assistant Secretary Functions Delivery (AS FD)
DSPF Number	Control 11.1
Version	3
Publication date	1 September 2023
Type of control	Enterprise wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Security for Projects
Related DSPF Control(s)	Security for Capability Planning 10 – Classification and Protection of Official Information; 12 – Security for Capability Planning; 15 – Foreign Release of Official Information; 16 – Defence Industry Security Program 17 – Information Systems (Physical) Security; 18 – Information Systems (Personnel) Security; 19 – Information Systems (Logical) Security; 23 – ICT Certification and Accreditation 40 – Personnel Security Clearance; 41 – Temporary Access; 71 – Physical Transfer of Official Information, Security Protected and Classified Assets; and 82 – Procurement.

Version control

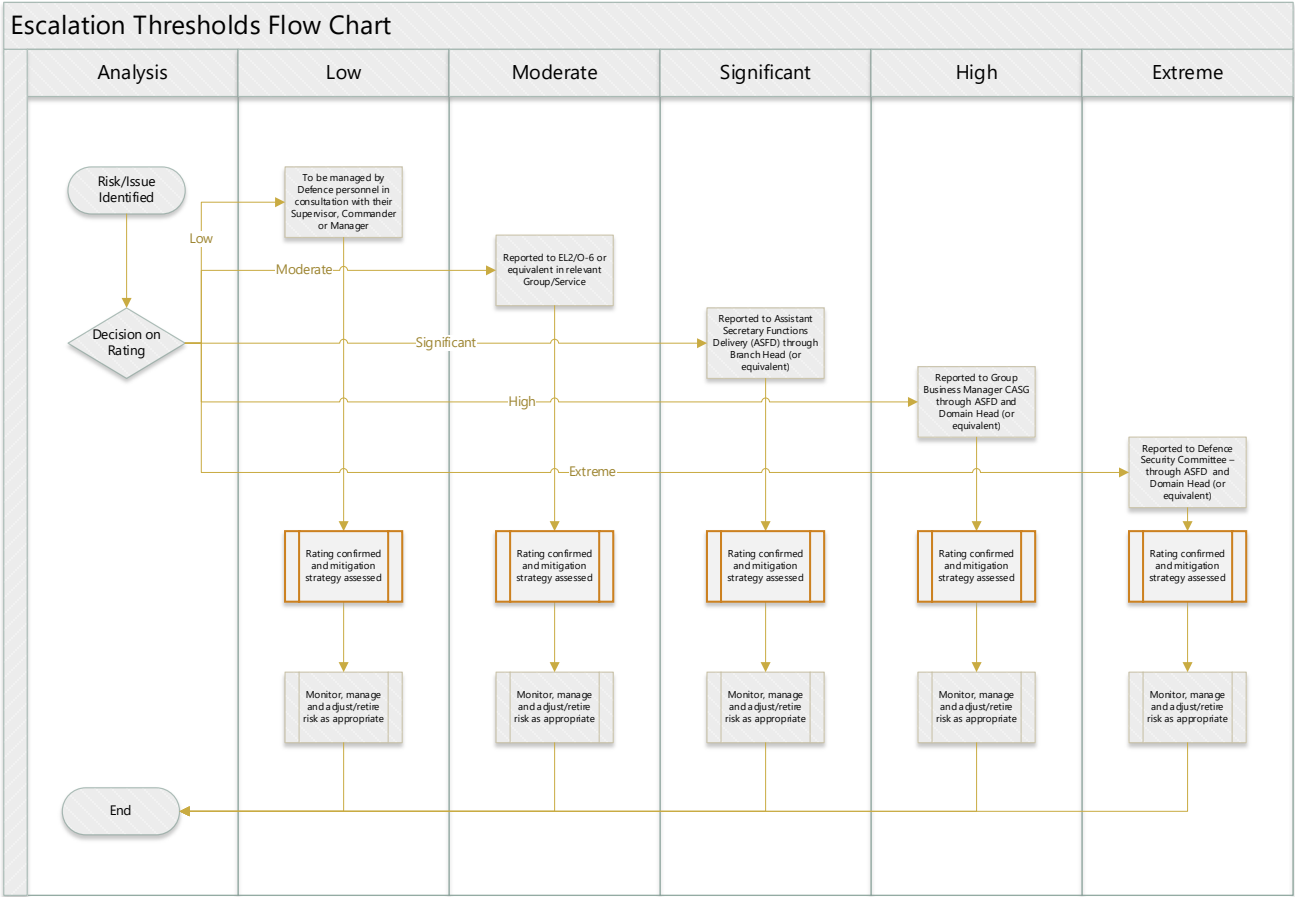
Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS PM	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	1 September 2023	AS FD	Amendments to update with the release of the Capability Program Management Manual, the One Defence Capability System the CASG Control Owner and administrative changes.



Defence Security Principles Framework (DSPF)

Annex A to Security for Projects – Project Risk Escalation Thresholds Flow Chart



Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Project Risk Escalation Thresholds Flow Chart
Annex Version	1
Annex Publication date	01 September 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Security for Projects
DSPF Number	Control 11.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	01 September 2023	AS FD	Launch



Defence Security Principles Framework (DSPF)

Security for Capability Planning

General Principle

1. The security of capabilities acquired, and their ongoing management, is to be considered at all stages of the Capability Life Cycle.

Rationale

2. Failure to consider and forecast security requirements during capability development and throughout the Capability Life Cycle, including assessing the security impacts on all Fundamental Inputs to Capability (FIC), could lead to operational failure, project delays and increased costs.

Expected Outcomes

3. Capabilities are delivered uncompromised in terms of security and are maintained as such throughout their lifecycle.
4. Domain Leads, Program Sponsors, Project Managers and System Program Offices (SPO) apply security controls throughout and project activities and budget for them accordingly.
5. Security guidelines are contained in the Capability Life Cycle.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Investment Portfolio (ASIP)
High	Defence Security Committee (DSC) – through ASIP
Extreme	DSC – through ASIP

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Security for Capability Planning
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 12
Version	2
Publication date	31 June 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	Assistant Secretary Investment Portfolio

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security Planning; Security governance for contracted service providers; and Eligibility and suitability of personnel.
Read in conjunction with	Interim Capability Life Cycle Manual
See also DSPF Principle(s)	Assessing and Protecting Official Information Security for Projects Physical Security Access Control Procurement
Implementation Notes, Resources and Tools	ASIO, Security Equipment Guides (SEGs) are available from theGovDex Protective Security Community

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Communications Security (comsec)

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Principle. To view the full Principle, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Document administration

Identification

DSPF Control	Communications security
Principle Owner	Defence Communications Security Officer (DEFCOMSECO)
DSPF Number	Principle 13
Version	3
Publication date	22 March 2021
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 13.1
Control Owner	Defence Communications Security Officer (DEFCOMSECO)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	Defence CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy.
3	22 March 2021	Defence CISO	Minor updates. Transfer of Principle ownership to DEFCOMSECO



Defence Security Principles Framework (DSPF)

Communications Security (comsec)

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Control has no Appendixes or Attachments.

Document administration

Identification

DSPF Control	Communications Security (Comsec)
Control Owner	Defence Comsec Officer (DEFCOMSECO)
DSPF Number	DSPF Control 13.1
Version	3
Publication date	22 March 2021
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Communications Security

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	Defence ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy.
3	22 March 2021	Defence ITSA	Significant updates. Transfer Control

Version	Date	Author	Description of changes
			ownership to DEFCOMSECO



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Audio-visual Security

General principle

1. Official Information is to be protected from deliberate and accidental compromise through technical means.

Rationale

2. The communication of Official Information is vital for Defence's objectives; however this information can be of great value to unauthorised persons who may undertake technical surveillance to acquire it. It is important for Defence Staff to be aware of these threats and to take appropriate measures to ensure classified communications and the integrity of classified spaces are protected from audio-visual surveillance.

Expected outcomes

3. Defence protects the confidentiality and integrity of its communications from technical surveillance or compromise by adopting necessary measures and controls to maintain the integrity of classified spaces and deny access to unauthorised persons.
4. Defence can communicate Official Information in a manner that does not compromise its operations.

Escalation Thresholds

5. The Assistant Secretary Security Threats and Assurance (ASSTA) has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Security Officer, Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Director Security Intelligence and Threats – through Defence Security and Vetting Service Technical Surveillance Countermeasures Team.
High	ASSTA
Extreme	Defence Security Committee – through ASSTA

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Audio-visual Security
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 14
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 14.1
Control Owner	ASSTA

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Classification of information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems; and Entity resources. ASIO Technical Notes 5/12 & 1/15 <u>Australian Government Information Security Manual (ISM)</u> Legislation: <u>Crimes Act 1914</u>, section 70 and 79 <u>Defence Act 1903</u>, section 73A <u>Criminal Code Act 1995</u>, Division 91 Standards: <u>ISO/IEC 27035:2011 International standard for information security incident management</u> (Due to become ISO/IEC 27035) Australian Communications Security Instruction (ACSI) Suite
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Information Systems (Physical, Personnel and Logical) Security Personnel Security Clearance Temporary Access to Classified Information and Assets Overseas Travel Working Offsite Physical Transfer of Information and Assets

Implementation Notes, Resources and Tools	• ACSI-101(B) – Communication Security (General), section 6: outlines the Australian Signals Directorate's (ASDs) whole-of-government responsibilities as the Australian National COMSEC Authority; • ACSI-53(E) – Communications Security Handbook (Rules and Procedures for the Agency COMSEC Officer and Custodian); • ADFP 6.0.3.1 Communications Security Instructions, noting in particular access requirements in paragraphs 53.44 and 53.46; • DI(G) CIS 6-2-002 – High Assurance Cryptographic Equipment Provision; • PSPF 8 – Sensitive and classified information – provides guidance to assist agencies in identifying the value of information, resulting in the application of a suitable protective marking; • PSPF 15 – Physical security for entity resources; • PSPF 16 – Entity facilities; • PSPF – Information Security – Protectively marking and handling sensitive and security classified information - provides guidance on procedures for applying protective markings and information handling procedures; and • Australian Government Information Security Manual (ISM) – sets out the standard governing the security of Australian Government ICT systems.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Audio-visual Security

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this enterprise-wide control.
2. Assistant Director Technical Surveillance and Countermeasures (TSCM) provides TSCM certification services and audio-visual security advice, through the Director Security Intelligence and Threats, for ASSTA.
3. Defence Security and Vetting Service (DS&VS) is the TSCM authority within Defence.
4. ASSTA is responsible for:
 - a. the provision of advice regarding audio-visual security compliance requirements and technical standards;
 - b. providing advice and services to designate a facility as audio-secure as a part of the accreditation process; and
 - c. ascertaining that the facility is physically suitable for use as an audio-secure room at the level required (refer Annex A of this Control -Construction and Acoustic Testing of Audio Secured Rooms).

Escalation Thresholds

5. ASSTA has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Security Officer, Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Director Security Intelligence and Threats through the DS&VS TSCM
High	ASSTA
Extreme	Defence Security Committee – through ASSTA

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel]

Audio-visual Security

6. Audio-visual security is measures undertaken to secure classified information from compromise by unauthorised persons through surveillance or other technical collection methods. Ensuring that classified information is communicated within appropriately security accredited facilities is the primary measure taken to mitigate audio-visual security risks. Modern, well-concealed, covert surveillance devices (bugs) are unlikely to be detected in the short term, prior to harm being caused. The first line of defence is appropriate protective security.

Key Definitions

7. Audio-security level (ASL) is a designation that describes the level of audio-security certification of a facility. A Certified Audio Secure Room is a room that is rated ASL3 or above and has been certified as audio secure.

8. TSCM is the term to describe methods taken to identify and mitigate potential technical vulnerabilities or a deliberate audio or visual attack. TSCM measures are implemented to reduce the vulnerability of technical compromise of classified discussions.

9. Such countermeasures also apply to covert video interception of proceedings. TSCM certification within Defence is carried out as a part of the security accreditation process and is conducted by appropriately trained TSCM technicians. Training is provided by DS&VS and other Australian government agencies. See 'Arranging a TSCM inspection' below for further information.

Audio Secure Facilities

10. Access to rooms with audio security measures should be strictly controlled. Access should be limited to authorised persons with the appropriate security clearance, briefings and need to know. Refer to the DSPF Principle 72 – *Physical Security* and the DSPF Principle 74 – *Access Control* for more information.

11. Table 1 describes the appropriate audio secure facilities for classified conversations. Audio secure facilities are rated in accordance with a measure of audio privacy.

Table 1: Audio Secure Facilities Appropriate for Classified Conversations

Facility use	Requirement
Regular CLASSIFIED / 'PROTECTED' discussions, or Ad-Hoc (irregular – (no more than once each month) 'SECRET' discussions.	ASL 2
Regular 'SECRET', or Irregular 'TOP SECRET' discussions.	ASL 3
'SECRET' (with amplified speech) (microphone, conference call, etc).	ASL 3 +
'TOP SECRET'	ASL 4 or above
'TOP SECRET', with amplified speech and Sensitive Compartmented Information (SCI).	ASL 5

+ denotes a requirement of an acoustic weighted level difference (Dw) rating increase of 5 points due to speech amplification IAW ASIO Technical Note 1/15.

12. Control Implementers and Control Officers are to consider the relevant risks and obtain advice from the DS&VS TSCM unit or the compartment controller ASL 2 rated rooms may be used at a higher ASL rating after seeking advice from the DS&VS TSCM unit, and will require a risk assessment that is available to the Control Owner.

13. Facilities rated lower than ASL 3 are not normally subject to TSCM testing unless special circumstances are identified through liaison between the Control Implementer and DS&VS TSCM.

14. If meetings or activities to discuss classified information or topics are required in a Defence facility that is not normally maintained for audio-security, advice on security requirements is to be obtained from the DS&VS TSCM. Meetings or activities held at SECRET and above in non-accredited facilities are not to be held without prior approval by the Control Owner (ASSTA), or Australian Signals Directorate Defence Intelligence Security (ASD DIS) if at TOP SECRET. In seeking this approval, Control Implementers should undertake a security risk assessment, considering the mitigations listed in ASIO Technical Note 1/15 para 16.8.

15. If an audio-secure room with a suitable ASL rating is not available, Control Implementers may allow irregular meetings up to the SECRET level in a room if the risks involved are adequately assessed and managed in accordance with the Risk Escalation Thresholds for this Control. Advice from DS&VS TSCM is available to inform this risk assessment. In these circumstances Control Implementers are also to:

- a. ensure that anyone in adjoining areas is cleared and authorised for access to the material to be discussed;
- b. put in place measures to ensure that nobody is allowed to loiter in adjoining corridors;
- c. document the frequency and nature of such arrangements, which may be subsequently used as evidence for creation and certification of an audio-secure room; and
- d. ensure signage is placed on all entry doors and on or near any equipment that is used to generate amplified speech. These signs will indicate that local Standard Operating Procedures (SOPs) apply when using this equipment for conversations including classified information.

Authority to Vary the Audio Standards for Audio-Secure Rooms

16. The Control Owner may approve the variation of the audio secure standards for rooms up to and including the SECRET level following a risk assessment from the Control Implementer.

17. Only the relevant compartment controller may vary requirements for TOP SECRET compartmented material. Any audio-secure room that comes under internationally agreed audio-security requirements is not to be modified without the permission of the compartment controller.

Electronic Equipment within Certified Audio-Secure Rooms

18. Any electronic device that can store or transmit information that is brought into an audio secure room can compromise classified discussions. Devices that are not appropriately classified and/or accredited are not to be taken into audio secure rooms. For information on selecting appropriate ICT equipment and electronic devices, refer to:

- a. DSPF Principle 22 – *Mobility Device Security*;
- b. DSPF Principle 72 – *Physical Security*;
- c. DSPF Principle 73 – *Physical Security Certification and Accreditation*;
- d. DSPF Principle 23 – *ICT Certification and Accreditation*; and
- e. [Information Security Manual](#) (ISM) Controls.

19. Electronic equipment in audio-secure rooms need to be approved as a part of the certification and accreditation process, and advice should be sought on adding any equipment to an existing room.

20. The following describes the electronic requirements that cannot be used:

- a. The area is not to have installed any unaccredited audio or video transmitters, wireless microphones, intercom systems, facsimile equipment, public address systems or cordless telephones; and
- b. Other devices capable of transmitting or recording sound or video (including mobile phones) are not to be brought into the room unless their purpose is to overtly record a meeting. If this is the case, the device(s) are to be declared to the Security Officer, and the device(s) and media are to be classified, registered and labelled according to the maximum classification of the material recorded; refer to DSPF Principle 22 – *Mobility Device Security* for further information.

Exclusion: Accredited Defence laptops identified and classified as *SECRET* or higher may be brought into the room on a temporary basis if they are classified at or above the current activity within the room.

Classified Conversations in Non-Audio Secure Spaces

21. **Off-site** – classified conversations are to be protected from being overheard when conducted off-site, refer DSPF Principle 70 – *Working Offsite* for further information.

22. **Open plan facilities** – open plan offices present an increased security risk as conversations can be overheard by those that are not appropriately cleared or do not have a need to know. Personnel in open plan spaces are:

- a. to consider moving their discussion to an accredited audio secure space;
- b. to ensure that all personnel within hearing range hold an appropriate security clearance and have a genuine need-to-know before discussing classified material. Personnel should also ensure no Portable Electronic Devices (PEDs) or other items that may present a risk to the discussion are in the vicinity; and
- c. not to discuss TOP SECRET material unless the entire open plan facility is a designated Zone Five (refer DSPF Principle 72 – *Physical Security* for descriptions of Physical Security Zones).

Amplified Speech

23. Audio amplification is any electronically distributed content such as video conference, teleconference and speaker phone, amplified for the purpose of sound distribution. Where amplified classified speech is generated the audio is to remain within the physical boundaries of that certified audio-secure room.

24. A risk assessment should be completed prior to installing equipment generating amplified speech in certified audio secure rooms.

25. These systems are not to be installed in any Zone Five unless they have been accredited by the area's Physical and ICT Accreditation Authorities.

Hearing Augmentation in Conferencing Facilities

26. The National Construction Code requires facilities (such as conference rooms, video conference, theatres) in certain circumstances to be fitted with a hearing augmentation system. DS&VS TSCM can provide advice on acceptable listening systems for hearing augmentation where required.

27. The listening system is to be designed so as it can be physically isolated from the main audio-visual system until it is required. The transmission signal of the hearing augmentation system is to be contained within the audio-secure facility.

Operational Deployments, Trials and Exercises

28. Long-term operational deployments are to be treated in the same manner as a fixed secure-facility in Australia, if possible. If deemed not possible, a security risk assessment should be undertaken in accordance with the Risk Escalation Threshold of this Control. Control Implementers should seek the advice from the DS&VS TSCM when setting up audio-secure facilities while on operations.

29. In the case of short-term operational deployments, trials and exercises, Control Implementers can determine the need for audio-security, particularly where other measures have been taken to ensure security of the facility or area. Control Implementers should undertake a security risk assessment, taking into consideration the history and location of a fixed facility and the possibility of audio-security compromise. Advice on mitigating these risks can be sought from DS&VS TSCM and records should be made available to the Control Owner. These requirements only apply to 'SECRET' and below spaces. For 'TOP SECRET' spaces refer to ASD DIS.

ADF Platforms

30. TSCM inspections and testing on Australian Defence Force platforms are conducted on a needs basis with consultation from DS&VS and ASD DIS. As a Control Implementer, if the Unit Commander has a concern with or requires advice on audio-security, the DS&VS TSCM can be contacted directly or through the Service Security Adviser.

Arranging a TSCM Inspection

31. TSCM tests are conducted to determine whether unauthorised devices have been placed in an accredited audio secure facility. TSCM tests are not a guarantee of long-term audio integrity, which can only be assured by the appropriate use of protective security measures and access controls.

32. TSCM tests are to be conducted periodically in audio-secure facilities, and before conferences and meetings in other facilities, if deemed necessary after a security risk assessment and consultation with DS&VS TSCM.

33. The Control Implementer responsible for the security of a certified audio-secured room is to arrange TSCM services:

- a. for periods not exceeding five years, or in accordance with advice from DS&VS TSCM;
- b. following any actual or suspected compromise of an audio-secure room;
- c. following any works, alterations, furniture and appliance changes or other activity which may have introduced a security risk to an audio-secure room; or
- d. when the Control Owner considers that TSCM testing is warranted.

34. To request TSCM services please contact via the Defence Secret Network – DSVSTSCM@dsn.mil.au. Knowledge of a forthcoming TSCM inspection should be restricted to staff with a need to know. A TSCM inspection can provide a high level of assurance about an area's technical security and assists in lessening the risks, but it does not guarantee that the area is free from the risk of technical compromise. If an intended TSCM inspection is well known, covert surveillance devices may be removed.

Actions on Finding a Suspected Intelligence Collection Device

35. The discovery of a suspected intelligence collection device is a major security incident and the following actions are to be completed:

- a. cease all classified discussions;
- b. do not touch, move, or test the object; and
- c. immediately:
 - (1) report it to the relevant Control Implementer and/or Unit Security Officer;
 - (2) secure the facility, if practical, so the suspect device cannot be removed; and
 - (3) report the discovery to the DS&VS Security Incident Centre (SIC) as a MAJOR Security Incident. (refer DSPF Principle 77 – *Security Incidents and Investigations*, and consider the classification of the incident report. Guidance on submitting a Security Incident Report at SECRET and above can be found here).

Further Definitions

36. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Constructing Audio-Secure Rooms*.

Document administration

Identification

DSPF Control	Audio-visual Security
Control Owner	ASSTA
DSPF Number	Control 14.1
Version	3
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Audio-visual Security
Related DSPF Control(s)	Assessing and Protecting Official Information Information Systems (Physical, Personnel and Logical) Security Personnel Security Clearance Temporary Access to Classified Information and Assets Overseas Travel Working Offsite Physical Transfer of Information and Assets

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ASSTA	Launch
2	27 September 2018	ASSTA	Removed the ASL requirement for UNCLASSIFIED discussions in Table 1
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Audio-visual Security – Construction and Acoustic Testing of Audio Secured Rooms

Construction of Audio Secured Rooms

1. Audio-secured rooms are constructed to:
 - a. minimise or prevent unauthorised access;
 - b. provide evidence of any attempted or actual physical penetration or audio attack;
 - c. minimise the number of places where devices could be located; and
 - d. facilitate audio Technical Surveillance Countermeasures (TSCM) testing.
2. The services of an accredited acoustics engineer are to be sought for design advice and build consultation. On completion of the works, the acoustics engineer provides a formal weighted level difference (Dw) certification.
3. A TSCM certification **must** be conducted at the end of construction as a contribution to the audio-security rating of the room, consult the Defence Security and Vetting Service (DS&VS) for further advice.

Additional Considerations

4. The construction standards shown below are designed for a room in isolation, however, the following considerations may apply:
 - a. if a room is located within a secure area that is rated at an equal or higher level, some of the construction and acoustic requirements may be reduced depending on the surrounding environment;
 - b. if the risk of accidental compromise, such as overhearing, is high, the audio attenuation may need to be increased to a level above the minimum standard for that room; and
 - c. for areas located within heritage listed buildings, careful consideration and alternatives will be required to maintain audio and physical security while complying with the construction standard constraints.

5. Advice is to be obtained from the Group or Service Security Authority and DS&VS TSCM on a case-by-case basis.

Audio-Secure Level 4 Rooms

6. Table 1 outlines the minimum requirements for the construction of an audio-secure level (ASL) 4 room. This is to be read in conjunction with the Australian Security and Intelligence Organisation (ASIO) Tech Notes ATN1-15 & ATN5-12 Physical Security of Zones & Physical Security of Zone 5 (Top Secret) Areas.

Table 1: Minimum Requirements for the Construction of an ASL 4 Room

Component	Requirements
Room location	The room shall be an internal room with corridors on all outside walls so there are no adjoining rooms. Corridors are to have controlled access, particularly when the room is in use. It is best practice to: a. locate the room on the upper or basement level to minimise access above and below the room; and b. control access to rooms and corridors above and below the protected area.
Dw rating	The acoustic attenuation weighted level difference (Dw) rating of the room shall be: a. Dw 45, including above any false ceiling and around doors and windows; and b. tested on-site by Certified Acoustic Testing Engineers to AS/NZS 717.1:2004 standards.
Construction materials	Construction and lining materials for all six sides shall be selected from suitable material to meet the Dw rating.
Walls and ceilings	Walls are to be of slab-to-slab construction. Walls and ceilings shall be of tamper evident construction. Do not use relocatable partitioning or wallpaper. DS&VS recommends a surface finish of a light coloured, gloss paint.
Doors	Doors are to be: a. constructed with a block board core; b. fitted with Security Construction Equipment Committee (SCEC)-approved mortice locks; and c. able to be secured from the inside. To achieve the Dw rating, doors may require: a. fitting with acoustic drops; b. soundproof lining on the doorjamb; and c. covers on internal keyholes. The use of an airlock is recommended where possible and where double doors are required it is usually the most practical way to achieve the Dw rating.

Component	Requirements
Windows	DS&VS recommends that windows or glass panels are not used in audio-secure rooms. If windows are used: a. external windows are to be double glazed; b. fit scrim curtains to prevent over viewing; and c. keep windows locked.
Other features	DS&VS recommends a security alarm system for times when the room is unoccupied; If public address speakers are required for emergency evacuation: a. fit each speaker with isolation amplifiers; or b. replace speakers with lights and buzzers in piezo alarms. Treat air-conditioning or service ducts with acoustic baffles and lining.

Audio-Secure Level 3 Rooms

7. Table 2 outlines the minimum requirements for the construction of an ASL 3 room. This is to be read in conjunction with ASIO Tech Note ATN1-15 Physical Security of Zones.

Table 2: Minimum Requirements for the Construction of an ASL 3 Room

Component	Requirements
Room location	If the Dw rating is achieved, speech privacy rooms may share common walls with other rooms. DS&VS recommends that speech privacy rooms do not adjoin public areas or waiting rooms.
Noise Isolation Class (NIC) rating	The acoustic attenuation Dw rating of the room shall be: a. Dw 40, including above any false ceiling and around doors and windows; and b. tested on site by Certified Acoustic Testing Engineers to AS/NZS 717.1:2004 standards. If a public address system will be used, the Dw rating may require upgrading.
Construction materials	Construction and lining materials for all six sides shall be selected from material to meet the NIC rating.
Doors	Doors are to be: a. constructed with a block board core; b. fitted with SCEC-approved mortice locks; and c. able to be secured from the inside. To achieve the Dw rating doors may require: a. fitting with acoustic drops; b. soundproof lining on the doorjamb; and c. covers on internal keyholes.

Component	Requirements
Walls and ceilings	DS&VS recommends that walls be of slab-to-slab construction. If this is not possible, either: - prevent access by: - a fixing 3 mm thick, 12 mm x 19 mm opening size Expanded Metal Mesh in the false ceiling between the top of the perimeter wall partitioning and the ceiling slab; - welding the mesh to 38 mm x 38mm steel angle fixed to the underside of the ceiling slab with Loxins or similar and screw-fixed to the top of the wall partitioning; and - welding the mesh panels to each other to form a single unit; or - maintain controlled access to the ceiling space with alarms and locks on access panels. Outside walls are to be kept free of plant growth for at least 500 mm to allow the walls to be inspected. If wall partitioning finishes at a drop or false ceiling, install a 50 mm sound attenuation blanket extending 600 mm on each side of the partition.
Other components	Treat air-conditioning or service ducts with acoustic baffles and lining. Lock windows.

Acoustic Testing of Audio Secure Rooms

8. Acoustic testing is carried out by an appropriately qualified Audio Engineer on a room or area to establish audio attenuation and to identify any points of weakness. The testing is also conducted to determine whether a facility has met the required benchmarks for the level classified discussions that will take place within the confines of the area

9. Rooms intended for sensitive activity usage are tested to specific audio standards to minimise:

- the risk of accidental audio compromise where intelligible speech can be heard from the room by someone in an adjacent space or transiting past; and
- the risk of a deliberate technical attack utilising audio leakage where covert access into the controlled space is not easily possible.

Requirements

10. The average sound pressure level should be achieved by the following:

- the use of the enlarged frequency range as per AS/NZS 717.1:2004;
- using a single microphone moved from position to position, or by an array of fixed microphones, as per AS/NZS 717.1:2004 and ISO 140-4 and not by a continuously moving or oscillating microphone;

- c. the position of the microphone locations should be such that they cover the weakest points in the area/room (such as doors, windows, and penetrations). The purpose of this test is to ascertain whether any sound is flanking around a building element rather than through the building element material;
- d. the test report should contain the average results and point/position measurement data including the results of any weak points identified;
- e. the test report should also include a diagram of the test area indicating test points used and weak point identified; and
- f. the average result is to meet the appropriate audio level for the designated audio-secured room type.

11. Point/position measurements should meet the appropriate audio level for the designated audio-secured room type. If a point/position measurement failure occurs the result may or may not require rectification depending on a risk assessment undertaken by DS&VS TSCM, as the certifying authority. DS&VS TSCM will consider variation approaches provided that, in its opinion, the overall outcome remains within acceptable risk tolerance.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Construction and Acoustic Testing of Audio Secured Rooms
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Audio-visual Security
DSPF Number	Control 14.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ASSTA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Foreign Release of Official Information

General principle

1. The release of Official Information to foreign services, organisations, or nationals must balance the benefits of sharing information against the likelihood and consequences of security harm.

Rationale

2. The release of Official Information to foreign governments, foreign organisations and foreign nationals is a key operational requirement for the pursuit of Defence objectives.

Expected outcomes

3. Appropriate consideration of the risk/benefit for the release of Official Information.
4. Sharing of information in accordance with agreed safeguards and controls.
5. Formal risk assessments are undertaken for foreign release requests outside of the scope of Defence-specific Security of Information Agreements and Arrangements (SIA)/ Whole-of-Government Security of Information Agreements and Arrangements (GSA).

Escalation Thresholds

6. Foreign Release of Official Information marked with a Dissemination Limiting Marker and/or an Information Management Marker:

Risk Rating	Responsibility
Low	EL1/O5 or equivalent in relevant Group/Service
Moderate	EL1/O5 or equivalent in relevant Group/Service
Significant	EL2/O6 or equivalent in relevant Group/Service
High	EL2/O6 or equivalent in relevant Group/Service
Extreme	EL2/O6 or equivalent in relevant Group/Service

7. Foreign Release of classified Official Information under a GSA/SIA:

Risk Rating	Responsibility
Low	EL2/O6 or equivalent in relevant Group/Service
Moderate	EL2/O6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Policy and Services (AS SPS)
High	AS SPS
Extreme	First Assistant Secretary Security & Vetting Service (FAS S&VS)

8. Foreign Release of classified Official Information outside of a GSA/SIA:

Risk Rating	Responsibility
Low	AS SPS
Moderate	AS SPS
Significant	AS SPS
High	FAS S&VS
Extreme	FAS S&VS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Foreign Release of Official Information
Principle Owner	First Assistant Secretary Security & Vetting Service (FAS S&VS)
DSPF Number	Principle 15
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 15.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Legislation	Criminal Code Act 1995
Government Compliance	PSPF Core Requirements : Security governance for contracted service providers; Security governance for international sharing; Eligibility and suitability of personnel; Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. ISM Control Principles
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information
Implementation Notes, Resources and Tools	Protective Security Policy Framework 8 – Sensitive and Classified Information General Security Agreements (GSA)/Security of Information Agreements/Arrangements (SIA) for the reciprocal protection of official information

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	23 November 2018	FAS S&VS	Correct Escalation Table, paragraph 6; correct Control Owner position title; add additional related information.
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Foreign Release of Official Information

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The escalation thresholds outlined below apply in circumstances where a stakeholder cannot follow, or deviates from, the mandated process in this Control.

	Responsibility	
Risk Rating	Classified Information being shared under a Security of Information Agreement or Arrangement (SIA)/ General Security Agreement (GSA)	Classified Information being shared outside of an SIA/GSA
Low	EL1/O5 or equivalent in relevant Group/Service	Director Strategic and International Security Policy
Moderate	EL2/O6 or equivalent in relevant Group/Service	AS SPS
Significant	Assistant Secretary Security Policy and Services (AS SPS)	AS SPS
High	AS SPS	FAS DS
Extreme	First Assistant Secretary Defence Security (FAS DS)	FAS DS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel. Delegations and decision making authorities are position based (eg. FAS DS).

Introduction

3. This DSPF Control provides guidance on releasing Official Information to Foreign Entities in a manner that balances the benefits of sharing information against the likelihood and consequences of harm.
 - a. All information received, developed or collected by, or on behalf of, the Australian Government by Defence personnel and persons engaged under a contract in their professional capacity is considered “Official”.
4. The foreign release process ensures Defence meets its legal and policy obligations when sharing Official Information with Foreign Entities. This process applies both when Foreign Entities are overseas or in Australia.
5. Additional guidance on the foreign release process, and visual tools, can be found in the Annexes of this DSPF Control.

Security of Information Agreements/Arrangements and General Security Agreements

6. The Australian Government can enter into a Defence-specific Security of Information Agreement or Arrangement (SIA) or a Whole-of-Government General Security Agreement (GSA) with another Foreign Entity that specifies the conditions under which Official Information can be exchanged.
7. These instruments establish protective standards and security classification equivalencies. Where an SIA/GSA is in place it makes the process of exchanging sensitive and security classified information easier, as both parties have agreed to safeguard each other’s sensitive and security classified information to a standard that is no less stringent than that of the releasing party.
8. The existence of an SIA/GSA does not automatically allow the release of sensitive or security classified information, but provides a measure of assurance from a foreign government that Official Information released to Foreign Entities will be appropriately protected.
 - a. A list of Defence’s and Australia’s SIAs/GSAs is available [here](#). If you are unsure if an SIA/GSA exists for a particular country, please contact Defence Security Division via DSVSDSP.International@defence.gov.au.
 - b. An SIA/GSA may only be used for the actions or activities outlined in the relevant agreement or arrangement. For example, if the SIA/GSA only covers

the exchange of Defence-originated information, it cannot be used by non-Defence organisations.

- c. An SIA/GSA may only be used to share sensitive or security classified information between the parties identified by the SIA/GSA itself. For example:
- (1) the AUS-NATO SIA is only applicable in instances where information is being released in support of NATO. As a result, the AUS-NATO SIA cannot be used to share AUS information directly with a NATO member state. This would require a specific bilateral SIA/GSA with that member state.

Principles of Foreign Release

9. The release of Official Information is built on five elements:
- (1) whether or not an SIA/GSA exists;
 - (2) the recipient having a need-to-know;
 - (3) written approval from the Originator (for OFFICIAL: Sensitive information or classified information);
 - (4) if necessary, the recipient having a recognised security clearance when information is released under an SIA/GSA; and
 - (5) if necessary, approval from a Foreign Release Authority.

Treatment of Official Information by marking

OFFICIAL information

10. Information with the protective marking OFFICIAL may be released to Foreign Entities on a need-to-know basis and does not require approval by a Foreign Release Authority.
11. OFFICIAL: Sensitive information shared under an SIA/GSA may be released to Foreign Entities on a need-to-know basis, providing Originator approval is granted. Release of OFFICIAL: Sensitive information shared under an SIA/GSA does not require approval by a Foreign Release Authority.
12. A Foreign Release Authority **must** approve the release of OFFICIAL: Sensitive information outside of an SIA/GSA.

Security Classified Information

13. All security classified information with the security classification PROTECTED or above may be released to Foreign Entities on a need-to-know basis, providing Originator approval is granted. This release **must** be approved by a Foreign Release Authority.

***Note:** Refer to **Table 1: Foreign Release Authority** to determine the minimum level of Foreign Release Authority approval required. The level of approval required will depend on the security classification of the information and whether an SIA/GSA is extant. At their discretion, Groups and Services may escalate responsibility to a level higher than outlined in the table.*

Foreign Release Authority

14. A Foreign Release Authority **must** be an APS or ADF official at the specified level/rank in the Requester's chain of command, who can make an informed decision about whether to approve or deny a foreign release request.

a. The Foreign Release Authority may choose to escalate this authority to a higher level/rank within their chain.

15. Defence Security Division acts as the final Foreign Release Authority for the foreign release of classified information outside of an SIA/GSA. If the Requestor's Foreign Release Authority approves a release, the request should then be sent to DSVSDSP.International@defence.gov.au with a lead time of 15-20 business days for processing and final approval.

Table 1: Minimum Foreign Release Authority

Protective Marking	Official Information being shared <u>under</u> an SIA/GSA	Official Information being shared <u>outside</u> of an SIA/GSA
OFFICIAL	This information can be shared on a need-to-know basis No Foreign Release Approval required	This information can be shared on a need-to-know basis No Foreign Release Approval required
OFFICIAL: Sensitive	This information can be shared on a need-to-know basis, <u>if</u> Originator approval is granted No Foreign Release Approval required	EL1/O5 or equivalent in relevant Group/Service
PROTECTED	EL1/O5 or equivalent in relevant Group/Service	Initial Approval: EL2/O6 or equivalent in relevant Group/Service Final Approval: Director Strategic & International Security Policy
SECRET	EL2/O6 or equivalent in relevant Group/Service	Initial Approval: SES Band 1/One Star or equivalent in relevant Group/Service
TOP SECRET		Final Approval: Assistant Secretary Security Policy & Services

Note: When determining the Foreign Release Authority for large compilations of Official Information or allowing access for extended periods of time, consideration is to be given to the aggregate classification in accordance with **DSPF Control 10.1 – Assessing and Protecting Official Information**.

Foreign Release Process

16. Where a legitimate business need has been identified to share Official Information with a Foreign Entity, the Requester is to follow the following foreign release process.

17. The Requester **must** complete the following three initial steps:
- a. confirm the recipient receiving Official Information has a genuine need-to-know and, if necessary, holds an appropriate level of security clearance;
 - b. obtain written advice from the Originator approving the foreign release of the information;
 - (1) The Australian Department of Defence and Defence portfolio agencies treat Defence-originated information with no releasability caveat as equivalent to REL AUS/CAN/UK/NZL/USA; however, it is recommended Requesters obtain Originator approval for release.
 - (2) Jointly originated information requires written consent from all Originators prior to release.
 - c. determine whether the proposed foreign release is covered by an SIA/GSA.
18. If the release is covered by an SIA/GSA, follow the secondary steps as listed **Annex A**.
19. If the release is not covered by an SIA/GSA – either because it is outside the scope of an existing SIA/GSA or an SIA/GSA does not exist with the proposed Foreign Entity – follow the secondary steps as listed in **Annex B**.
- a. A Risk Assessment **must** be completed as part of a foreign release of classified information outside of an SIA/GSA.
 - b. The recipient of information outside an SIA/GSA **must** also complete a commitment to protect this information.
20. If a Requester is unsure whether the proposed foreign release is covered by an SIA/GSA, they should contact Defence Security Division via DSVSDSP.International@defence.gov.au.

Dissemination of Information after Foreign Release Approval

21. Once approval has been granted by the Foreign Release Authority (and Defence Security Division if necessary), the information may be released in accordance with the approved scope and purpose.
- a. Any additional security provisions imposed on the transmission of information outlined in the relevant SIA/GSA **must** be met.

- b. Where an SIA/GSA does not contain specific transmission requirements for information, or the release is conducted outside of an SIA/GSA, physical transmission of Official Information is to be conducted according to the requirements set out in [DSPF Control 71.1 - Physical Transfer of Information and Assets](#), and electronic transmission of Official Information is to be conducted according to the requirements set out in the *Australian Government Information Security Manual* and [DSPF Control 27.1 – Information Systems Data Transfer Security](#).

Note: The following text should be provided with any Official Information released to a Foreign Entity:

This information remains the property of the Australian Department of Defence. Unauthorised communication and use of this information is a security incident and must be reported to the Australian originator, which may result in the limiting of your future access to Defence information and may be a serious criminal offence. If you have received this information in error, you are requested to contact the sender and delete it immediately.

Security Caveat Markings

23. Security caveats are additional markings applied to Official Information to indicate additional protections in addition to the security classification.
24. Releasability indicators, including 'Australian Eyes Only' ('AUSTEO') and 'Australian Government Access Only' ('AGAO'), are security caveats that permit or limit the release of Official Information to individuals based on citizenship or employment in the Australian Government, respectively. Refer to [DSPF Control 10.1 Assessing and Protecting Official Information](#) for more information.

'Releasable to...' (REL)

25. The REL marking identifies information that has previously been approved for release to citizens of the indicated foreign countries or country grouping.
26. Information marked REL **must** only be released to citizens of the indicated foreign countries. For example, information marked REL AUS/USA cannot be shared with a UK citizen unless the Originator and Foreign Release Authority have provided approval in writing in line with the foreign release process outlined above. Once approval is received, the REL marking may be updated accordingly.
- a. Where information is jointly produced by Australia and a foreign country, approval **must** be received from both countries prior to release to a third party.

27. Prior to release of information with a REL marking, any SIAs/GSAs with the listed foreign countries should be checked to confirm the intended release is within scope.

- a. If there is a current and relevant SIA/GSA with the listed foreign countries, sensitive and security classified information may be released to appropriately cleared citizens or entities of those foreign countries without repeating the foreign release process.
- b. If there is no existing SIA/GSA for the listed foreign countries or the release is outside the scope of the existing SIA/GSA, the process for information outside an SIA/GSA is to be followed as per **Annex B**.

Note: *It is recommended Defence Security Division be engaged when stakeholders anticipate information is to be released outside of a SIA/GSA. Requests for assistance may be sent to DSVSDSP.International@defence.gov.au.*

28. Any security classified information approved for release under an SIA/GSA may have the releasability indicator followed by the appropriate country codes of the originating and receiving foreign countries added to the appropriate classification marking (e.g. SECRET REL AUS/USA). Further information on protective markings can be found in [DSPF Control 10.1 Classification and Protection of Official Information](#) and the [Australian Government security caveat guidelines](#).

- a. REL markings should only to be applied to Australian-originated security classified information marked PROTECTED or above and **must** be stored, processed and transmitted on the DSN.
- b. Foreign Information marked with a nationality-based releasability caveat **must** also be stored on the DSN.
 - (1) [DSPF Control 19.1 Information Systems \(Logical\) Security](#) contains further information about the requirements for the storage, processing and communication of information marked with nationality-based releasability caveats on the DSN.

Foreign national access to a Defence ICT system/network

29. Refer to [DSPF Control 18.1 - Information Systems \(Personnel\) Security](#) for the full application process for foreign national access to Defence ICT systems/networks.

30. Foreign Entity access to Defence ICT systems/networks without an appropriate Foreign Release Approval is a security incident and **must** be reported in

accordance with [DSPF Control 77.1 - Security Incident Management and Investigation](#).

Key Definitions and Acronyms

1. **Foreign Entity.** A Foreign Entity is any organisation formed, registered or existing outside Australia, or an individual without Australian citizenship. This includes, but is not limited to foreign governments, foreign companies, foreign non-government organisations, intergovernmental organisations, as well as foreign nationals whether they are located overseas or in Australia. Any individual not holding Australian citizenship is considered to be a foreign national for the purposes of this Control, including but not limited to contractors and subcontractors working for Australian companies with Defence Industry Security Program membership, and foreign exchange officers.
2. **Foreign Release Authority.** An APS or ADF official at a specified level/rank who holds an appropriate security clearance, and can make an informed decision about whether to approve or deny a foreign release request.
3. **GSA.** General Security Agreement. A treaty-level agreement between the governments of two or more countries, establishing conditions under which Official Information can be exchanged, protective marking standards and security classification equivalencies.
4. **Official Information.** Any information received, developed or collected by, or on behalf of, the Australian Government, by Defence personnel and person's engaged under a contract in their professional capacity. Includes sensitive and classified information, not to be confused with information with the non-security classified marking OFFICIAL.
5. **Originator.** The entity that created the Official Information or on whose behalf the Official Information was created. An Originator can be a military or business unit within Defence, an Australian government department or agency, or a foreign entity.
6. **Requester.** The individual placing the request for Official Information to be released to a Foreign Entity. This includes but is not limited to ADF members, APS personnel, contractors and DISP members.
7. **SIA.** Security of Information Agreement/Arrangement. A treaty-level agreement or less-than-treaty-level arrangement between governments or government departments, establishing conditions under which Official Information can be exchanged, protective standards and security classification equivalencies.

Further Definitions

8. Further definitions for common PSPF terms can be found in the [Glossary](#).
9. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Annexes and Attachments

Annex A – Foreign Release of Official Information – Under an SIA/GSA.

Annex B – Foreign Release of Official Information – Outside an SIA/GSA.

Document Administration

Identification

DSPF Control	Foreign Release of Official Information
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 15.1
Version	6
Publication date	14 July 2022
Type of Control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Foreign Release of Official Information (Principle 15)
Related DSPF Control(s)	Assessing and Protecting Official Information (Control 10.1) Information Systems (Personnel) Security (18.1) Defence Industry Security Program (16.1) Personnel Security Clearances (40.1) Security Incident Management and Investigation (77.1)
Related legislation	<i>Criminal Code Act 1995 (Cth)</i>

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	23 November 2018	AS SPS	Refine foreign release process for Unclassified DLM/Sensitive level information.
3	24 March 2020	AS SPS	Add note on escalation thresholds and refine foreign release process for REL caveated information. Clarify language and formatting for readability.
4	31 July 2020	AS SPS	Update to include Foreign National ICT Systems and Network access process in accordance with Control 18.1. Protective Marking update to align with PSPF
5	10 August 2020	AS SPS	Update hyperlinks to DSPF
6	14 July 2022	AS SPS	Revision of entire Control



Defence Security Principles Framework (DSPF)

Annex A to DSPF Control 15.1 Foreign Release of Official Information Foreign Release under an SIA/GSA

Foreign Release under an SIA/GSA

1. The following is applicable only when a foreign release is covered by an SIA/GSA.
2. After completing the initial steps found in paragraph 17 of DSPF *Control 15.1 – Foreign Release of Official Information*, the Requester **must**:
 - a. determine and submit the request to the appropriate Foreign Release Authority in their chain of command, including supporting documentation sufficient for an informed decision to be made regarding the foreign release.
 - (1) The supporting documentation should include the following:
 - (a) a statement outlining the scope of the release approval (e.g. is the approval for an individual document? Is all Official information up to a certain classification related to a specific operation/activity?);
 - (b) a statement outlining the purpose of the release (e.g. is it information to support a training activity? Is it information relating to a classified contract?);
 - (c) details about the end recipient (e.g. is the information being released to an individual? Is it being released to a government/organisation?); and
 - (d) written advice from the Originator of the information that supports its release.
2. Once a foreign release request is received, the Foreign Release Authority should consider whether the information provided in the request is sufficient to justify a release and inform the Requester of their decision.

3. Appendix 1 provides a summarised workflow of the release process under an SIA.

Appendix

Appendix 1 - *Workflow for Foreign Release under an SIA/GSA.*

Document administration

Identification

DSPF Annex	Foreign Release under an SIA/GSA
Annex Version	1
Annex Publication date	14 July 2022
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Foreign Release of Official Information
DSPF Number	15.1

Version control

Note: A new row is added for each version to show the version history of this document.

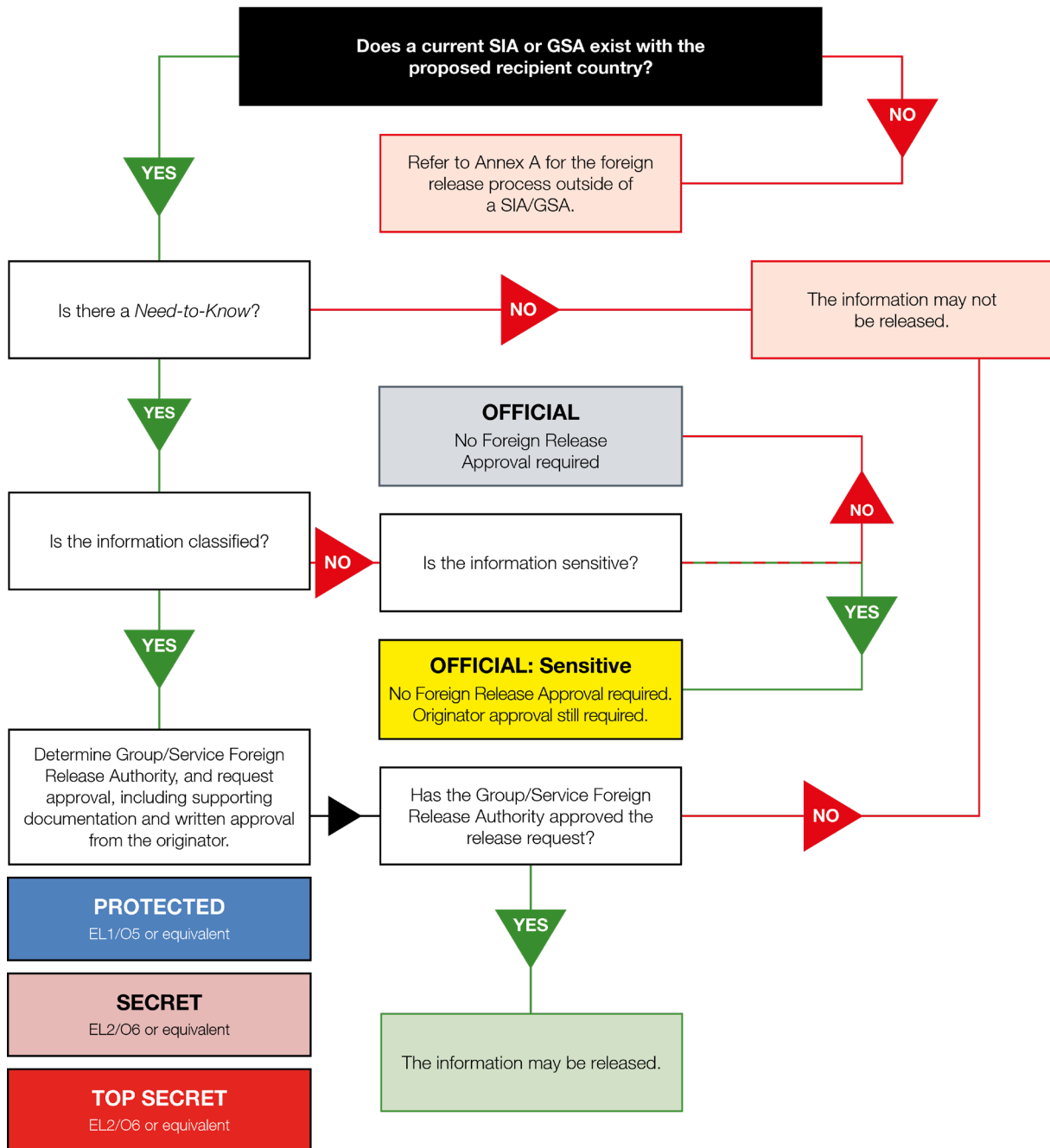
Version	Date	Author	Description of changes
1	14 July 2022	AS SPS	Created as part of the rewrite of Control 15.1 – Foreign Release of Official Information.

Appendix 1

Workflow for Foreign Release under an SIA/GSA.

Foreign Release Process under an SIA/GSA

Use this chart to assess if your information can be released under an SIA/GSA.





Defence Security Principles Framework (DSPF)

Annex B to DSPF Control 15.1 Foreign Release of Official Information Foreign Release outside of an SIA/GSA

Foreign Release outside of an SIA/GSA

1. There may be circumstances where it may not be feasible to conclude a standing SIA/GSA for the one off or ad hoc foreign release of sensitive and classified information.
2. In those circumstances, after completing the initial steps found in paragraph 17 of *Control 15.1 – Foreign Release of Official Information*, the Requester **must**:
 - a. determine and submit the request to the appropriate initial Foreign Release Authority, including supporting documentation sufficient for an informed decision to be made about whether to endorse the foreign release.
 - (1) The supporting documentation should include the following:
 - (a) a statement outlining the scope of the release approval (e.g. is the approval for an individual document? All Official information up to a certain classification related to a specific operation/activity?);
 - (b) a statement outlining the purpose of the release (e.g. is it information to support a training activity? Is it information relating to a classified contract?);
 - (c) details about the end recipient (e.g. Is the information being released to an individual? Is it being released to a government/organisation?);
 - (d) written advice from the Originator of the information supporting its release;
 - (e) a formal risk assessment covering the foreign release of classified information (see paragraph 6); and
 - (f) an outline of any proposed mitigation measures.

- b. If endorsed by the initial Foreign Release Authority, the Requester **must** send the release request to the appropriate final Foreign Release Authority in Defence Security Division by contacting DSVSDSP.International@defence.gov.au, who will make the final decision to approve or deny the request.
 - (1) Defence Security Division may seek further input from the initial Foreign Release Authority and Requester as part of this process.
- 3. If Defence Security Division provide final approval to release information, the Requestor **must** ensure the receiving Foreign Entity provides a written commitment to appropriately protect the shared information.
- a. Defence Security Division have created the *Non-Disclosure Agreement Template* provided in Appendix 2 to this Annex to facilitate this.
 - (1) In circumstances requiring one off or ad hoc foreign release of Official Information outside of an SIA/GSA, the Requester **must** ensure:
 - (a) the receiving official is notified in writing of the requirements for handling Australian information; and
 - (b) these requirements are acknowledged and accepted in writing by the receiving official.
 - (2) In exceptional circumstances, an exchange of emails prior to the provision of classified or sensitive information, or signed acknowledgement of receipt of classified or sensitive information by the receiving official, may suffice. Defence Security Division agreement should be sought in these circumstances.
 - (a) The exchange of emails should incorporate the relevant provisions of the *Template* outlining the protections in place for the information being released.
- b. The release of classified information outside an SIA/GSA without Defence Security Division approval and without a written commitment from the receiving Foreign Entity is a security breach and **must** be reported.
- 4. The releasing area should maintain an internal register of all instances of foreign releases of Official Information outside of an SIA/GSA.

Formal risk assessment

- 5. A formal risk assessment is only required for foreign release of information conducted outside of an SIA/GSA that is marked PROTECTED and above, but may be used to provide additional assurance when conducting a foreign release inside an SIA/GSA.

- a. The assessment could consider questions such as: what is the potential for the information to be compromised by misuse or unauthorised access – intentional or unintentional – or unauthorised modification? If any of these things were to happen, what would the nature of the impact be to Australia's national security, Defence capability, and/or international relations?
6. Defence Security Division does not prescribe how a risk assessment should be developed; however, it is expected that Requesters and their chain of command provide evidence that the risks of sharing information outside of an SIA/GSA have been appropriately considered and addressed as required. Final release approval by the Release Authority will not be granted until a formal risk assessment is complete, in line with the Escalation Threshold.
7. The Security Risk Management page within the Defence Security Division Security Toolkit contains guidance on conducting risk assessments, and a suite of security risk management tools are available [here](#).

Appendix

Appendix 1 – Workflow for the Release of Official Information Outside of an SIA/GSA

Appendix 2 – Non-Disclosure Agreement Template

Document administration

Identification

DSPF Annex	Foreign Release outside a SIA/GSA
Annex Version	1
Annex Publication date	14 July 2022
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Foreign Release of Official Information
DSPF Number	15.1

Version control

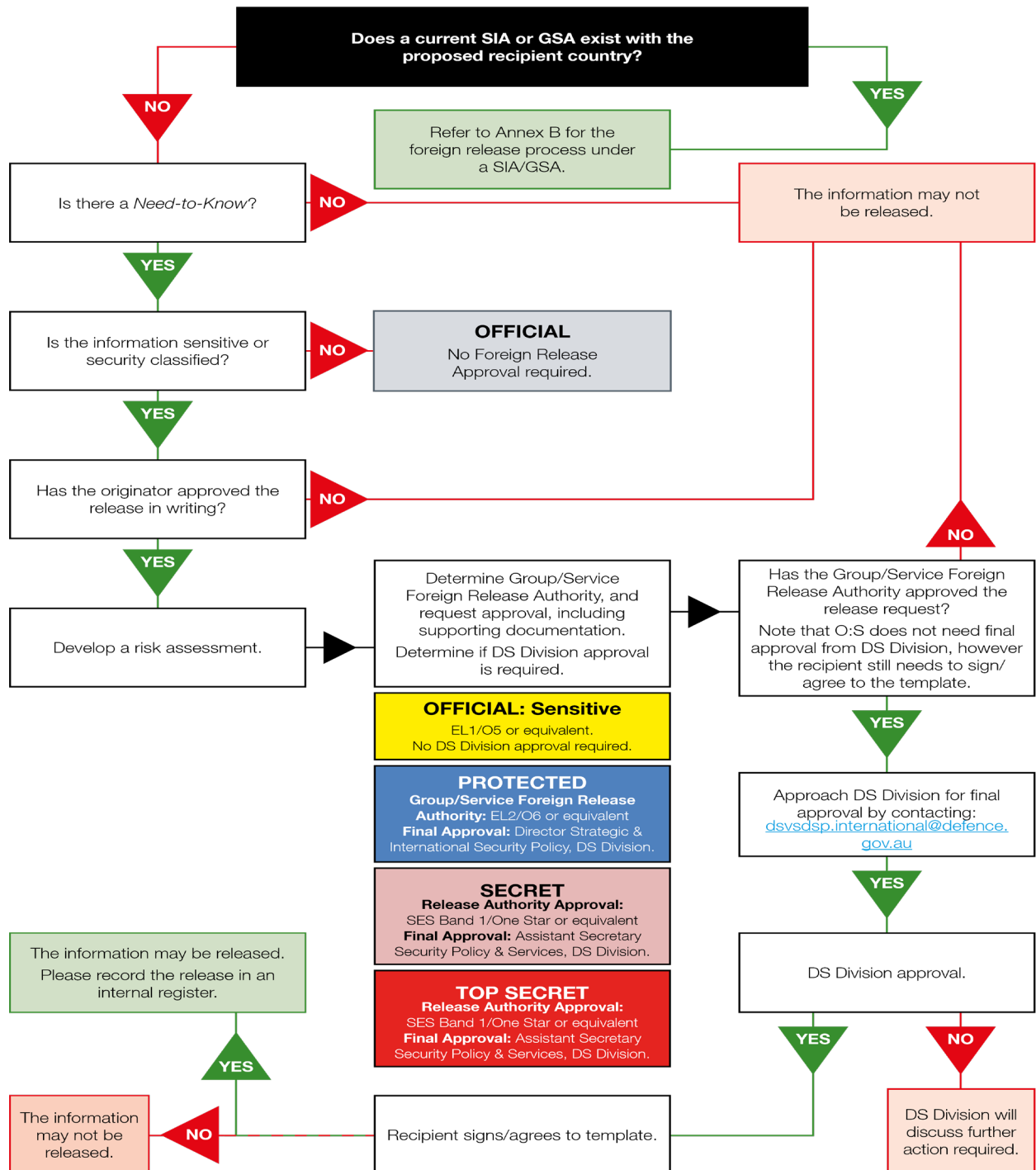
Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	14 July 2022	AS SPS	Created as part of the rewrite of Control 15.1 – Foreign Release of Official Information.

Appendix 1 – Workflow for the Release of Official Information Outside of an SIA/GSA

Foreign Release Process outside an SIA/GSA

Use this chart to assess if you can release your information outside an SIA/GSA.



DS004-02/22

Appendix 2 – Non-Disclosure Agreement Template

Non-Disclosure Agreement

In the absence of a Defence-specific Security of Information Agreement or Arrangement or a Whole-of-Government General Security Agreement between Australia and (Country/Department X), the Australian Department of Defence (ADOD) requests the acceptance of the following provisions to ensure the proper handling of Australian sensitive and/or classified Information.

Recipient:	Name: Country: Official Position: Government Agency: Email: Phone:
Brief Description of the Sensitive and/or Classified Information:	E.g. Australian OFFICIAL: Sensitive instructive materials and ADOD "Defence PROTECTED Network" access.
Permitted Purpose:	E.g. Conduct of a secondment/project to [area] during [period].
Releasing ADOD Point of Contact (POC):	Name: Phone: Email:

Provisions

- (1) The ADOD will provide the sensitive and/or classified Information to the Recipient in accordance with Australian law and Whole-of-Government and departmental foreign release policies.
- (2) After receiving the sensitive and/or classified information, the Recipient will:
 - (a) handle the information in a manner no less stringent than the requirements in Table 1 below;
 - (b) only use the information for the Permitted Purpose, and not change its classification, except with the approval of the ADOD POC;
 - (c) not disclose the information to any individuals who do not have a need-to-know, as well as unspecified third party National or Foreign Entities (including companies, foreign governments, or foreign nationals) without approval of the ADOD POC;

- (d) immediately notify the ADOD POC of any suspected or actual unauthorised or inadvertent disclosure of the information and take all practicable measures to minimise harm resulting from any disclosure;
 - (e) return or destroy the information once no longer needed for the Permitted Purpose, and promptly notify the ADOD POC; and
 - (f) ensure Recipient personnel do not access sites or ICT systems/networks which they have not been granted express permission to access by the ADOD.
- (3) The ADOD will regularly audit the Recipient's use of Australian ICT systems/networks to ensure that any potential inappropriate use is captured. **Delete if no ICT access sought.**

Signature of this letter indicates acceptance of all provisions and handling requirements and a commitment that the Recipient will act in accordance with these provisions. Failure to comply with any of these provisions could constitute a security breach/incident and lead to the termination of the Recipient's access to Australian sensitive and/or classified information, sites and ICT systems/networks. It could also result in Recipient personnel in Australia being returned to their home country.

Signature of Recipient (on behalf of the "Government Agency" listed above): DS Division preference is for an individual who is a manager/supervisor of the recipients of information to sign this. Date:	
Signature of ADOD POC: Date:	

Table 1 – Overview of minimum protection and handling requirements

The below table provides guidance on how the Recipient **must** handle the Sensitive and/or Classified Information.

Australian classification	Protection and handling requirements
OFFICIAL: SENSITIVE	Access: Personnel must have a 'need-to-know'. Storage: Minimum storage requirement in all areas is a lockable

	container. IT: Transmission is through a minimum of an Australian OFFICIAL network or encrypted public networks. The Recipient must also comply with the ADOD sponsoring area's Security Risk Assessment management plan and Standard Operating Procedures.
PROTECTED	Access: Personnel must have a 'need-to-know' and possess an appropriate personnel security clearance. Storage: PROTECTED information must be stored in a secure access controlled area and a safe. PROTECTED information may not be reproduced or stored electronically. The Recipient must also comply with the ADOD sponsoring area's Security Risk Assessment management plan and Standard Operating Procedures.



Defence Security Principles Framework (DSPF)

Defence Industry Security

General Principle

1. A secure and resilient defence industrial base is essential to meeting Australia's strategic objectives and maintaining the Department of Defence's (Defence) capability edge. Security risks associated with the procurement of goods and services need effective management to reduce the likelihood of increased security risk to Defence.

Rationale

2. Failure to consider and mitigate defence industry security risks could lead to compromised capability, operational failure, project delays and increased costs.
3. In addition to DSPF Principle 16, Defence uses DSPF Principles 11 – Security for Projects; 12 – Security for Capability Planning; and 82 – Procurement to support industry to improve their security posture and support industry to ensure Defence capability is underpinned by a strong security culture and secure workforce.
4. Defence also uses whole of government initiatives and frameworks to consider and mitigate security risks.

Expected Outcomes

5. Defence is assured that goods and services are delivered uncompromised. Accountabilities and responsibilities for security risk management are understood and suitable risk reduction activities are applied to effectively manage industry security risks.
6. Australia's defence industry sector is well positioned to be a trusted partner in the global defence supply chain.

Escalation Thresholds

Risk Rating	Responsibility
Low	Assistant Director Capabilities and Partnerships Security Policy
Moderate	Director Capabilities and Partnerships Security Policy
Significant	Assistant Secretary Security Policy and Services
High	First Assistant Secretary Defence Security
Extreme	Defence Security Committee – through Assistant Secretary Security Policy and Services

Note: Defence personnel and persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Defence Industry Security
Principle Owner	First Assistant Secretary Defence Security
DSPF Number	Principle 16
Version	4
Publication date	17 February 2022
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 16.1 – Defence Industry Security Program
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	<u>PSPF Core Requirements</u>: Security governance for contracted service providers. Legislation: Privacy Act 1988 (Cth) Standards: AS: 4811-2006: Employment screening
Read in conjunction with	Principles; 11 - Security for Projects 12 - Security for Capability Planning; and 82 – Procurement
See also DSPF Principle(s)	10 - Classification and Protection of Official Information 15 - Foreign Release of Official Information 17 - Physical, 18 - Personnel and 19 - Logical Information Systems Security 40 - Personnel Security Clearance 41 - Temporary Access 71 - Physical Transfer of Official Information, Security Protected and Classified Assets
Implementation Notes, Resources and Tools	DS&VS Defence Industry Security Program webpage AGSVA Resources

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	9 April 2019	FAS S&VS	DISP Reform Launch
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	17 February 2022	FAS DS	Enhancements to Defence Industry Security Program to improve the uplift of industry security and engagement



Defence Security Principles Framework (DSPF)

Defence Industry Security Program

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this control.

Escalation Thresholds

2. AS SPS has set the following general thresholds for risks managed against this *DSPF Enterprise-wide Control* and the related *DSPF Principle and Expected Outcomes*.

Risk Rating	Responsibility
Low	Assistant Director Strategic and International Security Policy
Moderate	Director Strategic and International Security Policy
Significant	Assistant Secretary Security Policy and Services (AS SPS)
High	First Assistant Secretary Defence Security (FAS DS)
Extreme	Defence Security Committee (Chair) – through AS SPS

Note: Defence personnel and persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

About the Defence Industry Security Program

3. Security is critical to the resilience of Defence systems, information, assets and our people. Defence industry partners ability to meet their security obligations and enhance their resilience is critical to protecting the Government's investment in secure, uncompromised Defence capability.
4. The Defence Industry Security Program (DISP) is one control in a layered approach to security that contributes to strengthening the assurance that the Government's significant investment in Defence capability is appropriately protected. Managed by the Defence Industry Security Office (DISO), the DISP:
 - a. is a membership-based program that sets baseline security requirements for Industry Entities wishing to engage with Defence;
 - b. supports industry to identify security risks and to understand and apply security controls across the domains of governance, personnel security, physical, and information and cyber security;
 - c. includes a system of reviews to ensure continued compliance; and
 - d. enhances Defence's ability to monitor and mitigate security risks.
5. DISP membership is **mandatory** for Industry Entities who:
 - a. require access to classified information or assets (i.e. PROTECTED and above);
 - b. supply, maintain, store or transport weapons or explosive ordnance;
 - c. provide security services for Defence bases or facilities; and/or
 - d. are required to hold DISP membership as a condition of a Defence contract.
6. The exception to this requirement is where:
 - a. an Industry Entity's personnel are handling classified information within Defence facilities and using Defence assets and ICT networks (refer to *DSPF Principle 74 – Access Control*).
 - b. an Industry Entity has accreditation recognised under a Security of Information Agreement or Arrangement (SIA) and Government Security Agreement (GSA) with an international partner (refer to *DSPF Principle 15 – Foreign Release of Information*).

7. Defence Officials undertaking procurement and managing contracts (Contract Managers), **must** stipulate whether DISP membership is a requirement, and specify the level of membership the Industry Entity should hold, in tendering and contracting documentation.

8. The AS SPS, supported by DISO, is the responsible decision maker for determining whether to approve, deny, limit, downgrade, suspend or terminate an Industry Entity's DISP membership.

Membership levels

9. DISP membership is defined by levels across the security domains of: governance, personnel, physical, and information and cyber security.

10. The DISP has four membership levels within each security domain that align with Australian Government security classifications and determine the level of information an Industry Entity is accredited to handle:

	Governance	Personnel Security	Physical Security	Information and Cyber Security
Entry Level	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive
Level 1	PROTECTED	PROTECTED (Baseline)	PROTECTED	PROTECTED
Level 2	SECRET	SECRET (NV1)	SECRET	SECRET
Level 3	TOP SECRET	TOP SECRET (NV2)	TOP SECRET	TOP SECRET

11. Industry Entities can apply for different membership levels across each domain based on their demonstrated business requirements.

12. An Industry Entity's governance membership level **must** be equal to the highest level applied for across the other three domains.

13. On initial application to join the DISP, Industry Entities can only apply for DISP 'Entry Level' membership for the Information and Cyber Security domain, unless they have existing certification and accreditation provided by the Chief Information Officer Group (ICT Security Branch (ICTSB)) or an explicit requirement to fulfil a current

Defence contract. Higher Information and Cyber Security levels may be applied for through ICTSB once DISP membership has been granted. Industry Entities who need to apply for Level 1 or higher will need to seek accreditation and certification under DSPF Principle 23.1 – ICT Certification and Accreditation.

14. Industry Entities without a Defence contract, who are seeking to position themselves to enter the defence supply chain, should apply for Entry Level membership across all domains. Industry Entities applying for Levels 1, 2 and 3 membership **must** provide an appropriate justification to support higher levels of membership (such as working on highly classified programs/projects).

DISP membership

15. DISP membership is open to any Australian business looking to become a part of the defence industry supply chain. You do not require a contract with Defence to become a member of DISP;

16. DISP membership is not automatic. On receipt of an Industry Entity's completed application, Defence will conduct an assessment of the Industry Entity's eligibility and suitability for DISP membership.

Eligibility considerations

17. To be eligible for DISP membership, the Industry Entity, **must** as a minimum:

- a. be registered as a legal business entity in Australia (i.e. has an ABN or ACN);
- b. be financially solvent (not under administration or receivership);
- c. have a director or senior executive able to obtain an Australian Personnel Security Clearance (at a minimum Baseline level) and fulfil the role of Chief Security Officer (CSO);
- d. have a staff member able to obtain an Australian Personnel Security Clearance (commensurate with the level of membership) and fulfil the role of Security Officer (SO) (the CSO and SO can be the same individual);
- e. establish, and be able to maintain, the security standards for their requested level of membership (refer to *Annex A*);

18. Defence will also consider the following when assessing an Industry Entity's eligibility:

- a. any risks arising from an Industry Entity's previous or current commercial activities with any listed terrorist organisation or entity linked to any listed terrorist organisations (as listed under the Criminal Code Act 1995 (Cth)), or to persons for mercenary, terrorist or other criminal activity);
- b. any relationships with regimes subject to Australian sanctions laws including the United Nations Security Council sanctions regimes and Australian autonomous sanctions regimes; and
- c. any relationship with persons and/or entities on the Department of Foreign Affairs and Trade Consolidated List.

19. An Industry Entity that meets the eligibility requirements can apply for DISP membership by submitting the following completed forms to _

DISP.info@defence.gov.au:

- a. *Defence Industry Security Program Application* (AE250) form; and
- b. *Foreign Ownership, Control and Influence* (FOCI) (AE250-1) form.

20. DISO may request additional information and/or documentation from the Industry Entity to confirm eligibility. Where such material is not provided within 75 days, the DISP application will become inactive until further information is received.

21. DISP applicants and members **must** have a centralised point of contact email (not attached to an individual person), that is clearly identifiable and verifiable as belonging to the entity that is applying, an example being "DISP@ company domain name". This account **must** remain current and be monitored on a regular basis. This email address will be the means by which DISO corresponds with Industry Entities in relation to their DISP membership.

22. Applicants without an ABN or ACN are not eligible for DISP membership. However, they may be able to participate in classified contracts if they are recognised under a SIA or GSA with an international partner (refer to *DSPF Principle 15 – Foreign Release of Official Information*).

23. Contract Managers **must** notify DISO when Defence engages (via contract, panel, or partnership) with an Industry Entity requiring DISP membership, when DISP membership is required as a condition of a Foreign Investment Review Board

decision, or when contractual security requirements have changed, through the *Notification of Engagement Requiring DISP Membership* (AE250-2) form.

Suitability considerations

24. On receipt of a completed application, DISO will assess the Industry Entity's suitability for DISP membership. Additional information and/or documentation may be required from the Industry Entity to determine suitability and the level of support the Industry Entity may require to meet DISP requirements.

25. As part of the application assessment process, Defence undertakes the following assessment activities:

- a. personnel security checks of nominated security staff;
- b. an assessment of an Industry Entity's cyber maturity;
- c. an Entry Level Assessment (ELA) to confirm that the Industry Entity has in place appropriate security governance and risk documentation;
 - i. The ELA is designed to confirm an Industry Entity meets the *DISP Membership Level Requirements* as described at *Annex A*. This Annex outlines the requirements for each membership level and security domain.
- d. Security Officer training for nominated security staff;
- e. FOCI checks;
- f. Physical accreditations (depending on membership level);
- g. ICT accreditations by ICTSB (depending on membership level); and
- h. an interview with the SO/CSO to confirm their understanding of their security obligations.

26. Defence may also consider the following when assessing an Industry Entity's application:

- a. any significant risks arising through the Industry Entity's reliance on international supply chains;
- b. any risks arising through an Industry Entity's exposure to criminal and other unlawful activities;

- c. any risks arising from an Industry Entity's previous or current commercial activities with states that have policies or strategic interests inconsistent with those of Australia or our allies;
- d. any other consideration that Defence considers relevant to the Industry Entity's suitability to hold DISP membership.

27. Industry Entities will not be granted DISP membership until they can demonstrate the security standards appropriate to their nominated levels.

28. Where an Industry Entity does not meet the security requirements for the level of membership elected, Defence may require the Industry Entity to enter an uplift program to assist compliance with DISP security obligations.

29. Once an Industry Entity has met the eligibility and suitability requirements, DISP membership will be granted in the form of a DISP Membership Certificate.

Refusing DISP membership

30. An application for DISP membership will be refused if Defence is reasonably satisfied that eligibility and suitability criteria are not met, or if there are concerns that granting membership would not be in Defence's interest or in the national interest.

DISP membership fees

31. There are no DISP membership fees, however, Industry Entities are responsible for covering the costs associated with meeting and maintaining the standards for their level of DISP membership.

Ongoing DISP membership requirements

32. DISP membership is ongoing provided members continue to meet their obligations under the program.

Ongoing security obligations

33. As DISP members, Industry Entities are responsible for safeguarding Defence information, assets, material and systems. DISP members **must**:

- a. comply with contemporary Australian Government and Defence security legislation and policies. This includes achieving and maintaining the standards required by the DSPF, the Protective Security Policy Framework, and the Information Security Manual;

- i. universities and research institutions may also need to comply with Defence Research, Innovation and Collaboration Security (DRICS);
- b. report all security and cyber security incidents in accordance with *DSPF Control 77.1 – Security Incidents* and *DSPF Control 24.1 – Information Systems Security Incident Management*; and
- c. complete an Annual Security Report (ASR).

Ongoing reporting obligations

34. As DISP members, Industry Entities **must** report to DISO all changes that might impact their membership, including (but not limited to):

- a. eligibility changes (including with regard to ownership or control);
- b. other changes in circumstances (such as change of contact details); and
- c. changes to the Industry Entity's CSO and SO.

DISP assurance and uplift program

35. DISO manages an active assurance and uplift program to assist Industry Entities to meet and maintain their security obligations under DISP, including:

- a. ASRs on the anniversary of the Industry Entity's membership grant. The ASR **must** be signed by the CSO and submitted to DISO.
- b. Ongoing Suitability Assessment (OSA) 'desk top' audits to confirm that members are continuing to meet their security obligations. OSA selection is an outcome of an internal risk-based framework.
- c. Deep-Dive Audits (DDA) ascertain the extent of compliance with required policies and procedures, including inspections of documents, as well as identify areas of potential improvements to manage governance, personnel, physical and cyber security risks.

36. A condition of DISP membership is that members **must** engage with uplift and assurance activities conducted by Defence (or a third party nominated by Defence) and provide requested security artefacts to support Defence assurance activities.

37. Industry Entities **must** implement recommendations from DISP uplift and assurance activities within a mutually agreed timeframe. Defence may vary, suspend

or terminate DISP membership if the DISP member fails to implement the recommendations within the agreed timeframe.

Non-compliance

38. Defence is committed to supporting Industry Entities to meet and maintain their obligations as DISP members. Where an Industry Entity fails to meet the requirements of their membership, Defence will employ a scalable approach in responding to the non-compliance.

Escalation pathway

39. Where non-compliance occurs, Defence will seek an informal resolution with the Industry Entity, where appropriate. If an informal approach is unsuccessful, Defence may seek a number of formal remedies, including – but not limited to:

- a. providing formal advice to the Industry Entity to address the non-compliance and prevent future non-compliance (or any precursor activities to non-compliance);
- b. requiring a DISP member to take specific actions (with supporting evidence of implementation);
- c. requiring additional security reporting from the DISP member and imposing additional compliance monitoring activities;
- d. limiting, downgrading, suspending or terminating DISP membership; and
- e. triggering breach of contract clauses where the DISP member is engaged in contracts with Defence.

40. DISO will consult with Contract Managers who hold a contract with the affected Industry Entity before making a determination to limit, downgrade, suspend or terminate DISP membership.

Limiting DISP membership

41. An Industry Entity may be restricted to a specified membership level for governance, personnel, physical, and/or information and cyber security when applying for DISP membership. Defence will work with the DISP member to establish the limits to be applied subject to the nature of the security risk and potential implications of the non-compliance.

Downgrading DISP membership

42. An Industry Entity may have their membership level downgraded across one or more of the membership categories. In such cases, all entitlements, certifications and accreditations at the membership levels held by the DISP member will be revoked.

Suspending DISP membership

43. DISP membership may be suspended following an assurance activity or security investigation which identifies non-compliance or security control breaches. This suspension may affect current contracts and prevent the DISP member from entering into additional contracts with Defence until the issues leading to the suspension are rectified.

Termination of DISP membership

44. If DISP membership is terminated, the Industry Entity will not be able to provide any services to Defence that require DISP membership. This includes storing or transporting Defence weapons or explosive ordnance; providing security services for Defence bases and facilities; any other Defence-related activity requiring secure-handling, or a service that requires DISP membership as a condition of a contract.

45. When DISP membership is suspended, withdrawn or terminated, an Industry Entity will no longer be able to:

- a. hold Defence-sponsored clearances for the CSO and SO;
- b. sponsor new and current security clearances;
- c. receive security information, materials or assets;
- d. continue to hold classified information, assets and materials belonging to Defence (in line with contract terms and conditions and *DSPF Control 10.1 Assessing and Protecting Official Information*);
- e. engage in Defence projects requiring DISP membership;
- f. continue Defence work at the facility where the security risk/breach occurred (where physical or ICT certification and accreditation has been deactivated); and/or
- g. use any DISP membership branding.

Procedure for membership modification by DISP member

46. A DISP member may apply in writing to upgrade or downgrade their DISP membership levels at any time as appropriate for their business requirements, or in order to meet contractual requirements.
47. When seeking to upgrade their DISP membership, Industry Entities will need to undergo an additional suitability assessment. Industry Entities will need to submit an *AE250 form* and include an appropriate justification for an upgrade. Requests for upgrades without an appropriate justification will not be considered.
- a. The suitability assessment may not be required for voluntary downgrading of membership levels where the DISP member can demonstrate compliance with the new level/s.
48. Defence will confirm the change in membership with a revised DISP Membership Certificate and notify relevant Contract Managers.

Voluntary suspension or withdrawal from DISP

49. DISP members can voluntarily suspend or cancel their DISP membership application or membership at any stage by contacting DISO.

Procedural Fairness

50. Procedural fairness applies to a decision to deny, limit, downgrade, suspend or terminate DISP membership. Procedural fairness ensures that a fair and reasonable procedure is followed when making a decision that may adversely affect an Industry Entity's DISP application for membership or current membership. If Defence intends to make a decision which may adversely affect an Industry Entity, the Industry Entity will have a reasonable opportunity to respond in writing before a final decision is made.

Appeals and reviews

51. If an Industry Entity receives notification that their DISP membership application has not been approved or that their DISP membership has been limited, downgraded, suspended or terminated, the Industry Entity can ask for a review of the decision. Defence Security Division will inform the Industry Entity of the relevant avenue(s) of appeal when notifying them of an adverse membership decision.

Roles and responsibilities

Defence

52. In the administration of the DISP, Defence has a responsibility to:
- a. act in good faith;
 - b. act in the national interest;
 - c. provide services to certify and accredit facilities and ICT networks (refer to *DSPF Principle 23 – ICT Certification and Accreditation*, and *Principle 73 – Physical Security Certification and Accreditation*) in support of a DISP membership;
 - d. provide vetting services through The Australian Government Vetting Agency (AGSVA) in support of a specific requirement for a DISP membership; and
 - e. uphold responsibilities under Commonwealth and Defence policy.

Defence Industry Security Office

53. DISO is responsible for the operations and management of DISP, including, but not limited to:
- a. providing information and support to Industry Entities wishing to join the DISP;
 - b. processing DISP membership applications;
 - c. providing ongoing security management advice; and
 - d. undertaking assurance and uplift processes associated with membership obligations and security requirements.
54. DISO will advise Contract Managers who have submitted an AE250-2 form of any changes in DISP member profiles during the life of a contract.
55. DISO will also notify Contract Managers of non-compliance with DISP obligations, including if Industry Entities:
- a. do not provide required information in response to an audit request within a 28 business day period;
 - b. have not met assurance reporting requirements; and/or

- c. have not implemented assurance uplift recommendations within agreed timeframes.

56. Where DISP membership is required by Defence in a tender or contract, DISO will provide Contract Managers with details regarding the DISP member sought for engagement. This includes confirmation of the DISP member's membership status and membership levels. Contract Managers are to consider the information provided to assess whether the DISP member is suitable for engagement (see *Annex B* for contact details).

Contract Managers

57. Contract Managers **must** stipulate whether DISP membership is a requirement, and specify the level of membership the Industry Entity should hold, in tendering and contracting documentation.

58. Contract Managers **must** notify DISO when engaging (via contract, panel, or partnership) with an Industry Entity requiring DISP membership, when DISP membership is required as a condition of a Foreign Investment Review Board decision, or when contractual security requirements have changed (see *AE250-2* form).

59. Contract Managers should notify DISO of any significant updates in relation to current engagements with a DISP member, including incidents of non-compliance with DISP obligations.

Industry Entities

60. Industry Entities applying and participating in DISP are responsible for:

- a. acting in good faith;
- b. ensuring information provided is not deceptive or misleading;
- c. applying the 'need-to-know' principle (including for cleared individuals within the Industry Entity itself);
- d. disclosing, and making available to Defence, all relevant and required information/artefacts as requested;
- e. meeting all security requirements specified by Defence, and any Australian Commonwealth Government Entity (including ensuring no unauthorised

access to official, sensitive and classified information, assets, materials and systems); and

- f. complying with all other obligations applicable to their DISP membership, including but not limited to:
 - i. engaging with assurance activities, such as ELAs, OSAs, and DDAs;
 - ii. providing required information and/or any other requirements to support DISP assurance and uplift activity; and
 - iii. maintaining communication with DISO.

Chief Security Officer

61. An Industry Entity's CSO **must** be able to obtain and maintain a minimum Personnel Security Clearance at the Baseline level, or the highest level of classification that the Industry Entity will have access to, whichever is greater.

62. The CSO is the authority for the Industry Entity's security posture and is responsible for the oversight of security arrangements and championing a positive security culture. They have the flexibility to delegate the day-to-day management of protective security to the SO/s where required (the CSO and SO can be the same person).

63. The CSO **must** be a director or senior executive with the ability to implement policy and direct resources to meet security requirements.

64. The CSO is accountable for ensuring:

- a. all obligations contained in this policy and other supporting documents for the Industry Entity's level of membership are met;
- b. an appropriate system of risk, oversight and management is operated and maintained;
- c. DISP reporting obligations are fulfilled;
- d. official, sensitive and classified materials entrusted to the Industry Entity are protected in accordance with DSPF requirements at all times;
- e. the DISP ASR is completed by the Industry Entity and agreed to by the executive (Board equivalent), all recommendations are implemented within the

agreed timeframes, and the ASR is provided to Defence annually on the anniversary of the membership grant; and

- f. any change in the Industry Entity's circumstances that may impact their ability to maintain DISP membership (including changes in ownership and control) is reported to Defence (refer to *Annex B*).

65. The Industry Entity **must** notify Defence in writing of any changes to the CSO or SO within 14 business days of the change.

Security Officer

66. Industry Entities may appoint multiple SOs in accordance with their operational footprint. All SOs **must** comply with the requirements of DISP membership.

67. An Industry Entity's SOs **must** be able to obtain and maintain a Personnel Security Clearance, commensurate with the level of DISP membership.

68. In order to obtain authority to sponsor and manage Personnel Security Clearances within the Industry Entity, a SO **must** have a minimum Negative Vetting 1 (NV1) Personnel Security Clearance.

69. A SO is required to complete the *Defence Security Officer Training Course* as part of the application process, and every three years thereafter. SOs **must** also undertake any additional required training associated with the SO position. A SO is responsible for:

- a. the development and application of security policies and plans for their Industry Entity;
- b. ensuring sensitive and classified materials entrusted to the Industry Entity are protected in line with DSPF requirements at all times;
- c. maintaining a Designated Security Assessed Position list, which is to be made available to Defence upon request (refer to *Annex A*). (The Protective Security Policy Framework mandates that Industry Entities identify and record positions that require a security clearance and the level of clearance required).
- d. where relevant, sponsoring and managing all Personnel Security Clearances issued under the authority of the Industry Entity's DISP membership in accordance with the *DSPF Control 40.1 – Personnel Security Clearances*.

- i. ensuring and facilitating Defence mandated security education and training courses for Industry Entity personnel engaged in Defence work;
- ii. implementing arrangements and training for insider threat identification, reporting and management;
- iii. reporting security and fraud incidents, and contact reports, in accordance with *Control 77.1 – Security Incidents and Investigations*;
- iv. A SO **must** actively monitor and manage the ongoing suitability of sponsored security cleared personnel including their security attitudes and behaviours;
- v. A SO **must** notify AGSVA when a clearance holder no longer requires their clearance or when they separate from the DISP Industry Entity;
- vi. Personnel Security Clearances requiring an eligibility waiver **must** be approved by Defence. Refer to *DSPF Control 40.1 – Personnel Security Clearances* for exceptional circumstances criteria; and
- vii. Positive Vetting clearances can only be sponsored by the authorities outlined in *DSPF Control 40.1 – Personnel Security Clearances*.

70. Where an Industry Entity or CSO/SO fails to meet these requirements, Defence may vary, suspend or terminate the Industry Entity's DISP membership.

Defence Industry Security Program Privacy Notice

71. Defence undertakes checks to assess an entity's suitability to hold and maintain DISP membership in accordance with Control 16.1 in the *Defence Security Principles Framework* (DSPF). This involves collecting, using and disclosing personal information to Defence capability managers, contract managers, project leads and other Australian Commonwealth departments and agencies.

72. The Defence Industry Security Office (DISO) respects your company's confidential information and the personal information of individuals who are associated with your company. DISO complies with the Australian Privacy Principles (APPs) in Schedule 1 to the *Privacy Act 1988*, which govern the handling of personal information (including sensitive information) for the efficient and effective administration of the DISP. DISO also operates in line with the Department of Defence's APP privacy policy under APP 1.3.

Appropriate use of DISP branding

73. Defence has a range of emblems and logos that are protected by legislation. Permission to use Defence logos and emblems is managed by Defence. Permission from Defence **must** be sought before using all Defence logos and emblems, including DISP branding.

Additional resources

Resource	Description
<u>Criminal Code Act 1995</u> (Commonwealth)	The <i>Criminal Code Act 1995</i> provides an integrated and coherent statement of the major offences against Commonwealth law. The statement of general principles is exhaustive; the principles apply to all Commonwealth offences, whether or not they are included in the <i>Criminal Code</i>
<u>Cybercrime Act 2001</u> (Commonwealth)	The <i>Cybercrime Act 2001</i> updates existing Commonwealth provisions on computer-related crime. The Act outlines main offences relating to computer-related crime, including: • Unauthorised access, modification or impairment to commit a serious offence • Unauthorised modification of data to cause impairment • Unauthorised impairment of electronic communication • Unauthorised access to or modification of restricted data • Unauthorised impairment of data held on a computer disk, credit card or other data storage device • Possession of data with intent to commit a computer offence • Production, supply or obtaining of data with intent to commit a computer offence
<u>National Legislation Amendment (Espionage and Foreign Interference) Act 2018</u> (Commonwealth)	The <i>National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018</i> criminalises covert and deceptive activities of foreign actors that intend to interfere with Australia's institutions of democracy, or support the intelligence activities of a foreign government
<u>Public Service Act 1999</u> (Commonwealth)	The <i>Public Service Act 1999</i> governs the operation of the Australian Public Service, and is supported by subordinate legislation: • <i>Public Service Regulations 1999</i>

	• <i>Public Service Classification Rules 2000</i> • <i>Australian Public Service Commissioner's Directions</i>
Privacy Act 1988 (Commonwealth)	The <i>Privacy Act 1988</i> was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations handle personal information. The Act includes 13 Australian Privacy Principles (Schedule 1), which apply to some private sector organisations as well as most Australian Government agencies
Australian Standard (AS):4811-2022 – Workforce Screening now incorporates Australian Standard International Organisation for Standardisation (AS ISO) 31000:2018 (both available for purchase on the Standards Australia website).	This is the Australian standard for workforce screening. Workforce screening applies to security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources. Requirements under the standard include: • An identity check requiring 100 points of ID • Address history checks for a minimum of five years • Character reference checks • A current national police check • An ASIC check (where relevant) • Checks on all declared experience and qualifications
Protective Security Policy Framework (PSPF)	The PSPF assists Australian Government entities to protect their people, information and assets, both at home and overseas. It sets out government protective security policy and supports entities to effectively implement the policy across the following outcomes: • Security governance • Information security • Personnel security • Physical security

Defence Security Principles Framework (DSPF)	The DSPF is the primary security framework for Defence to manage security risk.
Information Security Manual	A cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats.
Defence Privacy Policy	The Defence Privacy Policy is designed to inform individuals about the way Defence collects, stores, uses and discloses personal information. This policy provides guidance about how you can access, or seek correction of, personal information held by Defence

Definitions

Word	Definition
Australian Government Security Vetting Agency (AGSVA)	AGSVA is the central vetting agency for the Australian Government and conducts security clearance assessments for federal, state and territory agencies.
Chief Security Officer (CSO)	A role occupied by a senior executive in an Industry Entity that is responsible for the oversight of, and responsibility for, security arrangements and championing a positive security culture.
Contract Manager	For the purposes of this policy, Contract Managers are defined as Defence officials responsible for conducting procurement and managing contracts; this could include but is not limited to Program Managers, Project Managers, Senior Project Officers, Project Officers or any other role with contracting responsibilities.
Decision Maker	The Assistant Secretary Security Policy and Services (AS SPS) is the DISP Control Owner and, for the purposes of this policy, AS SPS will normally be the original decision maker for the purpose of determining whether or not to refuse, limit, downgrade, suspend or terminate an affected party's DISP membership.

	In the event AS SPS is conflicted or otherwise unavailable or unable to act as a Decision Maker, the Decision Maker will be the person appointed in writing by AS SPS to act as such.
Defence Industry Security Office (DISO)	DISO is responsible for the processing of DISP membership applications and undertaking the assurance and uplift processes associated with membership obligations and security requirements. DISO is also responsible for the ongoing assurance framework for DISP members, once admitted into the program.
Defence Industry Security Program (DISP)	A vetting and assurance program that supports Defence industry to improve their security posture for the purpose of engaging in Defence projects, contracts and tenders.
Deep-Dive Audit (DDA)	Deep-Dive Audits seek to provide an independent review of whether DISP members are continuing to meet ongoing security requirements commensurate with their level of membership. DISO audits involve interviews with Security, HR and IT staff, reviewing a company's security policies and plans, personnel, information and physical security arrangements and security registers, including physical security inspections.
Designated Security Assessed Positions (DSAP)	A Designated Security Assessed Position (DSAP) is a position that has been assessed by the DISP Industry Entity as requiring access to sensitive or classified information, materials and assets. A DSAP list identifies each position within an Industry Entity that requires a security clearance, the level of clearance required for each of those positions, and details of

	occupants of the positions. Maintaining a list of security assessed positions ensures that access to classified materials is appropriately monitored and managed.
Eligibility	Criteria outlining Industry Entity eligibility to apply for DISP membership, including legal operating status as an Australian business and ability to maintain the security standards for their requested level of membership.
Industry Entity	An Industry Entity (such as a sole trader, partnership, trust, company or university) that is registered as an Australian business and is located within the territory of Australia.
Entry Level Assessment (ELA)	An assurance activity to validate that information provided in the application is supported by evidence, and that the Industry Entity has in place the required security controls commensurate with the level of DISP membership sought.
Foreign Ownership, Control and Influence (FOCI)	Where a foreign interest has direct or indirect power, whether or not exercised, to direct or decide matters affecting the management or operations of the company.
Ongoing Suitability Assessment (OSA)	The OSA is a 'desk top' audit to confirm that members are continuing to meet their security obligations. OSA selection is an outcome of an internal risk-based framework. The OSA aims to increase awareness and enhance security policies, procedures and risk management strategies DISP members have in place. Where opportunities for improvement are identified, recommendations are provided to members to assist in uplifting their security policies and practices, ensuring that Defence and defence industry continues to protect its personnel, information and assets.
Personnel Security Clearance	A series of assessments into an individual's suitability to have ongoing access to security classified resources. The purpose is to determine whether an individual possesses and demonstrates an appropriate level of integrity (a range of character traits) that indicate the individual is able to protect security classified resources. These traits include

	honesty, trustworthiness, maturity, tolerance, resilience and loyalty.
Procedural Fairness	An administrative law principle that ensures a fair and proper procedure is followed when making a decision.
Security Officer	A role occupied by an individual in an Industry Entity with delegated authority from the Chief Security Officer to undertake the day-to-day management of protective security.
Suitability	Criteria outlining an Industry Entity's ability to demonstrate they can meet suitability requirements for DISP membership, outlined in the <i>DISP Suitability</i> section of DSPF Control 16.1.
Uplift and assurance program	A program managed by the DISO to assist DISP members with meeting their ongoing security obligations, including eligibility assessments, cyber assessments, annual self-reporting, ongoing suitability assessments and Deep-Dive Audits.

Annexes

Annex A – Defence Industry Security Program – DISP Membership Level Requirements

Annex B – Defence Industry Security Program – Contacts and Resources

Document administration

Identification

DSPF Control	Defence Industry Security Program
Control Owner	Assistant Secretary Security Policy and Services
DSPF Number	16.1
Version	6
Publication date	1 August 2022
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Defence Industry Security Program
Related DSPF Control(s)	Personnel Security Clearance Temporary Access Assessing and Protecting Official Information Information Systems Security Foreign Release of Official Information Physical Transfer of Information, and Assets Security Incidents and Investigations Procurement

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	9 April 2019	AS SPS	DISP Reform Launch
3	10 April 2019	AS SPS	Update
4	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
5	17 February 2022	AS SPS	Rewritten policy to improve the uplift of industry security and engagement
6	1 August 2022	AS SPS	Update to Escalation Threshold table, DRICS reference, workplace standard, and Entry Level and Level 3 membership requirements
7	30 March 2023	AS SPS	Update Paragraph 21 clarifying email address requirements for DISP members/applicants.

Defence Security Principles Framework (DSPF)

Annex A to Defence Industry Security Program – DISP Membership Level Requirements

Conditions applicable to all Industry Entities

1. All Industry Entities **must**:
 - a. meet and maintain the requirements outlined in Control 16.1 – Defence Industry Security Program (DISP);
 - b. demonstrate they have met, and are able to maintain, the requirements described in this Annex;
 - c. ensure the Security Governance domain matches or exceeds the highest level of membership sought for any other domain; and
 - d. engage with audit and uplift activities conducted by Defence (or a third party nominated by Defence).
2. Defence may refuse, downgrade, limit, suspend or terminate DISP membership if:
 - a. the eligibility and suitability criteria have not been met, or are no longer being met.
 - b. it is determined that granting or continuing an Industry Entity's DISP membership is not in the national or Defence's interest; and/or
 - c. the eligibility and suitability criteria have not been met, or are no longer being met.

Note: The Defence Industry Security Office (DISO) is available to assist Entities to determine their eligibility requirements and cyber security standards.

Membership Level Requirements

Membership Categories	 Security Governance	 Personnel Security	 Physical Security	 Information and Cyber Security
Entry Level 	Entities must: • appoint and retain a Chief Security Officer (CSO) and at least one Security Officer (SO) NB: The CSO and SO can be the same individual • establish and maintain policies and procedures, inclusive of registers and reporting activity/incidents, covering: - security governance arrangements, including designated security positions and their contact details; - risk management, inclusive of security considerations and business security risk assessments; - security training arrangements for all personnel; - security incidents, inclusive of a register covering all security incidents across all security types i.e. personnel, physical, information and cyber incidents; - security reporting arrangements (including security incidents and contact reporting) and register of contacts with foreign persons and entities; - a register of overseas travel with completed travel forms and records of travel briefings provided to security cleared personnel; and - arrangements and training for insider threat identification, reporting and management • engage in all annual DISP assurance activities, including, but not limited to: - annual DISP security reporting; - completing annual security training; and - implementing relevant uplift and assurance programs in accordance with agreed uplift and assurance requirements • notify Defence of changes affecting membership, including changes to: - ownership, board memberships, and financial structures/control; - financial position and financial viability; - international supply chain activities; - exposure to criminal or other unlawful activities; and - any other activity or incident which may influence the Entity's ability to continue working with Defence. The Entity's nominated CSO and SO must: • complete the Defence Security Officer Training Course as part of the application process, and every three years thereafter; and • be able to demonstrate the ability or have relevant experience to manage personnel/facilities and information and cyber security up to and including an 'OFFICIAL/ OFFICIAL: Sensitive' level. The Entity's nominated SO may: • request access to the DISP Security Portal to access security documents, templates, forms and tools relevant to performing their role.	Entities must: • establish and maintain policies and procedures in accordance with the AS4811-2022 Workforce Screening standards including, but not limited to: - workforce screening practices; - ongoing assessment of personnel; and - separating personnel. • establish and maintain a register of Designated Security Assessed Positions (DSAP) of all personnel with security clearances within the Industry Entity, including job role/position and security clearance level. This register must be made available to Defence on request. • report the engagement of foreign nationals and any other disclosures that may be of interest to Defence. • provide Defence a copy of workforce screening and management processes of personnel working with or on Defence-related work. The Entity's nominated CSO and/or SO must: • be Australian citizens and be able to obtain and maintain a minimum Baseline security clearance, in accordance with the Australian Government Security Vetting Agency (AGSVA) policy. The SO cannot sponsor security clearances.	Entities must: • establish and maintain policies and procedures covering details of physical security and access controls at each accredited facility and their location • provide facility ownership and leasing arrangement details to Defence as required.	Entities must: • meet or exceed one of the following information and cyber security standards across all of the Entity's ICT corporate systems used to correspond with Defence, including, but not limited to: - Australian Signals Directorate Essential 8 for ▪ application control ▪ patching applications ▪ restrict administrative privileges; and ▪ patching operating system vulnerabilities - Information security management: ISO/IEC 27001/2:2013 - Protecting Controlled Unclassified Information in Non-Federal Systems and Organisations (US ITAR requirement): NIST SP 800-171 - Cyber security for Defence: Def Stan 5-138) Note: As standards are superseded, the Information and Cyber Security requirements will be updated (e.g. CMMC).

Membership Categories	 Security Governance	 Personnel Security	 Physical Security	 Information and Cyber Security
Level 1 	Entities must: - meet or exceed all security governance requirements in Entry Level - establish and maintain a register of all personnel sponsored for a security clearance by the Entity - complete all annual assurance activities The Entity's nominated SO must: - maintain a NV1 clearance - be able to demonstrate the ability or have relevant experience to manage personnel/facilities and information and cyber security up to and including 'PROTECTED' level.	Entities must: - meet or exceed all personnel security requirements in Entry Level - complete all annual assurance activities The Entity's nominated SO must: - complete assurance activities required to maintain a NV1 security clearance - be able to provide active monitoring and management of the ongoing suitability of sponsored security cleared personnel, including the monitoring of attitudes to security and behaviours in accordance with AGSVA policy. For the purpose of sponsoring personnel security clearances within their Industry Entity commensurate to their membership level, the Entity's nominated SO must be able to obtain and maintain a Negative Vetting level 1 security clearance. The SO is eligible to sponsor security clearances up to and including the Baseline level.	Entities must: - meet or exceed all physical security requirements in Entry Level - ensure at least one facility is certified and accredited in accordance with the DSPF Principle 72 and Control 72.1 Physical Security to receive, handle, store and destroy 'PROTECTED' information and material in accordance with the ISM/DSPF - provide facility ownership and leasing arrangement details to Defence as required.	Entities must: - meet or exceed all information and cyber security requirements in Entry Level - ensure at least one system is certified and accredited in accordance with the DSPF Principle 23 and Control 23.1 ICT Certification and Accreditation to receive, handle, store and destroy 'PROTECTED' information and material in accordance with the ISM/DSPF - maintain the required physical security zoning where system servers are located.

Membership Categories	 Security Governance	 Personnel Security	 Physical Security	 Information and Cyber Security
Level 2 	Entities must: - meet or exceed all security governance requirements in Level 1. Entities are recommended to: - have arrangements agreed between the Entity and sponsoring Commonwealth Government entity for the management of compartment briefs by a Defence Communications Intelligence Security Officer (COMSO). The Entity's nominated SO must: - be able to demonstrate the ability or have relevant experience to manage personnel/facilities and Information and cyber security up to and including 'SECRET' level.	Entities must: meet or exceed all personnel security requirements in Level 1. The SO is eligible to sponsor security clearances up to and including the NV1 level.	Entities must: - meet or exceed all physical security requirements in Level 1 - ensure at least one facility is accredited in accordance with the DSPF Principle 72 and Control 72.1 Physical Security to receive, handle, store and destroy 'SECRET' information and material in accordance with the ISM/DSPF - provide facility ownership and leasing arrangement details to Defence as required.	Entities must: - meet or exceed all information and cyber security requirements in Level 1 - ensure at least one network is accredited in accordance with the DSPF Principle 23 and Control 23.1 ICT Certification and Accreditation to receive, handle, store and destroy 'SECRET' information and material in accordance with the ISM/DSPF - maintain the required physical security zoning where system servers are located.

Membership Categories	 Security Governance	 Personnel Security	 Physical Security	 Information and Cyber Security
Level 3 	Entities must: • meet or exceed all security governance requirements in Level 2 • have documented and agreed endorsement from a Commonwealth Government Senior Executive Service Band 3, or equivalent Australian Defence Force (ADF) position, before: - obtaining a Positive Vetting clearance; and/or - the certification and accreditation of a Secure Compartment Information Facility (SCIF) and/or a 'TOP SECRET' network. • have arrangements agreed between the Entity and sponsoring Commonwealth Government entity for the management of compartment briefs by a Defence Communications Intelligence Security Officer (COMSO) The Entity's nominated SO must: • be able to demonstrate the ability or have relevant experience to manage personnel/facilities, and Information and cyber security up to and including 'TOP SECRET' level	Entities must: • meet or exceed all personnel security requirements in Level 2 The Entity's nominated SO must: • obtain and complete annual assurance activities required to maintain a Negative Vetting 2 (NV2) security clearance • ensure compartment holders adhere to compartment requirements in accordance with the agreed sponsoring Commonwealth Government entity arrangements The SO is eligible to sponsor security clearances up to and including the NV2 level.	Entities must: • meet or exceed all physical security requirements in Level 2 • ensure at least one facility is certified and accredited in accordance with the DSPF Principle 72 and Control 72.1 Physical Security to receive, handle, store and destroy 'TOP SECRET' information and material in accordance with the ISM/DSPF • provide facility ownership and leasing arrangement details to Defence as required.	Entities must: • meet or exceed all information and cyber security requirements in Level 2 • ensure at least one network is certified and accredited in accordance with the DSPF Principle 23 and Control 23.1 ICT Certification and Accreditation to receive, handle, store and destroy 'TOP SECRET' information and material in accordance with the ISM/DSPF • maintain the required physical security zoning where system servers are located

Security Governance	Personnel Security	Physical Security	Information and Cyber Security
DSPF Governance and Executive Guidance	Principle 18 – Information Systems (Personnel) Security	Principle 17 – Information Systems (Physical) Security	Principle 10 – Classification and Protection of Official Information
	Principle 40 – Personnel Security Clearance	Principle 71 – Physical Transfer of Official Information, Security Protected and Classified Assets	Principle 15 – Foreign Release of Official Information
	Principle 41 – Temporary Access to Classified Information and Assets	Principle 72 – Physical Security	Principle 19 – Information Systems (Logical) Security
		Principle 72 – Physical Security Certification and Accreditation	Principle 23 – ICT Certification and Accreditation
		Principle 74 – Access Control	Principle 27 – Information Systems Data Transfer Security
			Principle 28 – Information Systems Log Management

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Identification

DSPF Annex	Defence Industry Security Program – DISP Membership Requirements
Annex Version	5
Annex Publication date	1 August 2022
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Number	Control 16.1

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	9 April 2019	AS SPS	DISP Reform Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	17 February 2022	AS SPS	Replacement of previous Annex A - Privacy Notice
4	4 March 2022	AS SPS	Update to clarify clearance sponsorship eligibility for each DISP level
5	1 August 2022	AS SPS	Update to workplace standard, and Entry Level and Level 3 membership requirements

Defence Security Principles Framework (DSPF)**Annex B to Defence Industry Security Program –
Contacts and Resources****DISP Contacts**

DISP general enquiries	1800 DEFENCE (1800 333 362)
DISP application enquiries and membership changes	DISP.info@defence.gov.au
Security Reporting • Security Incidents • Contact Reporting	security.incidentcentre@defence.gov.au

Resources

DISP website	DISP website
Working Securely with Defence guide	DISP Resources Defence Extranet
Defence Industry Security Program Application (AE250)	DISP Application (AE250)
Foreign Ownership Control and Influence (AE250-1)	FOCI (AE250-1)
Notification of Engagement requiring DISP Membership (AE250-2)	Notification of Engagement Requiring DISP Membership (AE250-2)

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Defence Industry Security Program – Contacts and Resources
Annex Version	3
Annex Publication date	17 February 2022
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Number	Control 16.1

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	9 April 2019	AS SPS	DISP Reform Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	17 February 2022	AS SPS	Replacement of previous Annex B – Suitability Matrix



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Physical) Security

General principle

1. Defence will protect ICT systems and networks with physical security controls that are proportionate to the assessed risks, which are informed by the confidentiality, integrity and availability business impacts applicable to the ICT asset.

Rationale

2. Defence personnel with a need to know and an appropriate level of clearance are able to securely access information from, and communicate with, information systems and electronic communications devices as required.

3. The security of Defence and Defence Industry Information Communications and Technology (ICT) systems is dependent on the physical context in which they operate. The degree of physical access could significantly affect the security risks to a system or network, regardless of geographic location.

Expected outcomes

4. Defence protects Information Communication and Technology (ICT) systems and networks with physical security controls that are proportionate to the assessed risks, which are informed by confidentiality, integrity and availability business impacts applicable to the asset;

5. Physical security controls are integrated with procedural, logical and personnel security controls, which are applied to ICT systems and networks in accordance with the Australian Signals Directorate's (ASD) [*Information Security Manual \(ISM\)*](#); and

6. High Assurance Products and Controlled Cryptographic Items are physically secured in accordance with DSPF Principle 13 – *Communications Security (COMSEC)*, and applicable *Australian Communications Security Instructions (ACSI/s)*.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	Group/Service managed systems
Low	EL1/O5 within the Directorate of Regional ICT Services (DRICTS), ICT Security Branch Integrated Risk Management (IRM) Directorate or Information Technology Security Manager (ITSM)	EL1/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	EL2/O6 within DRICTS, ICT Security Branch IRM Directorate or ITSM	EL2/O6 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor (CSA) Note: In the event that an appointment of a Group or Service CSA has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive (DSE) Note: In the event that an appointment of a Group or Service CSE has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Defence Chief Information Officer (CIO)	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems (Physical) Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 17
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 17.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. <u>Australian Government Information Security Manual</u> Standards: - AS/NZS 2053 – Conduits and fittings for electrical installations - AS/CA S009:2013 Installation requirements for customer cabling (Wiring Rules) - AS 3996-2006 Access covers and grates, where appropriate - AS/NZS 3084:2017 Telecommunications installations – Telecommunications pathways and spaces for commercial buildings
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Security for Projects Communications Security (COMSEC) Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Security Incident Management Information Systems Business Impact Levels and Aggregation Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	<u>Australian Government information security management guidelines – Australian Government security classification system</u> – provides guidance to assist agencies to identify the value of information, and, in turn, apply a suitable protective marking; <u>Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material</u> – provides guidance on procedures for applying protective markings and information handling procedures; <u>Australian Government Information Security Manual</u> – sets the out the standard governing the security of Australian Government ICT systems.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Physical) Security

Control Owner

1. Information Technology Security Advisor (ITSA) is the Control Owner for this policy.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	Group/Service managed systems
Low	EL1/O5 within the Directorate of Regional ICT Services (DRICTS), ICT Security Branch Integrated Risk Management (IRM) Directorate or Information Technology Security Manager (ITSM)	EL1/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	EL2/O6 within DRICTS, ICT Security Branch IRM Directorate or ITSM	EL2/O6 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor (CSA) Note: In the event that an appointment of a Group or Service CSA has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive (DSE) Note: In the event that an appointment of a Group or Service CSE has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Defence Chief Information Officer (CIO)	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

General

2. Facilities that contain fixed networks in Australia and overseas, including Australian Defence Force (ADF) platforms housing classified ICT systems, are to be compliant with:

- a. Defence physical accreditation process in accordance with DSPF Principle 73 – *Security Certification and Accreditation*;
- b. physical security requirements in accordance with DSPF Principle 72 – *Physical Security*; and
- c. PSPF policy and guidance including:
 - (1) [Australian Government physical security management protocol](#);
 - (2) Defence Security Toolkit – ASIO Technical Note 1/15 (Zones 2 -4);
 - (3) Defence Security Toolkit – ASIO Technical Note 5/12 (Zone 5); and
 - (4) Australian Government physical security management guidelines:
 - (i) [Security zones and risk mitigation control measures](#);
 - (ii) [Physical security of ICT equipment, systems and facilities guidelines](#); and
 - (iii) [Business impact levels](#).

3. Deployable ICT systems are to be accredited in accordance with DSPF Principle 23 – *ICT Certification and Accreditation*, including additional physical security requirements relating to the environment where the system will be operated (e.g. considerations to known threats within the Area of Operations).

Exclusion: Due to the differing environments in which deployed systems operate DSPF Principle 72 – *Physical Security* gives Commanders and Managers scope to risk manage some physical security aspects of SECRET and below deployed systems that do not host CODEWORD material.

4. Platforms and some overseas fixed installations may also require that Australian Signals Directorate (ASD) undertake an emanation security threat assessment in order to ensure that TEMPEST issues are adequately addressed. Refer to the [Information Security Manual \(ISM\)](#); section Emanation Security Threat Assessments for the relevant policy.

5. ICT equipment must be protected with controls appropriate to its Business Impact Level (BIL). For further information on BILs, see the DS&VS BILs intranet page.

Protective Marking and Labelling

Actual and 'Handle As' Protective Markings

6. A device that stores digital information has an actual Protective Marking and a 'handle as' Protective Marking. When ASD-endorsed encryption is used, the 'handle as' Protective Marking (and associated physical security requirements) may be lower than the actual Protective Marking.

Example: A Defence laptop with an actual classification of 'SECRET' has ASD-endorsed encryption applied to reduce its 'handle-as' Protective Marking to 'OFFICIAL'. When the laptop is powered down (not hibernating) it does not require secure storage other than for normal protections against fire and theft.

7. The degree of reduction depends on the Protective Marking of the device and the type of encryption used. Unencrypted devices must not have a 'handle as' Protective Marking lower than the actual Protective Marking. For further requirements and information, see:

- a. DSPF Principle 19 – *Information Systems (Logical) Security*; and
- b. ISM Cryptographic Fundamentals.

8. When encryption is used to reduce the 'handle as' Protective Marking, the reduction in handling requirements only applies when the device is in an encrypted state.

9. At any point in which the information is in its decrypted state (e.g. when personnel log into the device), the device's 'handle as' Protective Marking must revert to being equal to its actual Protective Marking.

Example: A laptop uses whole disk encryption. When the laptop is powered off (not sleeping or hibernating), the information is in its encrypted state. When the user powers on the laptop, the encryption product displays a username/login prompt. Prior to these being entered, the laptop is still in its encrypted state. Immediately after these are correctly entered and the user is authenticated to the encryption product, the laptop is in an unencrypted state.

10. Encryption is particularly important when devices or media are moved outside Defence controlled spaces. See DSPF Principle 22 -Mobility Device Security.

Labelling ICT Hardware

11. ICT assets, are to be labelled in accordance with the actual Protective Marking of the information being stored, processed or communicated in accordance with DSPF Principle 22 – *Mobility Device Security* (noting the exclusions for High Assurance Products). If devices are too small to apply appropriate labelling refer to DSPF Principle 22 – *Mobility Device Security*.

Storage of ICT equipment

Physical Security for Fixed ICT Equipment

12. ICT equipment is to be afforded appropriate protection when not in use. The physical security controls are to meet those detailed in DSPF Principle 72 – *Physical Security*.

13. System Owners should use dedicated ICT facilities to house ICT systems, their components and associated equipment. These facilities include, but are not limited to:

- a. server rooms;
- b. data centres;
- c. backup repositories
- d. storage areas for ICT equipment that hold Official Information; and
- e. communication and patch rooms.

14. Fixed ICT equipment and facilities must be within an accredited Security Zone appropriate to the aggregation of the information stored and highest BIL assigned to the system. Refer to DSPF *Physical Security Controls*.

15. When an ICT facility or room used to house ICT equipment is fully enclosed by a higher Security Zone, and so protected by that zone's alarm or physical delay factors, ICT containers in the facility or room may be of a class appropriate to the higher zone. Refer to DSPF Principle 72 – *Physical Security*.

16. When an ICT facility or room used to house ICT equipment is not fully enclosed by a higher Security Zone (e.g. where a server room rated at Zone Four has an external door that opens onto a Zone One or Two) then further treatments apply in addition to the normal DSPF *Physical Security* and *Access Control* Controls:

- a. the ICT facility is to be secured to meet the following requirements:
 - (1) windows are to be fixed to prevent access or permanently alarmed;
 - (2) external doors used for regular access are to be alarmed and use Electronic Access Control; and
 - (3) external doors used for regular access are to have door open timer alarms to alert if the door is kept open;
- b. the ICT facility is to be on a separate alarm zone and armed at all times when not occupied; and

- c. any security containers used in the facility must be appropriate for the lower zone (i.e. a higher class of container is required) and locked at all times when the ICT facility is unattended.

17. These additional treatments do not apply where an ICT facility has fire escape doors or other doors intended for occasional use, such as loading bay access that are continuously alarmed or in their own alarm zone.

18. As with any other asset, assigned BILs will help to determine the appropriate security controls to apply to ICT equipment. For more information refer to Physical Security Controls.

Example: A system may have a high availability BIL, but a low confidentiality BIL will require a greater focus on preventing theft, accidental damage, or sabotage. Human Resources data, for example, is essential information for Defence, however may not require a high clearance for access.

High Assurance Products

19. High Assurance Products and Controlled Cryptographic Items are to be physically secured in accordance with DSPF Principle 13 – *Communications Security (COMSEC)*, applicable Australian Communications Security Instructions (ACSI) documents and relevant instructions issued by ASD.

20. Electronic Media that cannot be kept in Security Containers when not in use. Some ICT equipment cannot feasibly be stored in security containers or rooms when not in use (e.g. desktop computers, printers, Multi-function device (MFD)). Measures such as removable media, encryption and thin client technology can help to reduce the storage requirements of such devices.

21. Where possible ICT equipment that cannot be stored in security containers or rooms should make use of removable non-volatile media (e.g. removable hard-drives) that can then be stored in an appropriate security container when not in use. In such cases:

- a. the media are to be labelled with appropriate Protective Marking;
- b. physical storage, handling and management processes must be documented and accredited as part of a system Standard Operating Procedures (SOP);
- c. all users handling the media must be aware of their responsibilities; and
- d. breaches of handling procedures that result in inadequate protection of media **must** be reported as a security incident in accordance with DSPF Principle 24 – *Information Systems Security Incident Management*.

22. If suitable encryption is applied to reduce the 'handle as' Protective Marking this might reduce the zone required for storage. Encryption is intended to protect the confidentiality of information and can have benefits in terms of integrity. However, it

does not protect the availability of information. These factors need to be considered when assessing suitable zones for encrypted devices.

23. Thin client technology can reduce physical requirements for storage when equipment is not in use by reducing or eliminating local storage of information. When assessing suitable zones for thin client devices, the following are to be considered:

- a. does the device store or cache any information locally;
- b. does the device contain any sensitive information locally in firmware; and
- c. could malicious modification of the device hardware or firmware affect the security of the network?

Example: A hardware keystroke logger could be covertly added in order to collect sensitive information.

24. In cases where the non-volatile media cannot be removed, suitable encryption cannot be applied, and thin client technology is not used, the owner or manager of the equipment is to determine the Physical Security Zone where the equipment can be kept based on the risks of compromise to the confidentiality, integrity or availability of the information.

ICT Used to Administer Physical Devices

25. ICT devices, such as laptops, that are used to administer classified physical devices or assets must be stored in accordance with their 'handle as' Protective Marking when not in use.

ICT Equipment During Development or Installation

26. Servers and network equipment may require a degree of physical protection during development and installation prior to them storing, processing or communicating Official Information. This may be required in order to protect confidentiality of the design and the integrity of the equipment.

Example: Prior to use or installation, a piece of ICT equipment may have low confidentiality and availability BILs. The integrity BIL may be high, though. This is because of the potential impact to Defence if the equipment is compromised or tampered with.

Lockable Commercial ICT Cabinets – Specifications for Defence

27. **Procurement.** Lockable ICT Cabinets may be procured from any vendor as long as the cabinet meets the following minimum specifications:

- a. all fixed panels must be secured internally and cannot be removed without the use of tools;

- b. front and rear doors must have as a minimum single point locking. This does not need to be an approved lock from the Security Equipment Evaluated Products List (SEEPL);
- c. doors must either:
 - (1) have hinges internally mounted; or
 - (2) utilise hinge bolts on the hinge side of the door that secures that side of the door into the frame when closed;
- d. door panels:
 - (1) if wholly constructed of metal, may be perforated with holes no more than 5mm diameter to assist in air circulation; and
 - (2) if Perspex, these must have the Perspex sealed and mounted using cup head screws, or equivalent, such that tampering or forced intrusion is clearly evident;
- e. the cabinet must have four levelling feet designed to enable bolting to floor, and be secured to the floor where possible; and
- f. where possible, power must be terminated within the cabinet.

28. **Instructions for use of products.** ICT Cabinets must be assembled, installed and loaded according to manufacturer's guidance.

Visual Oversight

Visibility of Displays

29. The information processed by a system or device are to be protected from oversight (and/or overhearing) by anyone not authorised to know the information.

Example: In most cases this will involve people viewing the contents of a screen ('shoulder surfing'). However this also applies to audio that might be overheard.

30. Fixed ICT systems should be positioned to prevent information visible on displays or projections from being observed by people without the required clearance or need to know.

31. Portable devices are not to be used when there is potential for Official Information to be overseen (or overheard) by unauthorised people. Full policy including approvals processes and access restrictions for working outside of Defence environments is contained in DSPF Principle 19 – *Information Systems (Logical) Security*.

Example: A device processing Official Information cannot be used on a commercial flight when another passenger might see or hear the information.

Digital cameras, recording devices and wearable computing

32. Privately owned devices with recording capability (including still photography, video capture and audio recording) are not to be used to capture sensitive or classified information or be used in an environment in which this might inadvertently occur. Full policy on the use of portable electronic devices and private electronic devices is contained in DSPF Principle 22 – *Mobility Device Security*.

33. Any sensitive or classified information captured on a personal device is to be considered as a data spill and must be reported as a security incident in accordance with DSPF Principle 24 – *Information Systems Security Incident Management*.

Technical Surveillance Counter-Measures

34. For policy regarding Technical Surveillance Countermeasures see DSPF Principle 14 – *Audio-visual Security* and the *Emanations Security* section of the [ISM](#).

Movement of ICT Equipment

35. The transfer of ICT equipment is to be conducted in accordance with DSPF Principle 71 – *Physical Transfer of Information and Assets* and DSPF Principle 22 – *Mobility Device Security*.

Tamper Evidence

Tamper Evident Seals

36. The Owner or Manager of ICT equipment may seal access to ICT assets using SCEC approved tamper evident wafer seals suitable for application to hard surfaces. The use of seals provides a visual indication of unauthorised access. When SCEC endorsed seals are used:

- a. they should be selected from the [Security Equipment Catalogue](#);
- b. system SOP should include processes for applying, recording details, and replacing seals; and
- c. incident response plans covering a system should include processes to manage situations in which broken seals are detected.

Auditing of Fixed Equipment

37. System Owners and Equipment Managers must record the physical location of fixed ICT equipment in an inventory and audit against this on a regular basis.

38. The frequency of audits must be based on the assessed risks to systems, documented in system SOP and considered during system certification and accreditation.

39. System and Equipment Managers are to, based on their risk assessments, consider visually inspecting ICT equipment as part of their asset control audit as a means of detecting non-approved or malicious devices connected or installed.

40. Portable ICT assets (including Mobile devices) are to be tracked and accounted for in accordance with DSPF Principle 22 – *Mobility Device Security*.

Wireless LAN Availability Considerations

41. Wireless Local Area Network (LAN) and ad hoc networks are susceptible to electronic attack or disruption of service, therefore when designing a wireless LAN or considering an ad hoc networking arrangement, it is important to consider the availability BIL of systems that will rely on that network segment.

42. Where a wireless LAN will provide service for systems with availability BILs of high or greater the network owner **must** undertake a risk assessment, develop and implement a mitigation plan during the network design and construction phase.

43. See the *Wireless LAN* section of the [ISM](#) for further requirements and guidance.

Loss and Recovery of ICT Equipment

Loss of equipment

44. Lost or stolen *ICT* equipment is to be reported as a security incident in accordance with:

- a. DSPF Principle 24 – *Information Systems Security Incident Management*; and
- b. DSPF Principle 18 – *Information Systems (Personnel) Security*.

Recovery of Equipment

45. If ICT equipment previously reported lost or stolen is recovered, the initial incident report is to be updated to reflect this.

46. The recovery of ICT equipment not previously reported lost or stolen must be reported as a security incident.

47. In the event that lost or stolen ICT equipment is recovered, all reasonable measures are to be taken to preserve any evidence for use by an investigative authority.

48. If the ICT equipment or device is not required, or has been released by the relevant investigative authority, it must be sanitised and reinstalled from a trusted source before it is reused.

Note: Installation media lost and recovered with the device is not to be considered trusted for the purposes of reinstalling the system. This includes reinstalling a laptop from a recovery partition on the laptop's hard drive.

Cable Security

49. Cabling and associated physical infrastructure is to meet the security requirements stated in the Communications Infrastructure section of the [ISM](#).

Use of Shared Conduit

50. Where Defence cabling occupies the same conduit as used by other Australian Government agencies, the ITSA is to coordinate with their counterpart in the other agency on any relevant ICT matters.

Use of Public Utility Conduit

51. Defence or Defence Industry Security Program (DISP) member conduit (pit, pipe etc.) should be used for the distribution of Defence cabling.

52. If Defence conduit is not available and a Telecommunications or Public Utilities' conduit is to be used to run Defence cabling, the system owner must seek approval from the conduit owner before installing Defence cables in third party conduit.

Note: DISP members may share Defence conduit where there is a requirement for a DISP company network to be installed on the Defence estate.

53. Official Information not for public release that is unencrypted, or encrypted but not to the [ISM](#) standards necessary to reduce transmission requirements to 'OFFICIAL', must not be run in non-defence conduit unless the conduit owner has consented to it being secured and inspected in accordance with the requirements for unsecured areas below.

A Requirement for Cable Runs in Unsecured Areas on the Defence Estate

54. Unsecured areas are those spaces where access is not controlled or limited to staff with an appropriate security clearance. On the Defence Estate this includes all areas of a base (conduit in pit and pipe) that are open to the public, or other uncleared persons (e.g. uncleared family or dependents etc.).

55. The [ISM](#) requires encryption wherever a cable is run in an unsecure area. Encryption requirements may be reduced on the Defence Estate, provided that the requirements of this section are met. The requirements of this section have been designed to address the risk of unencrypted communications being intercepted.

56. Conduits for unencrypted cable installation in unsecured spaces must be assessed by the certification authority and approved by the accreditation authority.

57. Buried conduits between buildings **must**:
- a. be marked as per AS/NZS 3085.1:2004 Telecommunications installations – Telecommunications pathways basic requirements;
 - b. be coloured white or grey;
 - c. comply with the minimum requirements of AS/NZS 2053 -Conduits and fittings for electrical installations:
 - (1) rigid PVC conduit; or
 - (2) flexible PVC conduit; and
 - d. comply with AS/CA S009:2013 Installation requirements for customer cabling (Wiring Rules).
58. Defence controlled cable pits that carry unencrypted classified data must be constructed to the following standards:
- a. AS 3996-2006 Access covers and grates, where appropriate; and
 - b. AS/NZS 3084:2017 Telecommunications installations – Telecommunications pathways and spaces for commercial buildings.
59. Surface mounted cable pit construction must incorporate SCEC approved:
- a. tamper evident pit lids; and
 - b. locking devices which have been endorsed for Secure Area applications, to secure the lid.
60. Sub-surface cable pit construction must incorporate:
- a. lockable pit lids; and
 - b. SCEC approved locking devices that have been endorsed for Secure Area applications, to secure the lid.
61. A management plan for key control of pits must be approved by the accreditation authority and implemented by the System Owner.
62. Inspections of external pits and pipe must be conducted:
- a. in accordance with a cable inspection plan endorsed by the accreditation authority; or
 - b. within the following schedules:
 - (1) visible portions of cable every six months;

- (2) concealed portions, via inspection points each year; or
 - (3) optical fibre with approved intrusion detection products or devices, a minimum of 10 percent of the total optical fibre must be inspected each year;
- c. if a possible security irregularity or breach is discovered, the remaining cable must be inspected.

Cabling Requirements on Defence Platforms

63. The accreditation authority will risk assess the requirements for conduit for ADF Platforms. Platforms are normally the subject of increased guarding and access control measures therefore inspectable conduit will not normally be required within the platform.

Personnel Requirements in Secure Areas

64. Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis.
65. Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities.
66. Areas containing particularly sensitive materials or ICT equipment can be provided with additional security through the use of a designated No Lone Zone. The aim of this designation is to enforce two-person integrity, where all actions are witnessed by at least one other person. Further information available in the [ISM](#).
67. Vacant secure areas should be physically locked and periodically checked.
68. Third party support services personnel are only to be granted restricted access to secure areas or sensitive information processing facilities when required for service delivery. This access should be authorised and monitored. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.
69. Photographic, video, audio or other recording equipment should not be allowed, unless authorised.
70. In aggregation, all of the control requirements, ACSI and Governing standards suggest that portable ICT devices should be banned from a secured facility. Information Assurance, in its capacity of Accreditation Authority has also deemed that RED processing areas are portable ICT device (including Mobile phones) Prohibited Areas and No Lone Zones. It should be noted that noncompliance with this directive can be construed as a breach of the [Crimes Act 1914](#).

Mobile Devices in Security Areas

71. There are hazards associated with TEMPEST radiation; acoustic coupling and separation requirements for Private Automatic Branch Exchange (PABX) (unencrypted) telephones and operating information systems within the vicinity of Radio Frequency (RF) transmitters (e.g. mobile cellular telephones and some pagers).

72. Defence deploy security measures to detect and respond to active RF devices in secured spaces in accordance with ACSI 61(C) and ACSI 61(D).

Roles and Responsibilities

First Assistant Secretary Security and Vetting Service

73. The First Assistant Secretary Security and Vetting Service (FAS S&VS) is responsible for:

- a. developing security policy (refer to DSPF *Physical Security Controls*);
- b. managing physical certification and accreditation (refer to DSPF *Physical Security Certification and Accreditation Controls*);
- c. reviewing and reporting of security performance; and
- d. overseeing the management of security incidents (refer to DSPF *Physical Security Incidents and Investigations Control*).

Chief Information Officer (CIO)

74. The CIO is responsible for ensuring that the SIE operates in spaces that offer appropriate physical security.

Chief Information Security Officer (CISO)

75. The CISO is responsible for:

- a. establishing the strategic direction for ICT security across Defence and Defence industry;
- b. developing and maintaining an ICT security strategy;
- c. contributing security expertise to the development and maintenance of an ICT security architecture;
- d. maintaining an effective ICT certification and accreditation framework for Defence and Defence industry in accordance with Government expectations, Defence policy and the Defence ICT security strategy; and
- e. liaising with FAS S&VS and SSA to ensure that information systems security is integrated with broader protective security strategies, policies, and plans.

Information Security Technology Adviser (ITSA)

76. The ITSA is responsible for:
- a. coordinating ICT certification functions to a standard that meets Government expectations, ensuring that ICT certification authorities liaise with physical certification authorities as required; and
 - b. liaising with ITSA in other agencies on technical ICT security matters, including situations in which physical security issues in either agency affects shared ICT risks.

Information Technology Security Manager (ITSM)

77. The ITSM function is a specific subset of the System Manager role. It may be performed by the System Manager directly or the System Manager may delegate the function to a separate appointment.

78. The ITSM is responsible for:
- a. liaising with the Defence ITSA;
 - b. informing the system manager of any identified risks to the systems for which they are responsible;
 - c. informing the ITSA of any risks that may also affect other systems;
 - d. identifying potential security improvements;
 - e. ensuring that security recommendations or requirements provided by the ITSA are enacted; and
 - f. maintaining system configuration in accordance with accredited processes.

Information Technology Security Officer (ITSO)

79. The ITSOs are responsible for:
- a. implementing directions from the ITSM, system manager and the ITSA;
 - b. notifying the ITSM of any identified vulnerability that may prejudice the security of the system;
 - c. reporting any security incidents detected or identified; and
 - d. performing security management tasks in accordance with applicable SOPs and any other conditions stipulated during accreditation.

Note: This role has been introduced in order to align Defence terminology with the [ISM](#). Previously within Defence, many functions of this role would have been performed by the ISSO. In many cases ISSO will become ITSO. In cases where an ISSO manages or coordinates other ISSO, the lead ISSO may become an ITSM.

System Owner

80. System Owners are responsible for:
- a. ensuring that systems are afforded physical protection suitable to address the risks informed by assessed BIL;
 - b. ensuring that equipment is appropriately labelled and that security obligations are effectively communicated to system users;
 - c. maintaining an inventory of fixed ICT equipment, including its physical location, and performing periodic audits against this inventory;
 - d. ensuring that systems are operated and managed in accordance with their accreditation; and
 - e. ensuring that systems are securely decommissioned at the end of their lifecycle.

Note: Where security requirements cannot be met, system owners are responsible for requesting dispensations in accordance with the processes stipulated DSPF Principle 23 -ICT Certification and Accreditation. System owners are responsible for developing dispensation requests in a timely manner to allow the process to complete before non-compliance occurs.

ICT Certification Authorities

81. Certification Authorities are responsible for:
- a. ensuring that the certification of information systems considers the physical environment in which the system operates; and
 - b. liaising with physical certification authorities as required.

ICT Accreditation Authorities

82. Accreditation Authorities are responsible for:
- a. ensuring that physical security requirements have been addressed as part of the certification process; and
 - b. deciding whether or not to accept any residual risk(s) resulting from physical security matters.

Commanders and Managers

83. Commanders and Managers are responsible for:
- a. ensuring that workspaces continue to meet physical security requirements applicable to systems within that workspace;
 - b. ensuring that local security standing orders afford proper protection to digital media and hardcopy that forms input to or output from ICT systems; and
 - c. ensuring that personnel undertake required training and awareness activities.

Contract Managers

84. Contract managers are responsible for ensuring that Defence information provided electronically to industry is processed, stored and communicated by accredited systems with appropriate levels of physical security.

Equipment Managers

85. Equipment Managers are responsible for:
- a. ensuring that equipment is used and stored in areas with appropriate levels of physical security;
 - b. maintaining an inventory of equipment under their control and auditing against this inventory; and
 - c. reporting any incidents involving equipment under their control and performing any remedial action as required by relevant investigative authorities.

System Users

86. System Users are responsible for:
- a. using systems in accordance with applicable SOP;
 - b. handling physical media and hardcopy material associated with ICT systems in accordance with applicable security requirements; and
 - c. reporting any physical security incidents affecting ICT systems.

Key Definitions

87. **Information and Communications Technology (ICT):** ICT encompasses any medium used to record, process, store and transfer information, including:
- a. data storage devices (e.g. magnetic disk/tape, compact disks/digital video disks, flash memory, etc.);

- b. the technology used for transferring or communicating information; and
- c. the operating systems, hardware and software applications used to operate networks and systems.

88. **ICT Equipment:** Any device that can process, store or communicate electronic information. For example, computers, multifunction devices, landline and mobile phones, digital cameras, electronic storage media and other radio devices.

89. **ICT Facility:** A building, a floor of a building or a designated space on the floor of a building used to house or process large quantities of data. For example, server and gateway rooms, data centres, back up repositories, storage areas for ICT equipment, and communications and patch rooms.

90. **ICT System:** A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.

91. **ICT System Equipment:** A subset of ICT equipment that is used to maintain an ICT system. For example, servers, communications network devices such as PABX, gateways and network infrastructure such as cabling and patch panels. This equipment is normally continuously operational.

92. **Network Infrastructure:** The infrastructure used to carry information between workstations and servers or other network devices. For example: cabling, junction boxes, patch panels, fibre distribution panels and structured wiring enclosures.

93. **Non-volatile Media:** A type of media which retains its information when power is removed.

94. **Security Rated Area:** A collective term describing areas on a site that have adequate physical security measures in place to process, handle and store security classified information and other official resources. Individually, these areas are known as Secure Areas, Partially Secure Areas and Intruder Resistant Areas. An area that does not meet any of these standards is known as an unsecured area.

95. **Volatile Media:** A type of media, such as Random Access Memory (RAM), which gradually loses its information when power is removed.

Further Definitions

96. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems (Physical) Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 17.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems (Physical) Security
Related DSPF Control(s)	Assessing and Protecting Official Information Security for Projects Communications Security (COMSEC) Offshore and Cloud Based Computing Security ICT Certification and Accreditation Information Systems Security Incident Management Information Systems Business Impact Levels and Aggregation Access Control Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Personnel) Security

General principle

1. Defence will ensure that Information Communications and Technology (ICT) systems are only accessed by authorised users who hold a Defence personnel security clearance at, or above, the required level, and who have a demonstrated need-to-know.

Rationale

2. Confidence in the security of an ICT system can only be maintained if personnel security is applied to the systems users.

3. Different users present different security risks to Defence and Defence Industry information systems. For this reason, Defence needs to understand the mix of users of its systems and ensure that the right information is available to the right people at the right times.

Expected outcomes

4. Defence ICT systems are only accessible by authorised personnel with:

- a. an appropriate level of clearance; and
- b. a demonstrated need-to-know.

5. The number of privileged users is kept to a minimum and regularly reviewed.

6. Privileged users are only assigned the minimum amount of privileges to be able to perform their assigned tasks related to their role and responsibilities.

7. Foreign nationals are only able to access information that is releasable to their nationality. On the rare occasions when privileged access by foreign nationals is required, it is tightly controlled.

Escalation Thresholds

8. The Information Technology Security Advisor (ITSA) has set the following general threshold for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Residual Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems (Personnel) Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 18
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 18.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	PSPF Core Requirements : classification of Information; access to Information; safeguarding information from cyber threats; and robust information and communication and technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Information Systems (Logical) Security Mobility Device Security Protected Identities Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government information security management guidelines – Australian Government security classification system Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material Australian Government Information Security Manual (ISM)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Personnel) Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the Owner for this Enterprise-wide Control.
2. The Accountable Officer for the Information and Communications Technology domain is the Chief Information Officer. The ITSA also works under this domain.

Escalation Thresholds

3. The ITSA has set the following general threshold for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Residual Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

Information Systems (Personnel) Security

System Access Approval

4. All access to ICT systems and networks is to be governed by an approval process that ensures users meet all applicable security requirements and are assigned an appropriate level of privilege before access is granted.
5. Access to ICT systems, including any internal or external facing ICT systems, is only granted on a need-to-know basis. Unauthorised access, use, disclosure, disruption, modification, or destruction of ICT systems or the information they store, process, or communicate, is prohibited.
6. System Owners are to:
 - a. ensure ICT systems under their control provide only the minimum level of access required for an individual to be able to perform their assigned duties based on the least privilege principle. Defence personnel are only to be granted the least amount of privileges to ICT systems to perform their duties based on these requirements; and
 - b. specify approval processes in system documentation for consideration as part of system certification and accreditation.
7. System Managers are to ensure that:
 - a. all account creation is formally recorded and managed in order to safeguard system integrity. These records are to be immediately available upon request to appropriately authorised investigators and auditors;
 - b. user accounts are suspended or revoked when:
 - (1) they are no longer required;
 - (2) there is a period of inactivity;
 - (3) the user no longer meets access suitability requirements;
 - (4) the user's access to the system poses an unacceptable risk;
 - (5) the user account has not been, or will not be, used for a period in excess of 30 days (the account is to be suspended); or
 - (6) the user account has not been used for a period greater than 120 days (the account is to be revoked.); and

- c. when an individual leaves Defence, the Commander and/or Manager will ensure that all Defence user accounts attributed to that individual are removed from all ICT Systems at the time their employment or duties with Defence cease.
- 8. System Users:
 - a. **must not** share their account with any other person (irrespective of whether they are authorised system users or not) and are responsible for ensuring:
 - (1) their logon credentials are not shared; and
 - (2) they do not log into a system with the intent to allow someone else to use their account.
 - b. **must not** deliberately, or intentionally elevate, or attempt to elevate, their own user account privileges, or any other ICT System account, to cause, or lead to, an adverse or undesirable outcome or effect to the security of the Single Information Environment (SIE). This includes any action that may jeopardise the confidentiality, integrity and availability of ICT systems, devices and information which may result in harm to Defence capability, resources, reputation or people; and
 - c. are to ensure the continued accuracy of their personal details in the *Defence Corporate Directory* so that it reflects their correct name, organisation, location, contact details and HR data.

Security Training and Awareness Requirements

- 9. All Defence personnel are to understand their obligations when using ICT systems. All users:
 - a. are to be aware of system specific security obligations as specified in security policies and procedures;
 - b. are to be aware of, and agree to, the extent of potential system monitoring for security purposes and the ways in which the collected information may be used; and
 - c. are to maintain a current knowledge and understanding of the ICT system aspects (including software) to be used, supported, or managed whilst undertaking their duties.
- 10. Defence personnel are to be made aware of security threats, the protective security measures to counter these threats, and their responsibilities.

User Passphrase

11. System users are to maintain a strong passphrase/password management regime for all user accounts assigned to them and are to change their passwords on a regular basis.
12. All passwords, including initial passwords, must be constructed and implemented according to the following rules:
 - a. passwords are to meet length and complexity requirements stipulated within the ISM;
 - b. users are to change their account password on first login;
 - c. system users or account holders can only request a password to be reset for their own account;
 - d. no default passwords are provided to or otherwise exposed to the user during the handover procedure;
 - e. system users **must not** disclose their own individual passwords to other system users or any other entity;
 - f. passwords should not contain anything that can be easily attributed to the account owner such as: username, social security number, nickname, relative's names, birth date, etc.;
 - g. passwords should not be dictionary words or acronyms;
 - h. password history is to be kept to prevent the reuse of passwords; and
 - i. stored passwords are to be encrypted.
13. Security tokens (i.e. smartcards, access passes, and multi-factor authentication devices) are to be returned to Defence upon termination of employment, or cessation of duties with Defence, or provided back to Defence upon request.
14. If the security of a password is in doubt, the password is to be changed immediately.
15. Administrators **must not** circumvent the Password Policy for the sake of ease of use.

16. System users are not to use automated authentication procedures (such as use of password keychains or password remembering features within applications), scripts, or other means to circumvent the password or authentication requirements for password entry or authentication every time access to an ICT system, resource or component (such as an application) is required. Exceptions may be made for specific ICT systems or scenarios (like automated backup) where approval has been explicitly authorised by the entity responsible for residual risk acceptance of that system or capability. In order for an exception to be approved, there should be a procedure to change the passwords.

17. Defence ICT Service Desk password reset procedures are to include the following:

- a. the user requesting a password reset is to be positively identified before their password is reset; and
- b. the user is to change their password at first login.

18. In the event passwords are found or discovered, the following steps are to be taken:

- a. ensure the password is secured;
- b. report the discovery to the Defence ICT Service Desk as an ICT Security Incident;
- c. the Defence ICT Service Desk will arrange for the affected account to be disabled immediately; and
- d. if physical, transfer the passwords to an authorised person as directed by the ITSM.

Hardware and Firmware Passwords

19. Passwords used to protect privileged access (i.e. administration access) to workstation/server Basic Input Output Systems (BIOS) or dedicated operating systems for network communications equipment is to be set and managed in accordance with the following:

- a. hardware/firmware passwords will be set by Defence Network Administration and support personnel responsible for that equipment. A record of current hardware/firmware passwords will be recorded within the Defence Network Password Escrow in accordance with the procedures detailed above for “systems” system account procedures;

- b. changing of Defence Network workstation/server BIOS passwords every 45 days is not considered practical, particularly where a large number of hosts are involved. BIOS passwords will be changed as the last action of a task to upgrade or reconfigure the BIOS of workstations at a site. In the absence of any such tasks, BIOS passwords will be changed annually; and
- c. the use of a common BIOS password for like hosts across a site is permissible.

System Access Requirements for Australian Citizens

General Requirements for System Access by Australian Citizens

- 20. To access classified Defence or Defence industry ICT systems, users should:
 - a. be Australian citizens;
 - b. hold an appropriate security clearance, and briefings (where applicable); and
 - c. have a legitimate need-to-know.

Note: The level of clearance and types of briefings needed to access Official Information depends on the Protective Marking and caveats applicable to that information. These requirements are specified by the Protective Security Policy Framework (PSPF) and in DSPF Principle 10 – Assessing and Protecting Official Information.

Note: Temporary provisions that allow a person to access classified information and assets without meeting security clearance requirements do not allow unrestricted access to ICT systems. For details of access restrictions see DSPF Principle 41 – Temporary Access to Classified Information and Assets.

Privileged Access by Australian Citizens

- 21. Privileged users are trusted to perform system administration activities that are not permitted for standard users.
- 22. Privileged users must only use their privileged credentials for execution of the functions for which they were issued. When conducting authorised tasking, they will be performed with the lowest level of privilege necessary to perform the action. All privileged user accounts will be strictly monitored.
- 23. System owners must limit the number of privileged users to the minimum required for the effective management of the system or network. As well, system managers:
 - a. **must** monitor and review the quantity of privileged user accounts to prevent inflation in the number of such accounts; and

b. **must** document any requirement to increase the number of privileged users. These records are to be retained for auditing and security performance reporting purposes.

24. Privileged users must have a clearance suitable for access to the system or network and a defined need to have privileged access. Privileged access is to be removed immediately after a user changes roles.

25. It is the prerogative of system owners to decide whether or not privileged users need a clearance higher than would normally be required for standard users. This should be a risk-based decision that considers risks, costs and factors specific to the system.

26. This decision should be reflected in system documentation and considered during certification and accreditation.

System Access Requirements for Non-Defence APS Employees

27. There may be circumstances in which APS employees from agencies other than Defence require access to Defence systems and networks.

***Example:** The Department of Veterans' Affairs may have a need and a right to access certain Defence information.*

28. Non-Defence APS employees have the same clearance and need-to-know requirements as other users. Responsibility for Other Defence Support (ODS) system/network sponsorship of non-Defence APS employees is to remain with Defence.

29. Formalised processes for requesting and approving ODS system/network sponsorship are to be developed in consultation with the ITSA and specified in system documentation. The ITSA will consider the proposed process in the context of recorded dispensations applicable to both agencies.

30. The ITSA is to be consulted on variations to the agreed process.

***Example:** A proposal to extend an existing agreement (allowing non-Defence APS employees desktop access to a Defence system) by introducing a remote access capability.*

31. The Defence ITSA will liaise with their counterparts in external agencies in order to monitor operation of the agreement and manage incidents.

System Access Requirements for Protected Identities

32. Protected Identity status is granted to Defence individuals associated with sensitive capabilities to protect against unauthorised disclosure of both their personal information and sensitive capabilities in order to maintain operational security.

33. Systems that hold and process the personal information of those individuals with Protected Identities are to provide adequate protection to those identities. For

requirements specific to protected identities, see DSPF Principle 42 – *Identity Security*.

34. Any unauthorised disclosure of a protected identity is a major security incident and is to be reported in accordance with DSPF Principle 24 – *ICT Security Incident Management*.

System Access Requirements for Foreign Nationals

General Requirements for System Access by Foreign Nationals

35. Foreign nationals will only be able to access information on ICT systems that is releasable to their nationality or when embedded within Defence as a seconded foreign national.

36. Foreign national access to Defence ICT systems is contingent on an appropriate foreign release approval in accordance with Control 15.1 – *Foreign Release of Official Information*.

37. Before a foreign national may be granted access to Australian ICT systems processing information 'PROTECTED' or above, the following requirements are to be met:

- a. The foreign national is to hold a foreign clearance at an equivalent level that is formally recognised under the provisions of an existing Security of Information Agreement or Arrangement (SIA) or hold an Australian security clearance supported by a Citizenship Eligibility waiver. For further information see DSPF Principle 15 – *Foreign Release of Official Information* and DSPF Principle 40 – *Personnel Security Clearance*; and
 - (1) Where an SIA exists, the requester is to provide foreign release approval from an EL2/06 level officer (or higher) and a security clearance verification from AGSVA to request ICT system access.
 - (2) Where an SIA does not exist, or if a security clearance cannot be verified, the requester is to provide Assistant Secretary Security Policy and Services (ASSPS) foreign release approval to request ICT system access.
- b. Where a foreign national does not meet the requirements set out in 37a (1) or (2), DS&VS International Security Policy is to be consulted prior to ICT access being granted.

Note: A list of 'OFFICIAL' SIAs are available on the Defence Protected Network (DPN).

Note: A personnel security clearance granted to a foreign national by their government (or any government other than Australia) does not automatically grant access to classified information generated by or on behalf of the Department of Defence, Australia or a third party, or automatically grant access to ICT systems or networks within the Defence SIE.

- c. The ICT system being accessed is to either:
- (1) hold only information that is releasable to the specified foreign nation; or
 - (2) be accredited in accordance with relevant ISM controls relating to including Access by foreign nationals to Australian systems 0409, 0411, and 0816.

38. Foreign national access to Official Information (including 'OFFICIAL', 'OFFICIAL: Sensitive' and sensitive information marked with an Information Management Marker) is to be managed on a case-by-case basis depending on the provisions of any existing SIA. This is to be managed in accordance with DSPF Principle 15 – *Foreign Release of Official Information*.

Exclusion: Foreign nationals may access 'OFFICIAL' information that has been approved for public release without restriction.

39. Access to the DPN and Defence Secret Network (DSN) is only to be granted to foreign nationals from the nations of Canada, New Zealand, United Kingdom or the United States (CAN/NZL/UK/USA).

40. Foreign national access to other classified systems will be governed by processes defined and approved during the certification and accreditation process.

41. Requests for access to the DPN by foreign nationals outside of CAN/NZL/UK/USA are to be managed on a case-by-case basis, and approved by ITSA, subject to the requirements at 37 being met.

42. Any security incidents reported involving foreign nationals are to accurately reflect the nationality of the user.

Protection of Foreign Government and Other Limited Releasability Material

43. Foreign government information on Defence systems is to be protected in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information*. Defence and Defence industry are required to ensure foreign government information and Limited releasable material is:

- a. stored only within data areas ("Personal", or preferably corporate) that have access permissions configured to deny access to those Integrated Foreign Nationals from countries not listed within the material's releasability markings; and
- b. not displayed from the SIE (e.g. via briefing room projected display) in a situation or manner that would permit the material to be accessible to Integrated Foreign National personnel not covered by the material's releasability.

44. Foreign nationals are only to have access to information that is releasable to their nationality, in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information*.

45. Foreign national access to information outside their nationality, without appropriate approval, is a security incident and is to be reported in accordance with DSPF Control 77.1 – *Security Incidents and Investigations*. DS&VS International Security Policy is to also be notified to ensure Defence fulfils our obligations under our SIA.

Foreign National Access Via Coalition Gateways

46. Foreign national access may occur from a foreign system to an Australian system via an accredited coalition gateway. When a foreign national accesses a Defence network via an accredited coalition gateway the information exchanged is subject to the relevant SIA defined above. This form of exchange is conducted as a Government to Government foreign release. For more information, see DSPF Principle 10 – *Assessing and Protecting Official Information* and DSPF Principle 15 – *Foreign Release of Official Information*.

47. It is the responsibility of the each government to ensure that their respective users accessing the coalition gateway hold a valid security clearance. However, it remains Australia's responsibility to configure system controls to restrict access according to the need-to-know principle.

Segregation of Duties

48. Duties and responsibilities are to be segregated in order to reduce opportunities for unauthorised or unintentional modification or misuse of information assets.

49. Security documentation should identify any key activities that are not to be performed by the same person.

Example: System documentation should specifically prohibit a person with 'copy to removable media' privileges from being able to delete or modify logs of such transactions.

Suspension or Revocation of Access

50. Defence business areas must have policies and procedures to ensure that system access rights are:

- a. reviewed at regular intervals; and
- b. are suspended or revoked if (applicable to both standard or privileged to Defence ICT systems):
 - (1) it is no longer required;
 - (2) users no longer meet access suitability requirements; or

(3) the user's access to the system poses an unacceptable risk.

51. If system access is to be suspended, disabled or revoked, it is to be done in a manner that preserves identity details that can be linked to existing event information. System owners are to avoid situations in which identity information is lost due to the deletion of an account. Such circumstances may result in a reduced ability to conduct audits or investigations in the future. To avoid this:

- a. the disabling, suspension or revocation of an account is to be documented;
- b. the re-enabling of an account is to be documented; and
- c. any unauthorised re-enabling of an account is a security incident and is to be reported in accordance with DSPF Principle 77 – *Security Incidents and Investigations*, and DSPF Principle 15 – *Foreign Release of Official Information* if for the users is that are a foreign nationals.

Access no longer required

52. Access to systems, subsystems or specific information assets is to be suspended or revoked if changing circumstances mean that access is no longer required. Changes in circumstances might include:

- a. the user leaves Defence or ends a contract with Defence;
- b. the user moves to another role that does not require system access;
- c. the activity that required the access ends; or
- d. the nature of the user's role changes and access is no longer needed.

Access Requirements No Longer Met

53. System access **must** be suspended, disabled or revoked if the user no longer meets access requirements. Circumstances might include:

- a. revocation or downgrading of a security clearance or required briefing;
- b. changes to citizenship; and
- c. changes to the system that increases access requirements.

Unacceptable Risk

54. System access **must be** suspended, disabled or revoked if the user poses an unacceptable risk to the system or information assets. Circumstances might include:

- a. a significant security incident caused by the user; or
- b. a pattern of minor security incidents caused by the user.

Maintaining System Access when Moving Between Roles

55. When a user moves between roles, ICT system access may be maintained during the transition if:
- the user maintains the necessary clearance and briefings (if applicable) to enable continued access to the system;
 - the person continues to have a need-to-know as verified by continued formal sponsorship; and
 - the user account is appropriately modified or recreated to reflect the user's new role and need-to-know.

Example: A serving ADF member transfers to the reserves and enters full time employment as a contractor to Defence. In this case, the user will be provided with a new account to use in their role as a contractor. The person's ADF account may be retained for their use when on duty as a reservist. If the person misuses their reserve account to access information as a contractor without authorisation, this is a security incident and needs to be reported.

56. Access to systems is not to continue 'just in case' it is needed in the user's new role.
57. Defence personnel who are employed by Defence in multiple roles (e.g. APS and Reservist, Contractor and Reservist) should only use their login credentials assigned to their current duty. This is to ensure as that identity to ensure a separation of duties and system security audit trails are maintained.

Account Records

58. System owners are to keep adequate records of account creation, disabling/enabling and revocation to enable Defence to know who is using its systems and networks. These records may be required in the event of an audit or security investigation.

Roles and Responsibilities

Chief Information Officer

59. With regard to the information systems (personnel) security, the CIO as the ICT capability owner is responsible for:
- ensuring that processes are in place to limit SIE systems access to personnel who meet applicable security requirements; and
 - ensuring that the SIE is covered by suitable acceptable use policies.

Chief Information Security Officer

60. With regard to the information systems (personnel) security, the CISO is responsible for:
- a. developing and maintaining an ICT security strategy that addresses the security of Defence information system users;
 - b. contributing security expertise to the development and maintenance of an ICT security architecture; and
 - c. liaising with FAS S&VS and ESA's to ensure that information systems (personnel) security is integrated with broader protective security strategies, policies, and plans.

Information Technology Security Advisor (ITSA)

61. With regard to the information systems (personnel) security, the Defence ITSA is responsible for:
- a. liaising with ITSAs in other Australian Government agencies on matters relating to non-Defence personnel accessing Defence systems; and
 - b. reporting information systems security incidents to relevant stakeholders; and
 - c. responding to and remediating information systems (personnel) security incidents (under the direction of a Defence Investigative Authority) when a formal investigation is undertaken.

Information Technology Security Manager (ITSM)

62. With regard to the information systems (personnel) security, ITSMs are responsible for ensuring that:
- a. processes governing access to information systems under their control meet policy and security requirements;
 - b. formal process are used to grant access to information systems;
 - c. system access is disabled or revoked if a user no longer requires access, no longer meets access requirements or otherwise poses an unacceptable risk to information security;
 - d. accurate records of account creation, disabling/enabling and revocation are kept; and
 - e. user accounts properly identify system users.

Information Technology Security Officer (ITSO)

63. With regard to the information systems (personnel) security, ITSOs are responsible for:

- a. ensuring that all accounts created accurately reflect the nature of the associated users and that this is visible to all other users;
- b. ensuring that an account for a foreign national accurately reflects the person's correct nationality;
- c. ensuring that ITSMs are notified of any:
 - (1) erroneously created accounts; or
 - (2) ensuring that ITSMs are notified of any unauthorised accounts or inappropriate privilege assigned to authorised accounts;
- d. ensuring that, when necessary, accounts are disabled or revoked in a timely manner; and
- e. assisting commanders and managers, and contract managers to meet their responsibilities through:
 - (1) the provision of security advice;
 - (2) the provision of briefings and awareness material to staff; and
 - (3) verification of staff clearances.

System Owner

64. With regard to the information systems (personnel) security, system owners are responsible for ensuring that:

- a. systems are only accessed by people that meet all access requirements;
- b. the number of privileged user accounts is minimised;
- c. foreign nationals can only access information that is releasable to their nationality;
- d. systems are covered by suitable acceptable use policies; and
- e. any incidents involving unauthorised access to systems, networks or information are reported.

System Manager

65. With regard to the information systems (personnel) security, system managers are responsible for:
- a. implementing processes for the management of users as approved by the accreditation authority;
 - b. maintaining appropriate records of user access to systems;
 - c. monitoring the number of privileged user accounts;
 - d. ensuring that controls designed to enforce access control decisions are effective; and
 - e. reporting any incidents that are identified during the course of system management activities.

Accreditation Authority

66. With regard to the information systems (personnel) security, the accreditation authority is responsible for:
- a. considering levels of compliance with policy requirements and areas of deficiency as advised by the certifying authority;
 - b. applying for dispensations as required;
 - c. deciding whether or not to accept the residual risk of operating the system; and
 - d. ensuring that system security documentation includes suitable processes for controlling access to Defence systems and information in accordance with the requirements of this chapter.

Certification Authority

67. With regard to the information systems (personnel) security, certification authorities are responsible for:
- a. assessing privileged user security documentation governing user management for compliance with policy requirements as part of the certification process;
 - b. assessing security documentation governing the use of systems by standard users for compliance with policy requirements as part of the certification process;
 - c. assessing technical measures designed to control the actions of users (standard/privileged users, Australian citizens and foreign nationals etc.); and

- d. communicating levels of compliance with policy requirements and areas of deficiency to accreditation authorities.

Commander and Manager

68. With regard to the information systems (personnel) security, commanders and managers are responsible for:

- a. sponsoring system/network access requests, including verification of a user's clearance and need-to-know information processed by the system;
- b. ensuring that information submitted as part of a system/network access request is correct; and
- c. ensuring appropriate ICT controls are implemented to manage foreign national access to information in accordance with Control 19.1 – *Information Systems (Logical) Security* and the relevant foreign release approval.

Contract Manager

69. With regard to the information systems (personnel) security, contract managers are responsible for:

- a. sponsoring system/network access requests, including verification of a user's clearance and need-to-know information processed by the system; and
- b. ensuring that information submitted as part of a system/network access request is correct; and
- c. ensuring appropriate ICT controls are implemented to manage foreign national access to information in accordance with Control 19.1 – *Information Systems (Logical) Security* and the relevant foreign release approval.

System User

70. With regard to the information systems (personnel) security, System users are responsible for complying with the relevant policies, plans and procedures for the systems they are using. Specifically they are responsible for:

- a. ensuring that information provided as part of a system/network access request is correct;
- b. ensuring that unattended equipment is appropriately secured;
- c. enacting a clear desk and clear screen policy;
- d. not allowing others to use their identity or authentication credentials; and
- e. reporting any security incidents of which they become aware.

Privileged User

71. With regard to the information systems (personnel) security and in addition the responsibilities of system users, privileged users are also responsible for:
- only using privileged access only for those assigned system administration tasks which require it and not for routine or user level business as usual activities such as email or internet access; and
 - ensuring that authentication credentials associated with privileged accounts are adequately protected.

Key Definitions

72. **Standard User.** Person who only has basic system privileges and cannot make significant changes that affect other users or the operation of the system itself.
73. **Privileged User.** Person who is trusted to perform system administration tasks beyond those that can be performed by standard users. They may be able to alter system configuration, vary access control permissions for other users or access data not available to standard users.
74. **Non-Defence APS Employee.** These are APS employees of Australian government agencies other than Defence. For the purposes of this policy, if the employee is not an Australian citizen they are to be considered as a foreign national.
75. **Foreign National.** A person who is not an Australian citizen.
76. **Seconded Foreign National.** A foreign national who is authorised to act on behalf of the Australian Government or assigned to an ADF unit. See DSPF Principle 40 – *Personnel Security Clearance* for further information.
77. **Five Eyes Foreign National.** The Five Eyes consist of Australia, the United States, Canada, the United Kingdom and New Zealand. From an Australian perspective, a Five Eyes foreign national is a citizen of the United States, Canada, the United Kingdom or New Zealand.
78. **Non-Five Eyes Foreign National.** A non-Five Eyes foreign national is a foreign national that is not a citizen of Australia, the United States, Canada, the United Kingdom or New Zealand.
79. **Demilitarised Zone (DMZ).** A small network with one or more servers that is kept separate from the core network, either on the outside of the firewall, or as a separate network protected by the firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.

Further Definitions

80. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems (Personnel) Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 18.1
Version	3
Publication date	10 August 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems (Personnel) Security
Related DSPF Control(s)	Assessing and Protecting Official Information Information Systems (Logical) Security Mobility Device Security Identity Security Access Control Foreign Release of Official Information Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective marking update to align with the PSPF; update of language to reflect Defence Admin Policy;
3	10 August 2020	AS SPS	Update to include foreign release approval for official information in accordance with DSPF Control 15.1.



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Logical) Security

General principle

1. Defence will protect ICT systems and networks with logical security controls that are proportionate to the assessed risks, which are informed by confidentiality, integrity and availability business impacts applicable to the ICT asset.

Rationale

2. Information security (logical) systems and associated procedures provide assurance and protection to the confidentiality, integrity, and availability of systems and the information within them.

Expected outcomes

3. Defence personnel is to ensure appropriate permissions are received before providing third parties access to Defence ICT Systems and networks not originating from Defence. Defence and Defence industry ensure that appropriate security measures have been taken to protect official, sensitive, and classified Defence information from unauthorised use, access, or accidental modification, loss or release.;

4. Defence and Defence Industry only use Defence ICT systems and networks in a manner that is appropriate and in accordance with Principle 10 – *Assessing and Protecting Official Information*; and

5. Defence personnel is to ensure appropriate permissions are received before providing third parties access to Defence ICT Systems and networks not originating from Defence.

Escalation Thresholds

6. The ITSA has set the following general thresholds for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility	
	CIOG managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor NB: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive NB: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	v
Principle Owner	Chief Information Security Officer
DSPF Number	Principle 19
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 19.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	<u>PSPF core requirements:</u> Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems Legislation: Electronic Transactions Act 1999 Telecommunications (Interception and Access) Act 1979 Archives Act 1983 Standards: Australian Government Information Security Manual (ISM) Australian Defence Force Communications Instruction (ADFCI) 6.2.5 Radiocommunications Monitoring Procedures
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Security for Projects Information Systems (Physical) Security Information Systems (Personnel) Security Remote Access to Defence Systems Information Systems Log Management Offshore and Cloud Based Computing
Implementation Notes, Resources and Tools	<i>Australian Government Information Security Manual</i> – sets out the standard governing the security of Australian Government ICT systems: http://www.asd.gov.au/infosec/ism/index.htm

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Logical) Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Escalation Thresholds

2. The ITSA has set the following general thresholds for risks managed against this *Defence Security Principles Framework (DSPF) Enterprise-wide Control* and the related *DSPF Principle and Expected Outcomes*.

Risk Rating	Responsibility	
	CIOG managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor NB: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive NB: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Process

Information Systems (Logical) Security

3. Logical security controls are enforced by systems or automated processes which complement personnel and physical controls to ensure that the confidentiality, integrity, and availability of ICT systems and networks are protected using security-in-depth principles.

4. System Owners are to ensure that ICT systems implement all applicable controls specified in the DSPF, [Information Security Manual \(ISM\)](#), Australian Communications Security Instruction (ACSI) publications and relevant security instructions.
5. Systems are to be certified and accredited prior to use in accordance with Principle 23 – *ICT Certification and Accreditation*.

Identification, Authentication and Authorisation

Identification

6. Identification is the process of establishing the identity of a user or device, taking into account name, clearance, and nationality.
7. System Users **must** be uniquely identified prior to gaining access to an ICT system.

Note: Shared ICT systems or devices, such as pool laptops, may maintain a register of system users where shared accounts are implemented

Exclusion: Systems that are intended to allow public access do not need to uniquely identify individual system users prior to access. However, Privileged Users (e.g. system administrators) do need to be uniquely identified.

8. Systems that store, process or communicate information that requires protection based on nationality (for example, AUSTEO, AGAO, AUS/USA etc.) **must** be able to accurately differentiate between System Users of different nationalities. See applicable [ISM](#) controls 0409, 0411, and 0816.
9. Users **must not** be assigned to incorrect nationality groups in order to facilitate the creation of an account.
10. With regard to the identification of System Users, the following events are security incidents and **must** be reported in accordance with Control 24.1 – *Information Systems Security Incident Management*, Control 77.1 – *Security Incidents and Investigations* and, when applicable, Control 10.1 – *Assessing and Protecting Official Information*:
 - a. impersonation of another user, sharing authenticators or authentication credentials, shared use of a user account assigned to an individual or interactive login to a service account in order to bypass security restrictions placed upon an individual's user or privileged access account;
 - b. the incorrect assignment of a user to a nationality based group; and
 - c. fraudulent enrolment of an entity as a legitimate user (standard or privileged). This includes the provision of incorrect information as part of the user account provisioning process.

Authentication

11. Authentication is the process of verifying an established identity of a device or user. System Users can be authenticated by something they know (passwords, passphrases etc.), something they have (passes, tokens, etc.) or something they are (biometrics).

Requirement for authentication

12. Once identified, System Users **must** be authenticated using methods specified within the [ISM](#).

13. Information Communications and Technology (ICT) systems that are intended to allow public access do not need to authenticate individual system users prior to access. However, privileged users (e.g. system administrators) of these ICT systems do need to be authenticated.

14. Privileged remote access introduces a higher level of risk than is the case for standard users. [ISM](#) controls related to privileged access systems apply. Control 30.1 – *Remote Access to Defence Systems* contains guidance on information processing restrictions for system administrators using remote access.

Protection of authenticators

15. When using a single factor of authentication, authenticators are to be protected at the same level as the system or information to which they allow access.

Example: When a password is used as a single factor authenticator allowing access to a *SECRET* system, that password is to be classified 'SECRET'. As such, Defence ICT system users should use passwords on Defence ICT systems that are different to those used by them in a personal capacity.

16. When using multi-factor authentication:

- a. system security documentation **must** specify the protection required for each factor to be considered during system certification and accreditation; and
- b. users must be informed of how they are to protect authenticators.

17. The compromise of an authenticator is a security incident and is to be reported in accordance with Principle 77 – *Security Incidents and Investigations*.

18. Systems **must** not store passwords in a clear text (unencrypted) form.

19. The Identification and Authentication section of the [ISM](#) specifies additional requirements for the use and protection of authenticators.

Password resets

20. System Owners are to ensure that all ICT system users are positively identified prior to resetting their network password. Most user names are predictable and are not to be considered as an authenticator for the purposes of access control or password reset mechanisms.

21. Positive identification for network passwords can be performed by an accredited electronic password reset tool. The tool:

- a. must enforce password length and complexity requirements (including any prohibitions on password reuse) as specified in the [ISM](#);
- b. must positively identify the individual before resetting a password; and
- c. should not provide an existing, clear text password to the user.

Authorisation

22. Authorisation control refers to determining and enforcing what an identified, authenticated user or device can do.

23. System security documentation should include plans for the testing of permissions and other access control mechanisms.

24. It is recommended that the test plan:

- a. identifies the controls to be tested;

Example: A system that uses technical controls to prevent foreign nationals from accessing AUSTEO material should include scenarios to test the effectiveness of those controls.

- b. Specifies the frequency of control testing; and

Example: Controls protecting AUSTEO information may need to be tested in preparation for a regular exercise involving foreign nationals.

- c. is considered during certification and accreditation.

25. The exposure of information to an unauthorised user, whether through failure or circumvention of a control, or the inappropriate granting of authorisation is a security incident and must be reported in accordance with:

- a. Control 24.1 – *Information Systems Security Incident Management*;
- b. Principle 10 – *Assessing and Protecting Official Information*; and
- c. Principle 77 – *Security Incidents and Investigations*.

Encryption

26. Encryption can reduce the handling and transmission security requirements of information and systems. This reduction only applies when the information is in its encrypted state. At any point in which the information is in an unencrypted state, its 'handle as' Protective Marking is to be equal to its actual Protective Marking or confidentiality BIL.
27. There are two type of encryption, encryptions at rest and encryption in transit.
28. **Encryption at rest** refers to the act of encrypting stored information. Encryption can be used to protect the confidentiality and possibly the integrity of information. However, it does not protect the availability of information.
29. **Encryption in transit** refers to the act of encrypting information during transmission or communication, protecting information against interception (loss of confidentiality), modification or fabrication (loss of integrity) during communication.
- Encryption in transit encryption does not provide protection against interruption or destruction (loss of availability).
 - In transit encryption can impede the legitimate inspection of network traffic by gateway systems or antivirus software.
 - Defence information which is encrypted during transmission must be encrypted in accordance with the requirements of the [ISM](#) and the ACSI series.
30. The effect of encryption on the 'handle as' Protective Marking of electronic storage media is shown in the table below. This only applies when the information is in its encrypted form.

Table 1: 'Handle as' Protective Marking

Encryption Status	'Handle as' Protective Marking
Media not encrypted.	is equal to actual Protective Marking.
Media encrypted – but not in accordance with ISM and ACSI standards.	is equal to actual Protective Marking.
Media encrypted in accordance with ISM and ACSI standards.	can be lower than actual Protective Marker. Degree of reduction depends on actual Protective Marking and type of encryption (see ISM for further information)

Public Key Infrastructure (PKI)

31. The Defence PKI is the main Defence Certificate Authority. It is managed by CIOG and is Australian Government compliant. Digital certificates issued by the Defence Public Key Infrastructure (PKI) meet the requirements of the [Electronic Transactions Act 1999](#), the *Electronic Recordkeeping Guidelines* issued by the National Archives of Australia and the *Financial Management and Accountability Regulations 1997* (FMA Regulations 7 to 12) as an appropriate method for digital signature and are authorised for use to sign Defence documentation.

32. Any digital certificate used to identify a transaction or resource at SECRET and below **must** be issued by the Defence PKI. The use of digital certificates issued by any other Certificate Authorities (internal or external to Defence) to identify a Defence transaction or resource requires a dispensation to be sought and granted from the Control Owner prior to use.

33. All digital certificates issued by Certificate Authorities other than the Defence PKI (including certificates issued by external entities) must only be used for those purposes approved by the Defence Public Key Infrastructure Policy Board (DPKIPB).

Example: DPKIPB may approve a PKI service for internal Defence usage as part of a weapon system. Certificates issued under this service would not meet Australian Government requirements and therefore cannot be used for financial transactions with external entities. They can only be used for the purposes for which they have been issued.

34. Refer also to Control 13.1 – *ICT Communications Security (COMSEC)* for policy on ICT Communications security within the single information environment (SIE).

System Integrity

System baseline

35. It is recommended that system managers maintain a 'known good' baseline of a system which is verified through the use of hashes or checksums. This will aid in the detection of, and recovery from, any incident affecting the integrity of the system.

Malicious code

36. System Owners are to protect systems against malicious code through the implementation of logical security controls specified in the DSPF, [ISM](#) and the [Australian Signals Directorate \(ASD\) Strategies to Mitigate Cyber Security Incidents](#).

Publicly available systems

37. Defence and Defence Industry ICT systems that are intended to be accessed by members of the public are to implement measures to protect the confidentiality, integrity and availability of the system and its information.

38. System Owners are to protect web servers and applications in accordance with the [ISM](#).
39. System Owners are to securely design, configure and harden web servers. The use of commercial web development standards and design patterns are recommended as good security practice that can further reduce risk.
40. System Owners should build web based systems in accordance with:
- any applicable Defence ICT security architecture;
 - the Open Web Application Security Project (OWASP) framework; and
 - the '[Protecting Web Applications and Users](#)' technical guidance published by ASD.

System utilities

41. In order to apply the 'principle of least privilege', System Users should be prevented from using system utilities that they are not authorised to use.
42. System utilities may include:
- network discovery and mapping tools;
 - packet capture tools; or
 - password auditing tools.
43. Standard System Users should not have access to system utilities that can affect the configuration of a system.
44. Privileged Users should only have access to utilities necessary for them to perform their assigned administrative tasks. Access to other tools should be prevented.

Example: A Privileged User responsible for the management of disk storage arrays should not be able to use network discovery tools unless this is necessary for the management of the storage array.

System Monitoring

45. All information (including personal data and emails) created, processed, transmitted or stored on Defence ICT systems is the property of the Australian Government and is subject to Commonwealth legislation, including audit by designated authorities. Stored data will be accessed, copied, deleted or disclosed, as required by legislation or regulation, or as the Australian Government deems appropriate. The [Telecommunications \(Interception and Access\) Act 1979](#) governs the extent of monitoring of ICT systems within Defence.

Appropriate Usage

46. All System Users are responsible for protecting the access rights they have been provided and only using those rights in the appropriate or approved manner.
47. Defence personnel are not to make unauthorised changes to Defence ICT resources within the SIE. This includes, but is not limited to, the connection of unapproved devices or the installation of unapproved software.

COMSEC monitoring

48. Australian Defence Force Communications Instruction (ADCI) 6.2.5 Radiocommunications Monitoring Procedures provides guidance on legislative and policy issues relevant to the conduct of ethical and appropriate communications security (COMSEC) monitoring of Defence systems by the Australian Defence Force (ADF). COMSEC monitoring is the act of reviewing friendly transmissions in order to assess the degree of security afforded to them.
49. Refer to Control 13.1 – *ICT Communications Security (COMSEC)* for policy on COMSEC monitoring.

Activity monitoring

50. ICT systems **must** be monitored in order to identify unauthorised activity.
51. If it is not feasible to log all system events:
- the activities of privileged users must be logged;
 - other logging should be prioritised according to a risk assessment; and

Example: A risk assessment may identify a profile of a user or device type that represents an increased risk. The actions of users in that profile group might therefore be considered a higher priority for log collection.

- Activity logs should be stored independently of the system being monitored.
52. Activity logs should be time stamped using an agreed accurate time source. Any known inaccuracies in, or corrections to, the time source **must** be documented.
53. Activity logs must be protected against disclosure, modification, fabrication and destruction and preserved in accordance with the [Archives Act 1983](#).
54. System Users that are the subject of log entries **must not** be able to delete, destroy or modify logs.
55. Any legitimate activity that affects the integrity or availability of logs is to be formally approved and documented.
56. Any unauthorised modification or destruction of system log files is a security incident and **must** be reported in accordance with the DSPF.

57. For specific information on ICT Security log management requirements within the SIE refer to Control 28 – *Information Systems Log Management*.

Intrusion prevention and detection

58. Defence ICT systems (including networks) are to be monitored by IDS/IPS systems in accordance with the [ISM](#).

System Availability

59. System Owners are to implement availability controls suitable to address assessed risks as informed by a system BIL.

Backup

60. Backup and restore processes **must** be included in system documentation and considered during certification and accreditation.

61. Backup and restore processes **must** be tested to verify that the process is sufficient to ensure the availability and integrity of the system and data in the event that restoration is required.

62. It is recommended that backups are kept separately from the system to ensure that an attack or failure does not affect the availability of the backup as well as the system.

***Example:** A system using an offline backup mechanism could be restored after a piece of 'ransomware' maliciously encrypts data in order to extort money from the victim.*

Cross Domain Security

Domain boundaries

63. System Owners **must** define and document the security domain boundaries of systems for which they are responsible. In most cases this will assist in defining the scope of documented security activities.

64. System security domain boundaries **must** be:

- a. specified in system documentation;
- b. considered as part of the certification and accreditation processes; and
- c. reviewed in accordance with any changes to the system or its environment.

65. Any information or program code traversing security domain boundaries must be controlled in accordance with the [ISM](#) cross domain security controls.

Use of virtualisation

66. The use of virtualisation does not provide any intrinsic degree of cross domain security. Virtualised systems within different security domains can be connected via an accredited Cross Domain Solution (CDS), just as for any other system. However, the virtualisation itself is not considered as a means of separating security domains. [ISM](#) Controls relating to functional separation of servers apply.

Access to the Internet

67. System Owners, or commanders and managers, must ensure that access to the Internet is via:

- a. an accredited gateway such as a High Availability Internet Gateway Service (HAIGS) for the DPN; or
- b. a standalone 'OFFICIAL' computer connected to an Internet Service Provider (ISP) via an authorised connection. Accreditation is not required, however, local management, in conjunction with Defence Voice Services, is responsible for administering the connection.
 - (1) If the connection is located in a 'TOP SECRET' area the 'TOP SECRET' accreditation authority must approve the connection as other systems may be affected.
 - (2) Commanders and managers may apply local use provisions in addition to Defence wide acceptable use policies.

68. System Users must not use Defence systems to access personal email or cloud services unless the system has been specifically approved by the System Owner for that purpose and accredited to provide assurance that all applicable security controls are met.

69. Personal email and cloud based storage may be accessed from Defence premises using personal devices that are not connected in any way to Defence systems provided that the requirements of Control 22.1 – *Portable ICT Asset (including Mobile devices)* are met.

Gateway and firewall connections to the Single Information Environment (SIE)

70. System Owners and coordinating capability managers responsible for networks and systems connected to the SIE via gateways or firewalls are to support CIOG, as the manager of the SIE, by providing visibility of any device or network connected through that gateway or firewall.

71. System Owners of any Defence or Defence industry network that connects to the SIE **must** configure their gateway or firewall to enable CIOG management systems to traverse the gateway to provide:

- a. visibility of connected networks and devices;
- b. event monitoring services; and
- c. the ability to confirm compliance with ICT security policy.

Data transfers

72. This section applies to any transfer of information between systems through means other than existing, accredited network connections. Data transfers of information between systems through means other than existing, accredited network connections, whether they are within the same security domain or across domain boundaries, **must** be approved and controlled. Data transfers within a security domain introduce some level of risk such as:

- a. the use of unapproved storage media from outside the security domain introducing associated malware risks; and
- b. poor handling practices involving storage media.

Example: *Unauthorised use of a data transfer device between different systems.*

73. Data transfers across security domain boundaries generally represent a higher risk than transfers within a domain and therefore require more stringent control.

74. Data transfers **must** only occur in accordance with approved processes that are:

- a. in accordance with the requirements in Control 22.1 – *Portable ICT Asset (including Mobile devices)*;
- b. in accordance with the requirements in the [ISM](#) Data Transfers and Media Security sections; and
- c. specified in system documentation and considered during the certification and accreditation processes.

Exclusion: *for systems that do not require accreditation in accordance with Control 23.1 – ICT Certification and Accreditation, data transfer processes are to be approved by System Managers.*

75. For specific information on data transfer requirements within the SIE, refer to Control 27 – *Information Systems Data Transfer Security*.

Data spills

76. A data spill occurs when information traverses security domains by unauthorised means. In most cases this involves information moving from one system to another that is accredited at a lower security classification.

Example: A 'SECRET' document is copied from the Defence Secret Environment (DSE), a 'SECRET' high domain to the Defence Protected Environment (DPE), a 'PROTECTED' high domain.

77. A data spill can also occur when information traverses security domains within the same classification.

Example: A 'SECRET AUSTEO' document is exposed to foreign national users by being copied from an 'AUSTEO' accredited 'SECRET' network to one that not accredited for 'AUSTEO'.

78. Data spills involving Foreign Government Information (FGI) must be reported in accordance with Principle 15 – *Foreign Release of Official Information*.

79. Other data spills are to be reported in accordance with Control 24.1 – *Information Systems Security Incident Management* and Principle 77 – *Security Incidents and Investigations*.

Remote Access

80. When Defence ICT systems implement remote access capabilities, this functionality **must** be documented and considered as part of the certification and accreditation processes. During this process, the following factors are to be considered:

- a. the use of the remote access capability from overseas;
- b. encryption required to protect information in transit;
- c. end-point hardening;
- d. persistence of information on remote end points and any relevant requirements for encryption at rest;
- e. procedural controls governing when and where remote end-points can be used; and
- f. any cascading network connections introduced by the end-point.

81. In addition to any encryption and end-point security requirements, remote access solutions are to be implemented in accordance with the Remote Access section of the [ISM](#).

82. See Principle 30 – *Remote Access to Defence Systems* for further information on the approvals and use of remote access systems.

Roles and Responsibilities

Chief Information Officer (CIO)

83. With regard to information systems (logical) security, the Chief Information Officer (CIO) is responsible for ensuring appropriate logical security controls are implemented within the SIE.

Chief Information Security Officer (CISO)

84. With regard to information systems (logical) security, Chief Information Security Officer (CISO) is responsible for:

- a. contributing security expertise to the development and maintenance of ICT security architecture;
- b. maintaining an effective ICT certification and accreditation framework for Defence and Defence industry in accordance with Government expectations, Defence policy and the Defence ICT security strategy; and
- c. liaising with First Assistant Secretary Security and Vetting Service (FAS S&VS) and Executive Security Advisors (ESA) to ensure that ICT system security is integrated with broader protective security strategies, policies and plans.

Information Technology Security Adviser (ITSA)

85. With regard to information systems (logical) security, the Information Technology Security Adviser (ITSA) is responsible for:

- a. coordinating ICT certification functions to a standard that meets Government expectations; and
- b. liaising with ITSAs in other agencies on technical ICT security matters.

Information Technology Security Manager (ITSM)

86. With regard to information systems (logical) security, the Information Technology Security Manager (ITSM) is responsible for:

- a. managing the implementation of ICT security policies and procedures for ICT systems;
- b. improving the security of ICT systems;
- c. coordinating or conducting periodic ICT security vulnerability and risk assessments of ICT environments;

- d. ensuring the periodic testing of the effectiveness of controls implemented for ICT systems;
- e. conducting periodic security evaluations of ICT systems, including an evaluation of configuration changes made to ICT systems;
- f. ensuring that ICT security incidents are managed and reported in accordance with Principle 77 – *Security Incidents and Investigations*.
- g. overseeing the development, maintenance and implementation of ICT system operating procedures; and
- h. providing technical support to reviews on the effectiveness of ICT system security capabilities.

Information Technology Security Officer (ITSO)

87. With regard to information systems (logical) security, the Information Technology Security Officer (ITSO) is responsible for:

- a. implementation and maintenance of ICT system security controls;
- b. reporting to ITSM any vulnerabilities detected through the course of their duties;
- c. reporting to ITSM any controls that are ineffective or incomplete; and
- d. reporting any security incidents detected through the course of their duties.

Business Owner

88. With regard to information systems (logical) security, Business Owners are responsible for:

- a. identifying the business requirement for an ICT system to the System Owner; and
- b. advising the System Owner and accreditation authority of the intended use of the system and the BIL assigned to the ICT system and its information.

System Owner

89. With regard to information systems (logical) security, the System Owner is responsible for:

- a. ensuring their ICT systems are built, operated and maintained in accordance with the [ISM](#), DSPF, the ACSI suite of publications and other relevant security instructions;

- b. ensuring appropriate security measures and controls are implemented for ICT systems under their responsibility to ensure risks to the confidentiality, integrity or availability of those ICT systems and their information are managed appropriately;
- c. ensuring threats and vulnerabilities arising from the operation of ICT systems under their responsibility are appropriately managed and mitigated.
- d. ensuring that system SOP are developed and maintained in accordance with applicable security policies and ICT system certification and accreditation requirements;
- e. ensuring that SOP are available to relevant parties (e.g. user SOP are available to standard ICT System Users, System Administration SOP are available to Privileged Users etc.); and
- f. ensuring a system ITSO is appointed for each ICT system under their responsibility.

Certification Authority

90. With regard to the logical security of information systems, Certification Authorities are responsible for:

- a. assessing the controls implemented for an information system against applicable minimum standards (DSPF, [ISM](#) and ACSI series of documents) and relevant policies;
- b. assessing the validity of any proposed control variations;
- c. identifying the need for dispensations where policy requirements cannot be met and communicating this to System Owners; and
- d. providing specialist advice to enable System Owners to develop any required dispensations.

Accreditation Authority

91. With regard to information systems (logical) security, Accreditation Authorities are responsible for ensuring that security requirements have been addressed through:

- a. the correct application of appropriate controls or ensuring that dispensations have been requested and approved by the appropriate authority; and
- b. deciding whether or not to accept any residual risks within their authority.

Commander and Manager

92. With regard to information systems (logical) security under the management of a single, discrete unit, commanders and managers assume the responsibilities of both the business owner and the system owner and are responsible for appointing a system ITSM and ITSO.

93. Commanders and managers may authorise the disposal of hardware products, or waste relating to these ICT systems into the public domain in accordance with the requirements specified in the [ISM](#).

94. If the system provides services to other client units, the commander or manager of the unit providing the ICT system will ensure that client units adhere to system SOP.

95. With regard to ICT systems used, but not managed by a unit, Commanders and Managers are responsible for ensuring that Defence and Defence industry personnel or entities under their management adhere to all applicable security policies, procedures and requirements relating to the ICT system being used.

Contract Manager

96. With regard to information systems (logical) security, Contract Managers are responsible for ensuring that Official Information provided electronically to industry or external entities is stored, processed and communicated by ICT systems accredited to the classification of the Official Information being provided.

System Users

97. System Users of ICT systems within the SIE are responsible for:

- a. complying with the relevant plans, policies and procedures for the ICT systems they are using;
- b. only using their own accounts;
- c. using passwords or passphrases that comply with [ISM](#) complexity requirements;
- d. ensuring authentication credentials (such as passwords, smartcards and tokens) are not provided to any other person or entity;
- e. ensuring their own account or identity is not used by any other person or entity. This includes locking computers before leaving them unattended and protecting authenticators;

- f. protecting ICT system resources, components, devices and information from unauthorised access, use, disclosure, disruption, modification, or destruction. This includes implementing the clear desk policy and adhering to any applicable storage, handling and operating requirements for ICT systems, information, media and devices being used; and
- g. reporting any suspected or actual security incidents of which they become aware and supporting any investigation by complying with directions given by a Defence Investigative Authority or other authorised entity.

Privileged Users

98. In addition to their responsibilities as a system user, Privileged Users are responsible for:

- a. only making authorised changes to ICT systems;
- b. not making unauthorised changes to their level of privilege;
- c. using privileged access only to perform authorised system administration tasks which require elevated privileges and not for routine or business as usual activities that can be performed on a standard System User account, such as email or internet access; and
- d. ensuring that ICT security incidents are managed and reported in accordance with Principle 77 – *Security Incidents and Investigations*.

Key Definitions

99. **Asset custodian.** A commander or manager responsible for the protection of an asset upon issue to them.

100. **Auditing.** The analysis of logged events in order to identify or investigate anomalies.

101. **Authentication.** The process of verifying the identity of a user or device.

102. **Authenticator.** An artefact that is used to verify the identity of a user or device. An authenticator may act as a single factor of authentication or be one part a multi-factor scheme. A password is an example of an authenticator.

103. **Authorisation.** The determination of what an identified and authenticated entity is allowed to do.

104. **Access control (logical).** The mechanisms used to enforce authentication and authorisation decisions.

105. **Identification.** Establishing who a user claims to be or what a device claims to be.

106. **Logging.** The collection of information about system events.
107. **Logical (security) control.** A technical control enforced by system or automated process as opposed to a physical or procedural control.
108. **Principle of least privilege.** Ensures Privileged Users are only given the privileges and tools necessary to perform their authorised tasks.
109. **Public key infrastructure (PKI).** An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for Department of Defence functional enterprise programs, including generation, production, distribution, control, and accounting of public key certificates. A PKI provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable certification authority.
110. **Remote access.** User access to agency systems originating outside an agency network. It does not include web-based access to DMZ resources.
111. **System utilities.** Software tools used to perform system administration, configuration and management activities. In most cases they are used by system administrators to control or monitor various aspects of system behaviour.

Further Definitions

112. Further definitions for common DSPF terms can be found in the Glossary.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document administration

Identification

DSPF Control	Information Systems (Logical) Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 19.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principles and Expected Outcomes	Principle 20
Related DSPF Control(s)	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Lifecycle Management

General principle

1. The security of Defence information systems will be managed throughout all stages of the system's lifecycle.

Rationale

2. Defence depends on its Information and Communications Technology (ICT) to deliver vital services in support of military operations and Defence business. Risks to Defence ICT systems can arise at a number of points throughout the lifecycle of a system, from design or acquisition, through development or operational usage, to decommissioning and disposal. The most effective use of security resources is achieved by considering security risks from the earliest stages of the system lifecycle.

Expected outcomes

3. All internally developed and commercially obtained systems address security requirements as part of their systems lifecycle.
4. Security is considered from the earliest stages of system development.
5. Systems are designed, built, managed and decommissioned in accordance with the Australian Government Information Security Manual (ISM) and relevant ISO standards.
6. Defence appoints a System Sponsor and System Owner for all production systems and they maintain an awareness of the system, security boundaries, and residual security risks for the systems which they are responsible for.
7. Defence, specifically the system owners across the members of the Groups and Services, who have responsibility for the ICT systems throughout the system lifecycle, understand its information assets and maintain an inventory of the systems on which they reside.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor. Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems Lifecycle Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 20
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 20.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Protective marking of information; Ongoing assessment of personnel; and Entity facilities Australian Government Information Security Manual (ISM) <u>Legislation:</u> Privacy Act 1988
Read in conjunction with	N/A
See also DSPF Principle(s)	Security for Projects Security for Capability Planning Defence Industry Security Program Information Systems (Physical) Security Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Log Management Information Systems Vulnerability and Patch Management Security Remote Access to Defence Systems
Implementation Notes, Resources and Tools	Australian Government information security management guidelines – Australian Government Security Classification System – provides guidance to assist agencies to identify the value of information and, in turn, apply a suitable protective marking. Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material – provides guidance on procedures for applying protective markings and information handling procedures. Australian Government Information Security Manual (ISM) – sets out the standard governing the security of Australian Government ICT systems.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Lifecycle Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The ITSA has set the following general threshold for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Group or Service Cyber Security Adviser Note: In the event that an appointment of a Group or Service Cyber Security Adviser has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Controls

System Planning

3. Defence and Defence Industry with responsibilities for projects within the Single Information Environment (SIE) are to implement approved measures to protect Official Information and resources in accordance with the classification of project information, systems and associated security risks. See DSPF Principle 10 – *Assessing and Protecting Official Information* and DSPF Principle 11 – *Security for Projects*.

4. The development and introduction of new ICT systems is to be planned in accordance with:
 - a. Business Impact Levels (BILs);
 - b. the [Essential 8 ASD Strategies to Mitigate Targeted Cyber Intrusions](#) (the top 4 of which are mandatory); and
 - c. applicable security architecture.

Planning and Design

5. Security is to be a fundamental consideration from the earliest stages of system planning and design. According to the PSPF 11 Robust ICT systems, core requirements of Defence must be to have in place security measures during all stages of ICT systems development. This includes certification and accreditation of ICT systems according with DSPF Principle 23 – *ICT Certification and Accreditation* when implemented into the production environment.
6. All Defence systems shall have a System Sponsor and a System Owner identified and documented who fully understand their security responsibilities for the systems they are responsible for. According to the PSPF 11 Robust ICT systems, Defence must develop a security risk management plan.
7. The security risk management plan must also include an assessment of the procurement of the ICT/Cyber products and services supply chain, for the life cycle of the system.

Supply Chain Risk Management

8. An important element of the Information Systems lifecycle management is the protection of the procurement supply chain from potential risk
9. In order to assess the security risk posed by the product (including product development) or service that is being procured by Defence, or Defence Industry, all ICT/Cyber procurement activities must be carried out in accordance with the CIOG Risk Management Guide for ICT Procurement.
10. As part of ICT/Cyber Procurement Supply Chain Risk Management (SCRM), the following must be undertaken:
 - a. An SCRM assessment which will include the following:
 - (1) a Vendor Assurance Assessment; and
 - (2) a Product (hardware or software) Service Evaluation.
 - b. The outcomes of those assessments/evaluations will be utilised to understand the potential SCRM risk the Vendor and their Product or Service will bring for the specific procurement being undertaking.

- c. The SCRM assessment must cover the potential supply chain risk the Vendor, and their Product or Service, will bring for the specific procurement being undertaken, and cover the Product or Service through its lifecycle within Defence including; initial purchase, through sustainment and into disposal.
11. The risk assessment must look at the procurement activity over the systems development life cycle (SDLC) and will feed into a number of other security activities outside of procurement and product selection, including:
- a. the BIL assessment; and
 - b. the certification and accreditation activity for the system.

Note: A Procurement Supply Chain Risk Management Framework is currently being developed and will be implemented in the near future. Until completion of the Procurement Supply Chain Risk Management Framework, continue to refer to the CIOG Risk Management Guide for ICT Procurement.

12. A core requirement for ensuring sound Information & Communications Technology (ICT)/Cyber system security is the robustness of the ICT supply chain. On this basis, all ICT hardware and/or software, including ICT infrastructure as a service or other cloud based service procurement within the Department of Defence must comply with contemporary Australian Government and Defence procurement and financial processes.

13. The ICT is defined as any technology that allows for the processing, storing or communication of information. This includes but is not limited to; networking equipment, computers, servers, mobile devices, software and cloud based service. By definition, ICT may form part of a greater system such as weapons, sensors or industrial control systems. Regardless of the final application, it is financially and commercially prudent that the procurement of all ICT hardware and/or software, including ICT infrastructure as a service or other cloud based service in the Department of Defence be centrally managed and coordinated. Principally, all Defence ICT hardware and/or software, including ICT infrastructure as a service or other cloud based service procurements must be made through CIOG, using CIOG commercial mechanisms and arrangements.

Assessment of Business Impact Levels (BILs)

14. System Sponsors are to assess the confidentiality, integrity and availability of information applies to BILs, as well as reputational risk. These should be communicated to the System Owner, who will also consider BILs specified by any other key stakeholders.

Protection of Design Documentation

15. System design information and documentation must be afforded protection in accordance with its Protective Marking, caveats and any associated BIL. Please refer DSPF Principle 10 – *Assessing and Protecting Official Information*, Consideration is to be given to a number of factors, including:

- a. the degree to which the information could highlight a vulnerability or facilitate an attack on the system (or related systems);
- b. commercial sensitivity;
- c. the impact of unauthorised modification to system documentation; and
- d. the impact that the loss or destruction of the information would have on the ability to operate and maintain the system.

Standalone Networks

16. Standalone networks (those not connected to Defence major fixed networks) increase the complexity of managing the security of Defence ICT infrastructure. The business need for a standalone network is to be weighed against the additional complexity of security management. CIOG is responsible for the policy and the approval of standalone networks a list of Accreditation Authority for ICT systems within Defence is at DSPF Principle 23 – *ICT Certification and Accreditation*.

Planning for Certification and Accreditation

17. System Owners are to identify the appropriate Certification Authority for each new system.

18. It is recommended that System Owners engage with the appropriate Certification Authority from the earliest stages of system development planning.

19. System Owners are to communicate the assessed and agreed system BIL to the Certification Authority.

20. It is recommended that System Owners identify any specific characteristics of the system that are likely to impact on certification and accreditation and discuss these with the Certification Authority at the earliest possible point. Examples might include:

- a. requirements for the system to store, process or communicate foreign government and/or caveat or code-word information;
- b. any intention to host foreign nationals on the system; and
- c. any use of Industrial Control Systems (ICS) (Supervisory and Data Acquisition (SCADA), Programmable Logical Controllers (PLC) etc.

Physical Context

21. The threat environment and degree of physical protection applied to a system can have a significant impact on the system's risk profile. Considerations may include:

- a. where the information/data will physically reside;
- b. where the system is to be deployed (including those integrated into vehicles and platforms);
- c. if the system is located within a mission; consulate; embassy or high commission overseas;
- d. if the system is outsourced or located within a contractor facility;
- e. if the system is in a space accessible by the public; Defence must not expose the public to unnecessary cyber security risks when they transact online
- f. if the system is not supported by trusted supply chains;
- g. if the system supports remote access; and
- h. if the system references operational BILs and Zones. Please refer to Annex A of this policy.

22. DSPF Principle 30 – *Remote Access to Defence Systems* should be considered when managing the lifecycle of a system.

23. In some cases availability controls and the infrastructure used may affect risks to confidentiality or integrity. Physical certification and accreditation requirements are specified in DSPF Principle 23 – *ICT Certification and Accreditation*.

Example: Data backups greatly reduce risks to availability, but may increase the risks to confidentiality if appropriate controls are not in place to protect backup media from theft or inappropriate access.

24. Service providers' systems that are used to provide information technology services, including outsourced cloud services, must be accredited prior to handling government information. Refer DSPF Principle 21 – *Offshore and Cloud Based Computing* and DSPF Principle 23 – *ICT Certification and Accreditation*.

System Procurement

25. Responsibility for security risks cannot be outsourced and are to remain with the Group or Service responsible for the procurement.

26. All system procurement activities must be carried out in accordance with the CIOG Risk Management Guide for ICT Procurement, as well as all relevant financial and contractual guidelines set down by Defence.

27. Where a Group or Service relies on an exception to this requirement as described within FINMAN2, the Sponsor must record their decision and the rationale within the AE643 – Defence Purchasing, and the suite of system security documentation.

28. CIO (or approved delegate) must approve any commitment of funds for procurement of any ICT hardware and/or software, including ICT infrastructure as a service or other cloud delivery models, in accordance with FINMAN2.

29. All ICT systems, hardware and software (including those acquired without specific CIO approval) must be assessed and approved by the CIO before being introduced into the SIE.

30. Contract Managers are to ensure that entities to which Defence has either granted access, or entrusted with Official Information or assets, take appropriate precautions to safeguard the information or assets.

31. Internally developed, and commercially obtained systems, are to address security requirements as part of their:

- a. initial design;
- b. development;
- c. testing; and
- d. during future reviews and updates.

32. Procurement officers and Contract Managers are to manage the security risks that result from allowing persons engaged under contract, and their subcontractors, access to Defence systems, applications, and Official Information, facilities and equipment. See DSPF Principle 11 – *Security for Projects* and DSPF Principle 12 – *Security for Capability Planning*.

Defence Contracts and Procurement

33. Defence is to document requirements for information security when entering into outsourcing contracts and arrangements with persons engaged under contract. Refer DSPF Principle 21 – *Offshore and Cloud Based Computing*.

34. All system procurement activities must be carried out in accordance with the CIOG Risk Management Guide for ICT Procurement, as well as all relevant financial and contractual guidelines set down by Defence. System procurement activities are to be approved by the relevant risk owner. Any use of third party untrusted suppliers (including the use of second-hand equipment) **must** be ICT Security risk assessed

and approved by the System Owner before procurement and being introduced into the SIE.

Example: If a procurement activity is 'OFFICIAL' and has been assessed as low risk through a Security Risk Assessment, then the Defence procurement officer can approve the ICT Security risk assessment of the procurement activity, rather than the System Owner.

35. Security risks cannot be outsourced or transferred to Defence Industry.

Product Selection

36. When acquiring products with security features, the acquisition must comply with the processes outlined in the [ISM](#) Product Selection sections, in addition to the following:

- a. the ICT/Cyber Procurement SCRM Framework;
- b. the Defence Approved Hardware List (DAHL); and
- c. the Defence Approved Software Library (DASL).

37. If a product providing lower security functionality is selected over one that offers higher security functionality, the decision maker is to be aware of the mandated requirements, possible alternatives and the basis for the decision. The associated risk is to be documented.

38. When selecting secure products for their own use, Defence Industry is to apply the Product Selection section of the [ISM](#) and to review both the DAHL and DASL.

Equipment Manager Appointment

39. An Equipment Manager is to be appointed if an ICT capability is purchased under a Defence wide support contract and is:

- a. evaluated under the Evaluated Products List (EPL);
- b. a Common Criteria Recognition Arrangement; or
- c. a High Assurance Product (HAP).

Note: These categories are further explained in the [ISM](#). Hardware that implements these features will have specific ISM requirements and security measures.

Exclusion: Where HAP is a Controlled Cryptographic Item (CCI) or implements key material eligible for the CRYPTO caveat then DSPF Principle 13 – Communications Security (COMSEC) is the authoritative policy.

40. The Equipment Manager is to develop a through-life support plan covering at a minimum:

- a. initial purchase arrangements, including adherence to all requirements of the ISM and any security processes identified in ACSC product specific advice and publications;
- b. Ensure that the products and services procured are in accordance with the ICT/Cyber Procurement Supply Chain Risk Management Framework;

Note: Where secure products apply, issues such as confirming anti-tamper mechanisms on receipt will need to be addressed. ACSC provides an analysis of security issues that will need to be followed in the product's evaluation, its documentation, and other product specific advice. Additionally, CIOG ICT security will also carry out its own risk assessment.

- c. vulnerability and patch management guidance for which can be found in the DSPF Principle 29 – *Information Systems Vulnerability and Patch Management Security*;
- d. a Key Management Plan (KMP) and other cryptographic considerations (in accordance with ACSC product advice);
- e. asset tracking and accountability procedures;
- f. maintenance arrangements including minimum personnel security requirements for individuals conducting maintenance activities; and
- g. a device recall and disposal plan to ensure secure remediation or disposal when:
 - (1) the capability reaches its planned end of life;
 - (2) devices become obsolete prior their planned end of life; or
 - (3) a critical vulnerability is discovered.

System Development

System Security Documentation

41. Systems are to have relevant authorised security instructions as detailed in the ISM. Larger, complex systems may require multiple sets of documentation addressing specific aspects of the system.

Example: In order to keep documentation manageable, a large network may have separate document sets for infrastructure, operating systems, account directories etc.

42. Further guidance for certification / accreditation can be found in DSPF Principle 23 – *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*.

Separation of Development, Test and Production Environments

43. Separate, isolated environments should be created for development, test and operational lifecycle phases.

44. Development and test environments are required to be accredited if any sensitive or classified hardware, software or information is present in the environment.

Example: A system uses off-the-shelf hardware and software. However, firmware settings contain sensitive information and require protection.

45. When accrediting a test or development environment, it is recommended that the following topics are considered during certification:

- a. the presence of development tools and utilities not normally present in a production environment;
- b. the volatility of the development environment. Development and test environments may be subject to frequent configuration changes;
- c. the degree of hardening and patching applied to the development or test environment as opposed to the production environment;
- d. network connectivity; and
- e. data transfers to, and from, the test environment.

Physical Security during System Development

46. Systems are to be afforded adequate physical protection during each stage of development, in accordance with DSPF Principle 18 – *Information Systems (Personnel) Security*. These requirements must be documented in system development plans.

Security of Source Code

47. System security documentation and plans must identify the confidentiality, integrity and availability requirements for specific classes of source code and enact suitable protective measures.

48. A software system may be built from source code with varying levels of confidentiality requirements. Source code may be:

- a. sensitive in its own right, e.g. the algorithm employed may be sensitive or classified;
- b. publicly available, e.g. standard code libraries that ship with common off-the-shelf development environments; or

- c. available to users, e.g. client side scripts implemented as part of a web application.
49. Consideration should be given to the degree of trust placed in third party code libraries. Specifically, does the code perform:
- a. the intended action; or
 - b. any unwanted or unauthorised actions.

Development Standards, Architectures, and Hardening Guides

50. Defence ICT systems should be built in accordance with a Defence endorsed security architecture. Further information about system development requirements, including standards, can be found in the Software Application Development and Web Application Development sections of the [ISM](#) or from ICT Architecture Branch.

Components and Subsystems

51. Some components of a larger system may entail specific types of risks and require additional consideration.
52. Systems that use ICS, Supervisory Control and Data Acquisition (SCADA) or Programmable Logic Controllers (PLC) as subcomponents used within traditional ICT systems, as part of base management systems, or operational technologies, may be exposed to risks that are not applicable to other systems and therefore require additional consideration. It is recommended that any use of such components be highlighted in system design documentation and discussed with the applicable certification authority from the earliest possible stages of system development.

System Testing

53. All input to systems are to be assumed to be untrusted until verified as correct, safe and suitable.
54. System development plans are to identify the type(s) of test data to be used.
55. Test data is Defence information and **must** be protected under PSPF Infosec 8 Sensitive and classified information. With the assessed risks detailed in the Security Risk Management Plan. Anonymising real data must not allow for reversal of the process, or for identities, capabilities or limitations to be inferred. Anonymising may reduce the sensitive or classified information.
56. Plans are to give consideration to the confidentiality of test data, particularly if the data is to leave Defence control. See DSPF Principle 21 – *Offshore and Cloud Based Computing* for further requirements. Anonymising may reduce the sensitive or classified information.

Vulnerability Assessment

57. As the ICT capability manager, CIOG is responsible for the development of a technical vulnerability assessment strategy for Defence. System Owners should consult with the relevant Certification Authority for advice on technical vulnerability assessments.

58. Vulnerability management must include monitoring and managing vulnerabilities in, and change to, a systems that can provide valuable information on the exposure to threats.

59. In accordance with DSPF Control 29.1 – *Information Systems Vulnerability and Patch Management*, change management process **must** include implementing routine and urgent changes to software or systems to maintain security (including if the change triggers the need for reaccreditation).

Introduction into Service

Certification and Accreditation

60. Defence systems are not to process Sensitive/ Classified information until awarded formal accreditation in accordance with DSPF Principle 23 – *ICT Certification and Accreditation*.

61. Security accreditation only attests that the system presents an acceptable level of security risk. It does not imply compliance with any other standards or requirements.

Merging and Connecting Systems and Networks

62. System Owners are to consult with any relevant Certification and Accreditation Authorities before merging or connecting systems or networks in order to ensure that all new risks are identified and appropriately managed.

63. The user base of each system/network is to be considered in consultation with the relevant Certification Authority before they are merged or connected and appropriate controls must be implemented.

Note: This is of particular importance if networks are used by foreign nationals and process information with nationality based restrictions.

System Operation

64. ICT systems and networks are to be monitored in accordance with the requirements of DSPF Principle 19 – *Information Systems (Logical) Security*.

65. Regular reviews should be conducted to manage risks throughout the operational phase of the system's lifecycle.

System Owner Responsibilities

66. System Owners are to manage the ongoing sustainment activities throughout the systems lifecycle.

67. System Owners are to ensure the application, system, or network they are responsible for has an effective ICT Security maintenance program that covers the following essential security requirements:

- a. configured and maintained end-point ICT security controls;
- b. enabled and effective application white listing; and
- c. up to date security patched core infrastructure software and hardware is applied.

68. System Owners are to ensure that all access controls associated with protecting sensitive or classified information are periodically reviewed to ensure only authorised users have access to sensitive or classified information. Reviews are to include ensuring appropriate protection methods are in place to ensure the protection of AUSTEO and foreign official information.

69. System Owners are to implement measures to control the installation of software on operational systems in accordance with the Software Security and Secure Administration sections of the [ISM](#) or those listed in the DASL should be used.

70. With regards to application whitelisting, System Owners are to ensure that users and system administrators are not permitted to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms once enabled.

71. When patching, updating, or managing a system incident, system Owners are to manage security incidents involving systems across all phases of the incident's life cycle in order to:

- a. inform understanding of Defence's security posture;
- b. minimize the impact of the specific incident;
- c. inform the continuous improvement of protective measures and controls; and
- d. ensure that people are accountable for their actions.

72. When maintaining a system accreditation, System Owners are to ensure that all systems under their control are operated and undergo regular re-certification and re-accreditation in accordance with DSPF Principle 23 – *ICT Certification and Accreditation*.

73. When changes or updates to system configuration are proposed, system Owners are to ensure that:

- a. all changes to ICT systems have successfully passed acceptance testing and received appropriate security certifications and accreditation prior to being commissioned for operational use;
- b. all changes to configuration baselines are updated as part of the Defence Change Management process and reflect the actual configuration that was implemented under an approved change;
- c. periodic reviews of configuration baselines are conducted to ensure no unauthorised changes have been performed outside of the approved Defence Change Management process; and
- d. all ICT products and services are procured in accordance the CIOG Risk Management Guide for ICT Procurement requirements, which includes a SCRM assessment.

74. When decommissioning or disposing of systems, System Owners are to ensure that all ICT systems within the SIE are decommissioned in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information* and DSPF Principle 22 – *Mobility Device Security* and that the supply chain risk management disposal requirements are addressed.

User Management

75. System Owners are to ensure that all user accounts are periodically reviewed, to ensure all users are accounted for and that the appropriate level of rights have been assigned to them.

76. The management of System Users and Privileged Users, is to be performed in accordance with:

- a. DSPF Principle 18 – *Information Systems (Personnel) Security*;
- b. system SOPS; and
- c. instructions as approved during accreditation.

System Log Management

77. System Owners are to ensure that system logs are being effectively managed throughout the life of all systems in accordance with DSPF Principle 28 – *Information Systems Log Management*.

Application Whitelisting

78. ICT systems approved to store and process 'OFFICIAL' or 'OFFICIAL: Sensitive' information are listed on Defence approved systems whitelists.

79. Application whitelisting must be enabled on ICT systems using one of the following:

- a. cryptographic hashes;
- b. publisher certificates;
- c. absolute paths; or
- d. parent folders.

80. These methods are to be applied in accordance with the appropriate [ISM Controls](#) and the ACSC's "[Essential 8 ACSC Strategies](#)" relating to Application Whitelisting to prevent the execution of unapproved/malicious programs.

Note: When enabling absolute paths, file permissions are to be configured to prevent users and system administrators from being able to modify files that are permitted to run.

Note: When enabling parent folders, file system permissions are to be configured to prevent users and system administrators from being able to add or modify files in the authorised parent folders.

Patching, Updating and Incident Management

81. Security patching of ICT System operating systems, applications, drivers, and hardware devices must be done in accordance with DSPF Principle 29 – *Information Systems Vulnerability and Patch Management Security* and ACSC "[Essential 8 Strategies](#)" to Mitigate Targeted Cyber Intrusions related to patching of applications. You can also refer to Defence patch management process.

82. Security incidents involving Defence and Defence industry information systems are to be managed in accordance with DSPF Principle 24 – *Information Systems Security Incident Management*; DSPF Principle 77 – *Security Incidents and Investigations*; and DSPF Principle 71 – *Physical Transfer of Information and Assets*.

Maintaining Accreditation

83. All changes that may impact the security of an ICT system, and are subsequently assessed as having changed the overall security risk for the system, are to result in reaccreditation.

84. Triggers for re-accreditation include significant changes to:

- a. system architecture or implemented controls;
- b. information stored, processed or communicated;
- c. user base;
- d. the environment in which the system operates; and

- e. any other conditions stipulated by the accreditation authority, such adherence to requirements around Supply Chain Risk Management.

Configuration and Change Management

85. All changes proposed or being considered are to have an ICT security impact analysis completed prior to being implemented to ensure security risks associated with the change have been assessed. This includes:

- a. upgrades to, or introductions of, ICT equipment;
- b. upgrades to, or introductions of, software; or
- c. major changes to security controls including:
 - (1) changes in the Business Impact Levels (BILs) associated with the system (for example, the integrity of a system is reassessed or the Protective Marking raised;
 - (2) significant changes to the architecture of the system or the security controls it implements;
 - (3) changes to the user base of the system, particularly in regard to foreign nationals and Privileged Users; or
 - (4) any other conditions stipulated by the Accreditation Authority.

Auditing ICT Equipment

86. The physical location of fixed ICT and electronic office equipment is to be recorded and documented. For portable ICT Assets (including Mobile devices), the custodian of the device is to be documented.

87. Auditing of ICT equipment, including electronic office equipment and networking devices, is to be performed in accordance with DSPF Principle 17 – *Information Systems (Physical) Security*.

System Maintenance

88. The security configuration of the device is not to be changed without prior authorisation via established Defence Change Management processes.

89. Where an escort is required to supervise maintenance of a classified device, the escort must ensure that non-volatile media is not removed from Defence custody unless the maintainer has been accredited to handle and dispose of classified material. If classified media is to be removed from the device and transferred to another person's custody, then procedures for the transfer of classified material contained in DSPF Principle 71 – *Physical Transfer of Information and Assets* are to be followed.

90. Devices containing non-volatile media are to be transferred as a classified item. For bulky equipment, non-volatile media may be removed from the device and securely transported according to its Protective Marking. A device with all non-volatile media removed has been sanitised and may therefore be transferred as an 'OFFICIAL' item.

Decommissioning and Disposal

Retention of Records

91. Records pertaining to a system may need to be kept after its decommissioning.

92. Investigation of a security incident suggests that classified information may have been previously compromised via a system which has since been decommissioned. Security logs from the old system may need to be audited to determine whether or not the information was compromised.

93. Event log retention requirements are specified in the ISM and DSPF Principle 28 – *Physical Transfer of Information and Assets*.

Sanitisation and Destruction of Electronic Storage Media

94. System Owners and Equipment Managers must document and enact processes to:

- a. identify electronic storage media containing classified or otherwise sensitive information. This process is to take into account the effect of information aggregation;

Note: When identifying electronic storage, it is important to recognise the different types of media as this can affect sanitisation and destruction requirements. In particular hybrid drives (those using a mixture of magnetic and solid state memory) have specific constraints in terms of sanitisation.

- b. prevent media containing sensitive or classified information from being released into the public domain or disclosed through inadequate protection. This process is to meet the requirements of DSPF Principle 10 – *Assessing and Protecting Official Information* and the ISM.
- c. record the reclassification, sanitisation or destruction of electronic storage media in a suitable register.

Disposal of Sensitive or Classified Hardware

95. Sensitive or classified hardware associated with an ICT system or electronic office equipment must be disposed of in accordance with accredited processes that comply with:

- a. DSPF Principle 10 – *Assessing and Protecting Official Information*;

- b. DSPF Principle 71 – *Physical Transfer of Information and Assets*;
- c. the ISM; and.
- d. the hardware SCRM through life disposal requirements.

96. When hardware is CCI (Controlled Cryptographic Item) or implements key material eligible for the CRYPTO caveat then it must be disposed of in accordance with ACSC advice.

Roles and Responsibilities

Chief Information Officer (CIO)

97. The CIO is responsible for:
- a. providing a secure and dependable information environment;
 - b. ensuring the information environment is covered by suitable acceptable use policies;
 - c. ensuring the development and maintenance of an ICT security strategy;
 - d. ensuring the development and maintenance of ICT security architecture;
 - e. delivering an effective certification and accreditation framework for Defence that meets Government expectations;
 - f. developing policy and guidance on the approval to operate standalone networks;
 - g. developing strategies to mitigate any identified risks arising from equipment supply chains;
 - h. approving ICT system and equipment procurement in accordance with FINMAN2;
 - i. developing Defence-wide vulnerability assessment and system monitoring strategies and capabilities; and
 - j. providing adequate capacity to ensure the performance of the SIE.

Chief Information Security Officer (CISO)

98. The CISO is responsible for:
- a. establishing the strategic direction for ICT Cyber security across Defence and Defence industry;
 - b. developing and maintaining an ICT Cyber Security strategy;

- c. contributing security expertise to the development and maintenance of an ICT security and Cyber Security architecture;
- d. maintaining an effective Certification and Accreditation Framework for Defence and Defence Industry in accordance with Government expectations, Defence policy and the Defence ICT security strategy; and
- e. liaising with DS&VS and Executive Security Advisers to ensure that information systems security is integrated with broader protective security strategies, policies, and plans.

Defence Information Technology Security Advisor (ITSA)

99. The Defence Information Technology Security Advisor (ITSA) is responsible for:
- a. coordinating ICT certification and accreditation functions to a standard that meets Government expectations;
 - b. coordinating of Defence Information Technology Security Managers (ITSM) across Defence in order to meet the strategic direction of the CISO;
 - c. liaising with Defence ITSA in other agencies on technical ICT security matters; and
 - d. maintaining visibility of certified systems and any associated recommendations made to accreditation authorities.

Defence Information Technology Security Manger (ITSM)

100. The Defence ITSMs function is a specific subset of the System Manager role. It may be performed by the System Manager directly or the System Manager may delegate the function to a separate appointment.

101. The Defence ITSM is responsible for:
- a. liaising with the Defence ITSA;
 - b. informing the system manager of any identified risks to the systems for which they are responsible;
 - c. informing the Defence ITSA of any risks that may also affect other systems;
 - d. identifying potential security improvements;
 - e. ensuring that security recommendations or requirements provided by the Defence ITSA are enacted; and
 - f. maintaining system configuration in accordance with accredited processes.

Note: This role has been introduced in order to align Defence terminology with the ISM. Previously within Defence, many functions of this role would have been performed by the Information Systems Security Officer (ISSO). In cases where an ISSO manages or coordinates other ISSO, the lead ISSO may become a Defence ITSM.

Information Technology Security Officer (ITSO)

102. With regard to the lifecycle management of information systems, the Information Technology Security Officer (ITSO) is responsible for:

- a. implementing directions from the Defence ITSM, system manager and the Defence ITSA;
- b. notifying the system manager and Defence ITSA of any identified vulnerability that may prejudice the security of the system;
- c. reporting any security incidents detected or identified; and
- d. performing security management tasks in accordance with applicable SOPs and any other conditions stipulated during accreditation.

Note: This role has been introduced in order to align Defence terminology with the ISM. Previously within Defence, many functions of this role would have been performed by the ISSO. In many cases ISSO will become ITSO.

System Sponsor

103. System Sponsors are responsible for:

- a. developing business cases that initiate the development and introduction of new systems;
- b. defining system boundaries and the scope of system functions;
- c. defining the BIL of information and providing this to System Owners;
- d. ensure that procurement and contractual activities are carried out in accordance with the ICT/Cyber Procurement SCRM Framework; and
- e. securing CIO approval for ICT system and equipment procurement in accordance with FINMAN2 prior to commitment of any funds. Where an exemption is applied the decision and rationale must be recorded within the AE643 -Defence Purchasing.

104. Under some circumstances, the System Sponsor may be the System Owner. Otherwise the System Sponsor will appoint a System Owner.

System Owners

105. System Owners are responsible for ensuring that:
- a. the BIL of the system is informed through the information held on behalf of stakeholders;
 - b. systems are built and maintained to a security standard suitable for their intended use;
 - c. systems do not store, process or communicate Official Information without appropriate accreditation;
 - d. systems maintain accreditation;
 - e. systems are operated and managed in accordance with their accreditation;
 - f. manage procurement activities in accordance with the CIOG Risk Management Guide for ICT Procurement requirements; and
 - g. systems are securely decommissioned at the end of their lifecycle in accordance with the disposal requirements of the original SC Risk Assessment.

System Managers

106. System Managers are responsible for:
- a. appointing a system specific ITSM;

Note: A system manager may assume the role of ITSM, depending on the size and complexity of the system.

- b. advising System Owners of any known vulnerabilities, non-compliances, unmanaged risks or other issues affecting the security of the system;
- c. supporting System Owners in the development of dispensation requests as required;
- d. managing and protecting system documentation;
- e. making system configuration changes which are approved in accordance with defined processes;
- f. monitoring and maintaining the security configuration of systems ensuring that applicable standards are met;

Example: Patches are tested and applied in a timely manner to maintain the standard of system security.

- g. monitoring system activity for anomalies that might indicate the realisation of a security risk; and
- h. reporting any security incidents affecting the system.

Privileged Users

107. Privileged Users are only to implement changes to information systems that have:

- a. been approved through a Defence Change Management process;
- b. been security assessed, and any increased risk to the information system and/or connected systems has been accepted by the System Owner (or their delegate);
- c. not introduced any significant risk that has not been duly assessed; and
- d. had all baseline configuration documentation updated as part of the Defence Change Management processes, and reflect the actual configuration that was implemented under an approved change.

System Users

108. Persons engaged under contract are not to make any changes to information systems (including installing software/hardware or changing existing system configuration) unless they are authorised to do so in accordance with formal Defence change management processes.

Certification Authorities

109. Certification Authorities are responsible for:

- a. ensuring that certification requests are supported by the necessary system documentation;
- b. assessing the submitted documentation against the requirements specified in all policy and standards applicable to the system;
- c. identifying areas in which the system does not comply with applicable security requirements;
- d. identifying (in conjunction with the System Owner) any aspects of the system or its environment that would require controls above minimum standards;
- e. communicating residual risk to the Accreditation Authority to enable an informed accreditation decision; and
- f. maintaining appropriate records of certified systems and recommendations made to accreditation authorities.

Accreditation Authorities

110. Accreditation Authorities are responsible for:
- a. confirming that system certification has been conducted to a suitable standard;
 - b. considering the residual risk (and any other associated recommendations) as communicated by the Certification Authority and deciding whether or not to accept the risks associated with operating the system;
 - c. documenting the decision whether or not to accredit the system in an accreditation report;
 - d. maintaining visibility of all systems awarded accreditation and their associated re-accreditation schedules; and
 - e. facilitating requests for dispensations raised by System Owners, or alternatively, notifying System Owners of the reasons for not supporting the request.

Equipment Managers

111. Equipment Managers are responsible for developing and implementing management plans for equipment throughout its lifecycle.

Key Definitions

112. **Application Whitelisting.** An approach in which an explicitly defined set of applications are permitted to execute on a given system. Any application excluded from this list is not permitted to execute.
113. **CCI.** Controlled Cryptographic Item.
114. **Configuration Baseline.** The term used to describe the current approved configuration state of an information system that has been managed through Defence Change Management.
115. **Defence Change Management** is the process used to make changes to information systems baseline with the SIE.
116. **Defence Approved Hardware List (DAHL).** The DAHL is the authoritative list of ICT hardware and components that can be deployed on the Defence protected environment (DPE), Defence Secret Environment (DSE) and other Defence related situations
117. **Defence Approved Software List (DASL).** The DASL is the authoritative list of ICT software that can be deployed on Defence networks.
118. **Firmware.** Software embedded in a hardware device.

119. **High Assurance Product (HAP).** A product that has been approved by ACSC for the protection of information classified CONFIDENTIAL or above.

120. **Industrial Control Systems (ICS).** A class of system that controls measures or otherwise manages industrial or mechanical processes. These often represent a boundary between logical systems and the physical world. The term ICS encompasses Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logical Controllers (PLCs).

121. **Patching.** The process of applying updates to software including operating systems and applications.

122. **SAFEBASE.** Defence's security alert level system that provides planning guidance and standards to Defence on appropriate measures to take in response to varying threat levels.

123. **Systems Development Life Cycle (SDLC).** Is used to describe a process for planning, creating, testing, and deploying an information system.

Further Definitions

124. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

125. Australian Government Information Security Manual-Supporting information-[Glossary of cyber security terminology](#).

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Lifecycle Management
Control Owner	ITSA
DSPF Number	Control 20.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Lifecycle Management
Related DSPF Control(s)	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Offshore and Cloud Based Computing

General principle

1. Offshore and cloud based Defence information is only hosted by cloud service providers on the 'Certified Cloud Services List' who have been evaluated and certified by the Australian Signals Directorate.

Rationale

2. Defence and Defence Industry personnel require secure access to, and communications with, information systems and electronic devices they require for work purposes.
3. Information stored offshore or in a cloud based environment is more vulnerable and subject to greater security risks than that stored in Defence or Defence Industry controlled systems and environments.

Expected outcomes

4. Technical security and business risks are managed effectively throughout each information system's life cycle. These include issues of privacy, data ownership and data sovereignty.
5. Business Impact Level assessments are used to determine the most appropriate host to be used for offshore or cloud based computing, and any arrangements are carefully considered and balanced against security risks.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	EL1/O5 employed within ICT Security Branch Integrated Risk Management (IRM) Directorate or Information Technology Security Manager (ITSM)	EL1/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	EL2/O6 employed within ICT Security Branch IRM Directorate or ITSM	EL2/O6 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive (CSE) Note: In the event that an appointment of a Group or Service CSE has not been made, the Defence CISO will be the appropriate escalation point
High	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor (CSA) Note: In the event that an appointment of a Group or Service CSA has not been made, the Defence ITSA will be the appropriate escalation point.
Extreme	Defence Chief Information Officer (CIO)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Offshore and Cloud Based Computing
Principle Owner	CISO
DSPF Number	Principle 21
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 21.1
Control Owner	ITSA

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Protective marking of Information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems. Australian Government Information Security Manual (ISM) Legislation: Archives Act 1983 Privacy Act 1988 Freedom of Information Act 1988
Read in conjunction with	Commonwealth Procurement Rules Foreign equivalent FOI acts Foreign operation of Foreign Intelligence Services, local intelligence collection laws Notifiable Data Breach legislation (under Privacy Act)
See also DSPF Principle(s)	Security for Projects Security for Capability Planning Foreign Release of Official Information Defence Industry Security Program Information Systems (Physical) Security Information Systems (Physical) Security Information Systems (Logical) Security Information Systems Data Transfer Security Information Systems Lifecycle Management Information Systems Log Management
Implementation Notes, Resources and Tools	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Offshore and Cloud Based Computing

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Offshore and Cloud Based Computing
Control Owner	ITSA
DSPF Number	Control 21.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Offshore and Cloud Based Computing
Related DSPF Control(s)	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Mobility Device Security

General principle

1. Defence provisioned mobility devices (including personal mobile Information and Communications Technology (ICT) e.g. phones, tablets, laptop computers etc.) are to be afforded security protections commensurate with the Protective Markings of information they process, store or communicate.

Rationale

2. Mobility devices present unique security challenges due to their:
- a. rapidly evolving nature;
 - b. ability to capture, record, process, transmit and store large amounts of information in almost any conceivable format; and
 - c. ability to provide a means to exchange that information via fixed and ad-hoc networks.

Expected outcomes

3. Defence provisioned mobility devices are configured and operated in a way so that the likelihood of compromise of Official Information, or connected ICT systems is as low as reasonably possible.
4. Information assets are protected in order to safeguard Defence's customers, intellectual property, and reputation.
5. Security measures and practices are in place to ensure official information is protected during offsite work.
6. Defence provisioned mobility devices are protected in an appropriate manner when used outside of controlled facilities.
7. Non-Defence mobility devices are not physically connected to the Single Information Environment (SIE).

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor. Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO); or Head of CIOG ICT Operations Division in the case of Accreditation matters	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Mobility Device Security
Principle Owner	CISO
DSPF Number	Principle 22
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 22.1
Control Owner	ITSA

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM) <u>Legislation:</u> Privacy Act 1988 (Cth)
Read in conjunction with	N/A
See also DSPF Principle(s)	Foreign Release of Official Information Information Systems Security Incident Management Media Protection Security Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Working Offsite Physical Security Security Incidents and Investigations
Implementation Notes, Resources and Tools	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Mobility Device Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide Control. Mobility Device Security

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor. Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	Chief Information Officer (CIO); or Head of CIOG ICT Operations Division in the case of Accreditation matters	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

Mobility Devices

Mobility Device Usage Policy

2. Defence owned mobility devices that have been used to process, store, or communicate sensitive or classified information must be protected in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information*.
3. Defence owned mobility devices may be connected to trusted Wi-Fi networks in order to conduct Defence business or receive software updates. Trusted Wi-Fi networks include those provided by Defence or a member's home Wi-Fi network that is appropriately secured.
4. Defence owned mobility devices must not be connected to an unknown or un-trusted Wi-Fi network (e.g. open public Wi-Fi networks such as those in public areas, shopping centres, departure lounges, hotel rooms, or Internet kiosks).

Note: *The use of an unknown or un-trusted Wi-Fi network can have associated security risks. Risks are due to public Wi-Fi not enforcing encryption rules on the connection, which makes eavesdropping and other attacks possible. Ensure that the trusted Wi-Fi network is configured to use strong encryption (minimum WPA2 with EAP-TLS security).*

Example: *Luke has poor mobile reception at his home, so when he is at home he connects his Defence-issued smartphone to his home Wi-Fi network. This is a security breach because the phone has not been accredited for connection to non-Defence networks.*

5. Defence personnel and persons engaged under a contract are to adhere to the Standard Operating Procedures (SOP) and Defence Instructions issued with Defence owned mobility devices, including any restrictions on connection of the device.
6. Refer to DSPF Principle 19 – *Information Systems (Logical) Security* for details on the use of public devices and remote access solutions such as Defence Remote Electronic Access and Mobility Services (DREAMS) for the processing of Official Information.

Personnel Awareness

7. Defence personnel and persons engaged under a contract are to be aware of their surrounding environment when using mobility devices outside of the office. Refer to DSPF Principle 70 – *Working Offsite*.

Non-Defence Owned Mobility Devices

8. Privately owned mobility devices may be used in business areas that are not categorised as PED prohibited areas (refer to DSPF Principle 72 – *Physical Security*). This includes for voice conversations and connection to public infrastructure, such as mobile carriers or public wireless internet.

Example: Kate wants to transfer an unofficial file from her Defence computer to her home computer, she uses a privately owned memory stick to do this. This is a security breach – she could have emailed the file to her private address instead.

9. Privately owned mobility devices must not be connected (either via a network connection or physical connection) to a Defence controlled device or system.

Example: Bill recharges his privately owned phone by connecting it via a USB cable, to a Defence workstation. This is a security breach – he should use a power point adaptor instead.

10. Privately owned mobility devices with recording capability must not be used to capture sensitive or classified information, or be used in an environment in which this might inadvertently occur.

Example: Rather than take notes at a meeting where 'SECRET' material is being discussed, Amy decides to record the audio on her privately owned phone. This is a security breach.

11. Privately owned mobility devices that have inadvertently been contaminated with security classified material must be reported as a security breach in accordance with DSPF Principle 24 – *Information Systems Security Incident Management*.

Defence Owned Mobility Device Storage Encryption

12. All internal storage and removable media of Defence owned mobility devices is to be encrypted with ASD approved encryption.

13. Defence personnel and persons engaged under a contract are not to store passphrases for the encryption software on, or with, the mobility device that the encryption software is installed on.

14. Unless the storage and physical transfer requirements of a mobility device can be lowered to 'OFFICIAL' through the use of ASD approved encryption, the mobility device must be stored and physically transferred as a sensitive or classified asset. Refer to DSPF Principle 71 – *Physical Transfer of Information and Assets*.

Mobility device communications encryption

15. Mobility devices must not communicate sensitive or classified information over public network infrastructure without encryption approved for such information over public network infrastructure. Refer to [ISM Cryptography](#) chapter for communication encryption requirements.

Mobility Device Privacy Filters

16. Privacy filters may be applied to the screens of mobility devices to prevent onlookers from reading content on the screen of the device.

Bluetooth Functionality for Mobility Devices

17. Bluetooth provides inadequate security for information passing between the mobility device and other connected devices. Defence personnel are to be aware of the risks of Bluetooth including when pairing, particularly with unknown devices. Defence owned mobility devices **must**:

- a. have Bluetooth functionality disabled on those devices processing 'SECRET' and above;
- b. be configured to remain undiscoverable to all other Bluetooth devices except during pairing;
- c. only be paired to devices when it is required for business needs, and then be unpaired when no longer required;
- d. have communication ranges reduced by selecting the appropriate Bluetooth class:
 - (1) class 1 devices can communicate up to 100 metres;
 - (2) class 2 devices can communicate up to 10 metres; and
 - (3) class 3 devices can communicate up to 5 metres; and
 - (4) only use Bluetooth version 2.1 when pairing.

Configuration Control

18. The ICT accreditation authority must approve the acceptable use of, and permitted configuration for, the Defence owned mobility device. This will be based on policy requirements detailed in the [ISM](#), the DSPF, and the specified purpose of the mobility device. Refer DSPF Principle 23 – *ICT Certification and Accreditation*.

19. The security of mobility device configuration should be controlled in the same manner as devices in the office environment. Defence owned mobility devices shall be periodically audited to ensure their configuration controls remain enabled and effective. This includes:

- a. ensuring the mobile carrier is able to provide security updates;
- b. ensuring mobility devices are able to accept security updates from the mobile carrier as soon as they become available;

- c. implementing a policy enforcing compliance with a defined security configuration for mobility devices; and
 - d. regular testing of devices to ensure they still meet the agency-defined security configuration, and that patches are up-to-date and effective.
20. Defence personnel must not disable security functions on a mobility device once provisioned.
21. All software updates to Defence owned mobility devices are to be applied in accordance with DSPF Principle 29 – *Information Systems Vulnerability and Patch Management*.

Standard Operating Procedures and Defence Instructions

22. Relevant system documentation and requirements must be provided for Defence personnel in either a system specific SOP or a Defence Instruction.

Note: DISP members may choose to apply instructions using an internal documentation framework provided the instruction has the endorsement of the appropriate ICT accreditation authority, and is enforceable within the company's governance framework.

23. If a Defence Instruction (or industry equivalent higher level document) is used to cover some aspects of the documentation, then the SOP provided with the system must reference all other relevant Instructions.
24. The SOP or Defence Instruction developed during the accreditation process must state the classification of the device in each functional state, according to the level of protection that is effective in that state.

Example: The SOP or Defence Instruction for a secure phone with embedded ASD-approved encryption technology may specify that it is 'OFFICIAL' when powered off and 'SECRET' when in standby mode, screen locked or operational.

Connecting Defence Mobility Devices to the Internet

25. When browsing the internet it is best practice to ensure the mobility device uses a Virtual Private Network (VPN) connection though Defence's Internet gateway rather than via a direct connection to the internet.
26. Split Tunnelling functionality is available on some Mobility Devices that allow personnel to access both a public network and a VPN connection at the same time, such as a Defence system and the internet. When using a VPN connection, Split Tunnelling should be disabled if the Mobility device supports this functionality. Refer to [ASD Additional Security Considerations and Controls for Virtual Private Networks – Split Tunnelling](#) for information on how to manage the residual risks associated with allowing split tunnelling.

Paging and Messaging Services

27. Paging and messaging services do not appropriately encrypt information. They are not to be used to send sensitive or classified information unless a third party product is in place to ensure content is transmitted via this means is encrypted.

Emergency Destruction

28. Emergency destruction procedures are to be developed for Defence-owned mobility devices. Procedures are to focus on destroying information on the mobility device as opposed to the device itself. This may be achieved through the use of a cryptographic key zeroise or sanitisation function. The use of a remote wipe can be used to achieve the destruction of information.

29. If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobility device, the function must be used as part of the emergency destruction procedures.

Working Outside the Office

Carrying Defence-Owned Mobility Devices

30. Defence owned mobility devices are to be carried in a secured state when not being actively used. This includes enabling encryption when the device is not in use.

Note: The effectiveness of encrypting a device's internal storage could be reduced while it is in sleep mode or powered on with a locked screen.

Using Defence-Owned Mobility Devices

31. Defence personnel and persons engaged under a contract using Defence owned mobility devices outside of the office, including conducting remote access to the Defence Single Information Environment (SIE) from both privately owned and Defence provisioned devices, are to comply with DSPF Principle 19 – *Information Systems (Logical) Security*.

Travelling with Defence-Owned Mobility Devices

32. Defence personnel and persons engaged under a contract travelling overseas with Defence owned mobility devices are to take additional steps to mitigate information security risks.

33. When travelling with mobility devices and media, personnel are to retain control over them at all times, this includes not placing them in checked-in luggage or leaving them unattended at any time.

34. Prior to departure personnel are to:

- a. patch applications and operating systems;

- b. implement multi-factor authentication;
- c. back-up all media
- d. remove all non-essential data including 'OFFICIAL' information;
- e. disable applications that are not essential for the period of travel;
- f. disable Bluetooth and wireless connectivity;
- g. configure wireless to connect only to known, secure networks; and
- h. implement technical controls on mobility devices and obtain an appropriate security briefing. Refer DSPF Principle 44 – *Overseas Travel*.

35. Defence personnel and persons engaged under a contract should take the following precautions when travelling overseas with a mobility device:

- a. do not store authentication details or tokens and passphrases with the device;
- b. avoid connecting to open Wi-Fi networks;
- c. clear web browser after each session including history, cache, cookies, URL and temporary files;
- d. encrypt emails where possible;
- e. ensure login pages are encrypted before entering passphrases;
- f. avoid connecting to untrusted computers or inserting removable media; and
- g. mobility devices are not to be left unattended at any time.

36. Any requests by customs personnel to decrypt Defence mobility devices for inspection, or any occurrence where the device leaves the holder's possession at any time, are to be reported to the local Security Officer as soon as possible as a potential compromise of information on the device.

Example: *Stefan is travelling with a Defence laptop that has a 'handle-as' classification of 'SECRET'. He locks it in the hotel safe while he goes out for dinner. This is a security breach, and it needs to be reported to the local Security Officer.*

37. Passphrases associated with mobility devices are to be changed upon return from overseas travel.

38. Mobility devices should be inspected following overseas travel to check for evidence that the device has been compromised. Refer *Configuration Control* heading above.

Working from Home

Securing Devices in the Home Environment

39. The [Australian Government physical security management protocol](#) is to be followed when handling and storing security classified assets and information outside of the regular work environment. Refer to DSPF Principle 70 – *Working Offsite*.

Roles and Responsibilities

ICT Accreditation Authority

40. The applicable ICT Accreditation Authority is responsible for accrediting:
- a. the mobility device either as a stand-alone device or as a component of a system;
 - b. the removable media types and the conditions of use. These details will be provided to users in the form of a SOP or issued as a Defence Instruction. A Defence Instruction may be issued to provide an umbrella policy across a number of systems, this approach helps to prevent repetition in individual system SOPs;
 - c. all data transfer mechanisms to and from the system or device including, but not limited to, air-gapped data transfers, gateways and other connections. Instructions for the conduct of data transfers will be provided in the form of a SOP or issued as a Defence Instruction and will cover the types of devices permitted for use, the systems to and from which data transfers may be conducted, and the procedures to be used to conduct data transfers. Accreditation of data transfer solutions will confirm that requirements contained in the [ISM Data Transfers and Content Filtering](#) section are met or relevant dispensations are in place;
 - d. procedures for securing mobility devices and removable media during operation, storage and transit, against the requirements specified in the ISM; and
 - e. disposal procedures for classified mobility devices and removable media against the requirements specified in the ISM.

System Owner

41. The System Owner is responsible for the provision of an ICT system. Where mobility devices are procured through a whole-of-Defence support contract, an equipment manager is to be appointed by the System Owner.
42. System Owners and/or Equipment Managers are responsible for:
- a. developing a through life support plan for the device;

- b. gaining and maintaining ICT accreditation for the device in accordance with DSPF Principle 23 – *ICT Certification and Accreditation*; and
- c. ensuring that all Defence-owned devices, whether on issue or transfer to individuals or stored pending issue, are accounted for.

Commanders and Managers

43. With respect to those areas of a base or facility that are not subject to mandatory mobility device prohibitions enforced by an ICT accreditation authority (for example TOP SECRET areas), a commander or manager may choose to implement additional mobility device prohibited areas within their base or facility to address identified security risks. Refer DSPF Principle 72 – *Physical Security*.

Security Officers

44. A Security Officer or regional Information Technology Security Officer (ITSO) may be appointed to assist the System Owner, or Commander or Manager; to fulfil their ICT security responsibilities.

45. The decision to appoint a Security Officer or ITSO is taken based on the complexity of ICT tasks to be performed. The use of the title ITSO reflects that specialist training or skill is required to perform the duties. When this is not the case it is more appropriate to name the position as a Security Officer.

46. It is recommended that security duties be delegated in writing. Examples of duties that may be delegated include:

- a. providing advice to commanders and managers regarding the use of mobility devices and removable media;
- b. maintaining a record of the location or issue of mobility devices held by the organisation (an asset register may be used for this purpose);
- c. recording user details (name, device accessed and time of login) for mobility devices that use shared passwords (for example, those in a training laptop pool); and
- d. assisting users to sanitise destroy or transfer for disposal, used electronic media which is no longer required (including hard disk drives, removable disk drives, and other removable media). Refer to DSPF Principle 26 – *Media Protection Security*.

Key Definitions

47. **Defence Controlled Device:** A device is under Defence control if it is owned by Defence or is subject to any agreement that legally binds the owner of the device to comply with all ISM security policies. Defence controlled devices include security classified assets owned by DISP members.

***Example:** A DISP member supplies their own computer to process SECRET information. DISP membership contractually obliges the company to comply with all Commonwealth policies and the DSPF, therefore the device is under Defence control.*

48. **Mobility Device:** A portable computing or communications device with information storage capability that can be used from a non-fixed location. Mobility devices include mobility phones, smart phones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers, and other portable internet-connected devices.

49. **Privately Owned and Public Mobility Devices:** Home computers, mobility devices, laptops, phones and removable media or any other form of computing device that is owned by an individual or a company and is not subject to Defence control.

- a. **Privately Owned Mobility Device:** A device where the end user has administrative control, responsibility and legal authority over the device's configuration. End users can exert control over these devices.

***Example:** A home computer or personal mobility phone. The end user can install virus detection software.*

- b. **Public Mobility Device:** A device where the end user has no administrative control over the device; they are not responsible for, and have no legal authority over, the configuration of the device.

***Example:** Devices in internet kiosks or shared devices in hotels.*

50. **Mobility Device Prohibited Area (or Portable Electronic Device (PED) Prohibited Area):** An area into which it is prohibited to bring mobility devices and media. Refer to DSPF Principle 72 – *Physical Security*.

51. **'Actual' and 'Handle-as' Protective Markings for Encrypted Devices and Media:** Where suitable Australian Signals Directorate (ASD)-approved encryption is applied to a device/media, that device/media has two different Protective Markings. These are:

- a. the 'actual' Protective Marking: the highest Protective Marking of Official Information stored on, or processed by, the device/media, regardless of whether encryption has been applied. This Protective Marking also applies whenever the device/media is in a keyed state, i.e. where the Official Information is accessible in an unencrypted form;

- b. the 'handle-as' Protective Marking: the Protective Marking of the device/media when the Official Information it contains is fully protected by encryption. This Protective Marking enables the device to be stored and physically transferred at a reduced Protective Marking due to the protection provided to stored information through the application of suitable ASD-approved encryption technology.

Note: *If suitable ASD-approved encryption is not used, the 'actual' and 'handle-as' classifications are the same, i.e. the highest classification of data stored or processed on the device/media.*

Exclusion: *ASD-approved remote access solutions such as Defence Remote Electronic Access Mobility Service (DREAMS) have been evaluated to ensure that information is not recoverable from the hosting device once the session ends. In these instances the degree of protection has been evaluated and the device is treated as 'OFFICIAL'.*

52. **Public Infrastructure:** Any infrastructure that is not supplied by Defence.

Further Definitions

53. Definitions for common Defence administrative terms can be found in the Defence Instruction -Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Mobility Device Security
Control Owner	ITSA
DSPF Number	Control 22.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Mobility Device Security
Related DSPF Control(s)	Foreign Release of Official Information Information Systems Security Incident Management Media Protection Security Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Working Offsite Physical Security Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

ICT Certification and Accreditation

General principle

1. Assurance processes, ensuring appropriate protections for Official Information during processing, storage and communication, are applied to all Information Communications and Technology (ICT) systems and capabilities prior to their operational use.
2. Regular assessments, performed against emerging cyber threats through the Certification and Accreditation process, ensure associated risks are considered, mitigated, and/or accepted as necessary.

Rationale

3. The certification and accreditation process:
 - a. enables Defence to understand and manage security risks to classified information, security-protected assets and infrastructure; and
 - b. provides assurance that sufficient security measures are in place or, that deficiencies and their associated risks have been mitigated or accepted.
4. Accreditation of ICT systems provides other Government agencies and coalition partners with confidence that Defence Groups and Services protect shared information and security protected assets.

Expected outcomes

5. Security controls are implemented to assure the protection of information and information systems, and reduce residual risk to an acceptable and manageable level.
6. Defence liaises with the appropriate government agency to accredit and certify TOP SECRET ICT systems.
7. Appropriate physical and personnel security controls are applied and are proportionate to assessed risks.
8. ICT systems meet mandatory minimum standards before they are authorised for use.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	Group/Service managed systems
Low	Accreditation Authority (must be SES1/1* or above)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Accreditation Authority (must be SES1/1* or above)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Accreditation Authority (must be SES1/1* or above)	Appointed Group or Service Cyber Security Advisor (CSE). Note: In the event that an appointment of a Group or Service Cyber Security Advisor (CSA) has not been made, the Defence Information Technology Security Advisor (ITSA) will be the appropriate escalation point.
High	SES2/2*	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	SES3/3*	Appointed Group Head or Service Chief.

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	ICT Certification and Accreditation
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 23
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 23.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	PSPF Core Requirements: Protective Marking of information; Access to information; Safeguarding information from cyber threats; Robust information and communication and technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Information Systems (Physical) Security]Personnel Security Clearance Temporary Access Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	PSPF Business Impact Levels (BIL)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

ICT Certification and Accreditation

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	Group/Service managed systems
Low	Accreditation Authority (must be SES1/1* or above)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Accreditation Authority (must be SES1/1* or above)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Accreditation Authority (must be SES1/1* or above)	Appointed Group or Service Cyber Security Adviser (CSE). Note: In the event that an appointment of a Group or Service Cyber Security Adviser (CSA) has not been made, the Defence ITSA will be the appropriate escalation point.
High	SES2/2*	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence Chief Information Security Officer (CISO) will be the appropriate escalation point.
Extreme	SES3/3*	Appointed Group Head or Service Chief.

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Process

Accreditation Requirements

- All Defence ICT systems must be accredited prior to processing, storing or communicating Official information.

3. ICT systems are to be reaccredited when one or more of the following conditions are met:
- Commonwealth or Defence policy changes;
 - new or emerging threats to systems are detected;
 - security measures are not operating as effectively as planned;
 - a cyber security incident occurs;
 - changes to the certified system architecture occur;
 - changes to the system risk profile occur;
 - the system extends outside the accreditation boundary;
 - the physical environment in which the system is installed changes; and
 - the system's accreditation expires.

Certification and Accreditation Appointments

4. Refer to Annex A of this Control for the key Governance and Functional appointments in the certification and accreditation process. The Annex also identifies the Certification and Accreditation Authorities for each Group or Service.

Certification and Accreditation (C&A) Process

5. Annex B of this Control demonstrates the C&A process and this should be read in conjunction with the *Roles and Responsibilities* outlined below.
6. If an external Certification Consultant (CC) is required to complete an assessment, they are to be approved by the ITSA or a delegated representative prior to conducting the certification. Failure to do so may render the certification void.
7. When conducting any assessment and/or certification activity for Defence, the Certification Consultant is to follow the Defence Certification and Accreditation Process. Refer to Annex B of this Control.
8. Prior to commencing an assessment, CC must be formally appointed (in writing) by a Certification Authority (CA) or delegated representative.
9. The table below provides the Residual Risk Rating and the responsibility of who can sign off on the risk for each domain/environment for the Certification and Accreditation process being accurately followed.

Table 1: Residual Risk and Responsibility

Residual Risk Rating	Responsibility			
	System	Domain	Security Environment	Defence Information Environment
Low	Accreditation Authority (must be SES1/1* or above)	IT Security Adviser	IT Security Adviser	IT Security Adviser
Moderate	Accreditation Authority (must be SES1/1* or above)	IT Security Adviser	Chief Information Security Officer	Chief Information Security Officer
Significant	Accreditation Authority (must be SES1/1* or above)	Chief Information Security Officer	Chief Information Officer	Chief Information Officer
High	SES2/2*	Chief Information Officer	Chief Information Officer via consultation with Defence Security Committee	Chief Information Officer via consultation with Defence Security Committee
Extreme	SES3/3*	Chief Information Officer via consultation with Defence Security Committee	Chief Information Officer via consultation with Enterprise Business Committee	Chief Information Officer via consultation with Enterprise Business Committee

Roles and Responsibilities

Certification Authority

10. A CA is responsible for:
 - a. identifying and appointing a suitably qualified CC to a Certification assessment (if required);

Note: an outside consultant will not always be required. This will be dependent on the Group/Service and the Protective Marking of material to be processed, stored and communicated on the system.

- b. awarding ICT Certification (endorsing the residual risk identified through a Certification assessment);
- c. providing recommendation(s) on Accreditation to the Accreditation Authority, including:
 - (1) whether to accept the residual risk;
 - (2) whether to issue a full ICT accreditation (ICTA) or a Provisional ICT Accreditation (PICTA);
 - (3) any conditions/Information Management Markers that should be placed on the approval;
 - (4) any remediation activities that must be completed during the approval period (PICTA only);
 - (5) the duration of the accreditation period; and
- d. reporting Certification outcomes to the ITSA.

Accreditation Authority

- 11. An AA is responsible for:
 - a. formal recognition, approval and acceptance of the risk(s) to a system;
 - b. approving a system into operation;
 - c. reporting Accreditation outcomes to the CISO; and
 - d. where required, delegating risk acceptance to the CSE/CSA within their Group/Service.

Cyber Security Executive

- 12. Where the AA chooses to delegate the responsibility of risk acceptance, the CSE must only accept risks up to and including HIGH.

Cyber Security Adviser

- 13. Where the AA chooses to delegate the responsibility of risk acceptance, the CSA may only accept risks up to and including MODERATE.

Certification Consultant

- 14. A CC is responsible for:
 - a. providing advice and guidance to the system owner on the assessment process;

- b. providing advice and guidance throughout all phases of the system development, on mitigation strategies and controls to effectively reduce risk within an acceptable risk tolerance;
- c. maintaining independence throughout the assessment process;
- d. conducting a Security Risk Assessment against current security policy and standards to assess residual risk and address any specific requirements of the CA;
- e. providing a Certification Report to the CA which articulates the risks(s) and recommendation(s); and
- f. maintaining evidence of activities conducted during a Certification Assessment.

System Owner

- 15. A System Owner (SO) is responsible for:
 - a. obtaining and maintaining accreditation of their systems in accordance with the above;
 - b. assessing the system's Business Impact Level (BIL);
 - c. determining Protective markings for information and assets for their systems;
 - d. developing relevant security artefacts for their system; and
 - e. maintaining independence from the AA.

Positions and Appointments

Functional Positions

- 16. Accreditation Authorities:
 - a. Capability Managers (generally the Group Head or Service Chief) are to act as the Accreditation Authority for their respective Group/Service. They may choose to delegate risk acceptance to their CSE or CSA but must retain the accountability for accreditation. A CSE or CSA must only accept risk to the level outlined under the CSE/CSA roles outlined above. Annex A is a list of functional positions and appointments within Defence relating to C&A.
- 17. Certification Authorities:
 - a. ICT Security Branch provides the majority of certification services for Defence SECRET and below systems, with the Assistant Secretary ICT Security (ASICTS) fulfilling the role of CA. Should a Group or Service wish to conduct certification activities for systems within their portfolio, a governance

and management structure must be developed and demonstrated prior to a CA being appointed.

- b. The Defence ITSA on behalf of the CISO is the only position in Defence authorised to approve the designation of a CA.
- c. A list of approved Certification Authorities is at Annex A.

Governance Positions

- 18. Information Technology Security Adviser (ITSA):
 - a. The ITSA is responsible for:
 - (1) managing and reporting on certification activities across Defence; and
 - (2) endorsing CAs and CCs.
- 19. Chief Information Security Officer (CISO):
 - a. the CISO is responsible for managing and reporting on accreditation activities across Defence.

Key Definitions

- 20. **Certification:** Certification is the process of identifying, assessing and reporting on the risk that an ICT system presents to an information environment.
- 21. **Accreditation:** Accreditation is the procedure by which an authoritative body (Accreditation Authority) gives formal recognition, approval and acceptance of the risk(s) to an ICT system.
- 22. **Provisional ICT Accreditation:** Provisional ICT Accreditation (PICTA) is a type of accreditation issued where the Accreditation Authority has requested further controls and/or risk mitigation activities to be undertaken during the provisional accreditation period.

Further Definitions

- 23. Definitions for common Defence administrative terms can be found on the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – Certification and Accreditation Appointments

Annex B – Defence Certification and Accreditation Process

Document administration

Identification

DSPF Control	ICT Certification and Accreditation
Control Owner	Information Technology Security Adviser
DSPF Number	Control 23.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise Wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	ICT Certification and Accreditation
Related DSPF Control(s)	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex A to ICT Certification and Accreditation – Certification and Accreditation Appointments

Accreditation Appointments

1. Governance Appointments:

Security Position	Organisational Position	Governance Scope
CISO	CTOD	Accreditation
ITSA	ASICTS	Certification

2. Functional Appointments for Group / Service.

Group/ Service	Accreditation Authority	Certification Authority	Cyber Security Executive	Cyber Security Adviser	Portfolio Scope
CIOG	CIO	ICTSB	HICTO	ASICTS	CIOG managed and interconnected systems
Army	CA	ICTSB	TBD	DLNI (AHQ)	Army standalone systems
Air Force	CAF	462SQN	TBD	TBD	Air Force standalone systems
Navy	CN	ICTSB	TBD	TBD	Navy standalone systems
E&IG	DSE&I	ICTSB	TBD	TBD	E&IG standalone systems
CASG	DSCASG	ICTSB	TBD	TBD	CASG standalone systems
DSTG	CDS	ICTSB	TBD	TBD	DSTG standalone systems
JCG	CJC	ICTSB	TBD	TBD	JCG standalone systems
VCDF	VCDF	ICTSB	TBD	TBD	VCDF standalone systems
SP&IG	DSSP&I	ICTSB	TBD	TBD	SP&IG standalone systems
JOC	CJOPS	ICTSB	TBD	TBD	JOC standalone systems
DPG	DSDPG	ICTSB	TBD	TBD	DPG standalone systems
CFOG	CFO	ICTSB	TBD	TBD	CFOG standalone systems
CDG	TBD	ICTSB	TBD	TBD	CDG standalone systems

3. Functional Appointments for Special Portfolios

Special Portfolio	Accreditation Authority	Certification Authority	Cyber Security Executive	Cyber Security Adviser	Portfolio Scope
ADSTC	CJOPS	ADSTC	HICTO	ASICTS	ADSTC Training and Simulation systems
ASD	TBD	TBD	TBD	TBD	TS systems
AGO	TBD	TBD	TBD	TBD	AGO systems
DIO	TBD	TBD	TBD	TBD	DIO systems
Industry (DISP)	ITSA	ICTSB	N/A	N/A	Defence industry systems

4. Certification Authorities

Area	Functional Appointment
ICTSB	ASICTS
462SQN	CO462SQN
ADSTC	DGADSTC (J7)

Note: In the above tables, TBD = To Be Determined.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Certification and Accreditation Appointments
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	ICT Certification and Accreditation
DSPF Number	Control 23.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

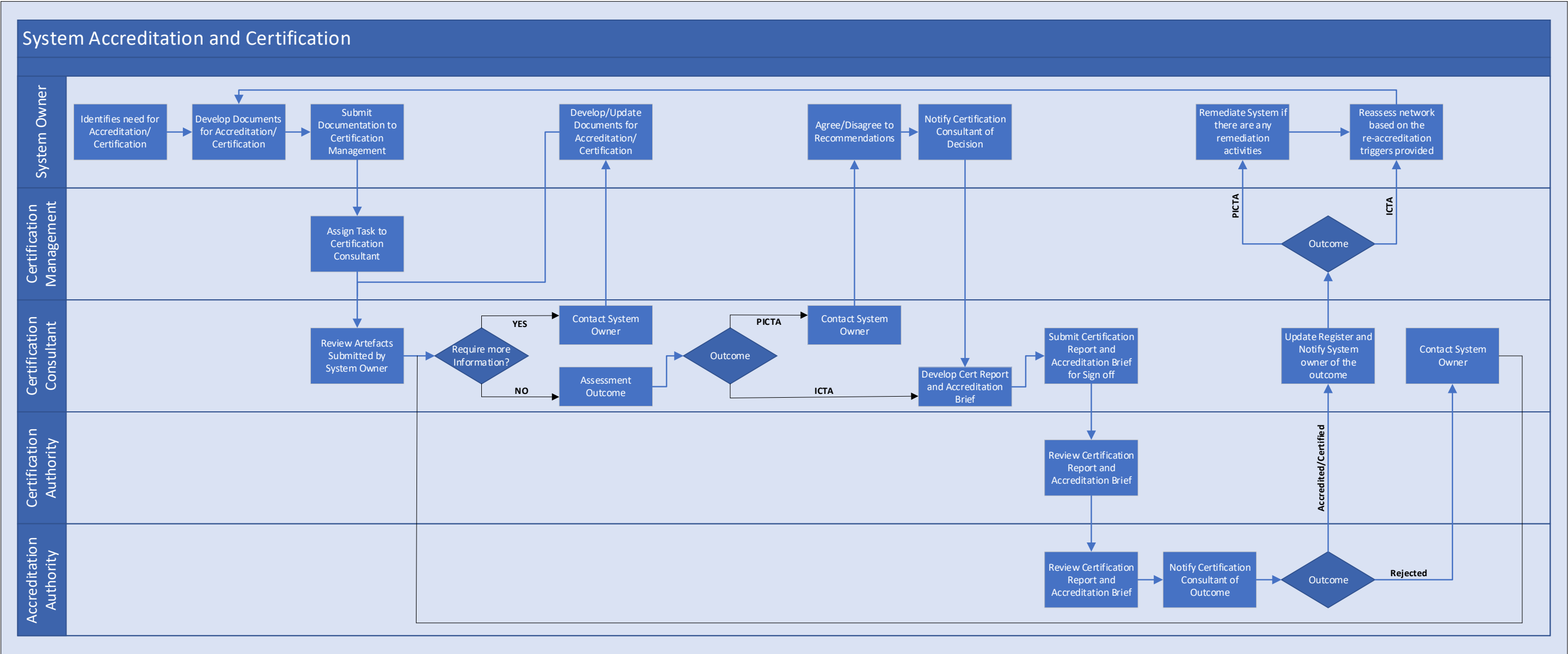
Defence Security Principles Framework (DSPF)

Annex B to ICT Certification and Accreditation – Defence Certification and Accreditation Process

System Accreditation and Certification Flow Chart

1. The following flow chart (Figure 1) lays out the process to be followed in the Certification and Accreditation process.

Figure 1: The Defence Certification and Accreditation Process



Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Defence Certification and Accreditation Process
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	ICT Certification and Accreditation
DSPF Number	Control 23.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update Figure 1 to better image quality



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Security Incident Management

General principle

1. Security incidents on Defence information systems require specialist management, as they can be difficult to detect, may affect large volumes of information in short timeframes, and are not dependent on physical proximity to the targeted asset.

Rationale

2. Information Systems security incidents may affect the confidentiality, integrity or availability of Information and Communication Technology (ICT) systems. This could result in harm to Defence capabilities, resources, reputation or people.

3. The appropriate management of security incidents involving information systems is important, not only for minimising the harm caused by the incident, but also for understanding Defence's security posture and preventing similar occurrences in the future.

Expected outcomes

4. Incident management processes are pre-planned and considered as part of the ICT certification and accreditation process.

5. Defence ICT system vulnerabilities to security incidents are identified.

6. The harm caused by incidents is reduced through suitable first response processes.

7. Defence manages security incidents involving information systems across all phases of the incident's life cycle in order to:

- a. minimise the impact of the specific incident;
- b. inform continuous improvement of protective measures and controls;
- c. inform understanding of the Defence security posture; and
- d. ensure people are held accountable for their actions.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1 AND reported to Chief Information Officer Group (CIOG) Defence Security Operations Centre (DSOC)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation and reported to CIOG DSOC
Moderate	Director ICT Security Management/Defence Information Technology Security Managers (ITSM) and reported to CIOG DSOC	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation and reported to CIOG DSOC
Significant	Defence Information Technology Security Advisor (ITSA) and reported to CIOG DSOC	Appointed Group or Service Cyber Security Advisor and reported to CIOG DSOC Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO) and reported to CIOG DSOC	Appointed Group or Service Cyber Security Executive and reported to CIOG DSOC Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division) AND reported to CIOG DSOC	Appointed Group Head or Service Chief and reported to CIOG DSOC

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems Security Incident Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 24
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 24.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Protective Marking of information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems; Entity physical resources; and Entity facilities Australian Government Information Security Manual (ISM) <u>Legislation:</u> Privacy Act 1988
Read in conjunction with	N/A
See also DSPF Principle(s)	Protective marking and Protecting Official Information Release of Official Information Physical Security Security Incidents and Investigations Escorting Security Protected or Classified Assets
Implementation Notes, Resources and Tools	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Security Incident Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The ITSA has set the following general threshold for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Information Communication and Technology (ICT) Security Branch EL1 AND reported to Chief Information Officer Group (CIOG) Defence Security Operations Centre (DSOC)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation <u>and</u> reported to CIOG DSOC
Moderate	Director ICT Security Management/Defence Information Technology Security Managers (ITSM) <u>and</u> reported to CIOG DSOC	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation <u>and</u> reported to CIOG DSOC
Significant	Defence ITSA <u>and</u> reported to CIOG DSOC	Appointed Group or Service Cyber Security Advisor <u>and</u> reported to CIOG DSOC Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO) <u>and</u> reported to CIOG DSOC	Appointed Group or Service Cyber Security Executive and reported to CIOG DSOC Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division) <u>and</u> reported to CIOG DSOC	Appointed Group Head or Service Chief <u>and</u> reported to CIOG DSOC

Note: *Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

3. This Control provides guidance specific to information systems security incident management across Defence and Defence industry. Unless stated otherwise the content refers to incidents that involve, or have a direct impact on, ICT and information systems used to store or process official information. For security incidents generally, refer to DSPF Principle 77 – *Security Incidents and Investigations*.
4. Methods of incident detection are to include both technical and non-technical means. The application of suitable first response processes will reduce the impact of an incident.
5. Incidents are to be reported in a timely manner, and may be referred for formal investigation – see DSPF Principle 77 – *Security Incidents and Investigations*.
6. Incident responses are to be proportionate to the business impact of the event and will be conducted in a manner that does not prejudice a formal investigation if required.
7. Defence is to make use of incident information and lessons learned to reduce the likelihood and consequence of future incidents.

Security Violation, Breach, Infringement Investigation and Management

8. In accordance with the Protective Security Policy Framework (PSPF), Defence is to identify and understand security threats in order to determine risks to its people, information and assets. A security investigation will establish the cause and extent of an incident that has, or could have, compromised the Australian Government.
9. All security incidents within the Single Information Environment (SIE) are to be reported using an XP188 – *Security Incident Report*, refer DSPF Principle 77 – *Security Incidents and Investigations*.

Note: *Investigations may only be conducted by a Defence Investigative Authority (DIA). DS&VS is the DIA responsible for managing security investigations.*

10. In addition to PSPF requirements, the [Privacy Act 1988](#) requires Defence to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This is established under the Notifiable Data Breaches (NDB) scheme. Defence has an obligation to ensure a process is in place to ensure the NDB is applied.

Security Incident Response Requirements

11. The Control Owner is responsible for ensuring all reported security incidents contain appropriate information and, where required, are investigated and dealt with in accordance with the relevant policies and legislation.

12. Reportable incidents include:
- a. incidents suspected of constituting criminal offences (reportable to the appropriate law enforcement authority);
 - b. incidents suspected of involving the compromise of information or assets classified at or above SECRET (reportable to Australian Security Intelligence Organisation);
 - c. major ICT incidents (reportable to Australian Signals Directorate (ASD)); and
 - d. incidents involving the compromise of Cabinet material (reportable to the Cabinet Secretariat).

Incident Lifecycle

13. Information system security incidents are to be managed across the following lifecycle phases (more detail regarding these phases is below):
- a. Prevention and Preparation;
 - b. Detection;
 - c. First Response;
 - d. Reporting, Assessment and Triage;
 - e. Remediation and Recovery; and
 - f. Analysis and Lessons Learned.

Prevention and Preparation Phase

14. Systems are to be covered by an Incident Response Plan (IRP). The size and complexity of the system determines whether an individual system requires its own IRP.

Note: A fleet of laptops delivering the same capability may be covered by one IRP, rather than having one plan per laptop. Larger, more complex systems may need an individual plan. Some very large, complex systems may need individual IRPs to cover various aspects of the system. In any case, all systems need to be covered by a suitable IRP.

15. IRPs comprise one element of the documentation suite required for system certification and accreditation and are to meet the requirements of the IRP section of the Information Security Manual ([ISM](#)).
16. IRPs are to address both technical and non-technical means of incident detection.

Detection Phase

17. ICT Security incidents may be detected through technical or non-technical means.

18. Examples of technical means include:

- a. alerts generated by intrusion detection or anti-virus tools;
- b. analysis of log files; and
- c. forensic analysis of a system, device or network traffic.

19. Examples of non-technical means include:

- a. self-reporting by system users;
- b. overt indicators such as defaced web sites;
- c. recovery of material or storage media not previously reported as lost; and
- d. information reported through media or on public websites.

20. Further information can be found in the Detecting Cyber Security Incidents section of the [ISM](#).

First Response Phase

21. An optimal first response to an ICT security incident will:

- a. contain the harm caused by the incident,
- b. preserve digital evidence;
- c. maintain business continuity; and
- d. facilitate recovery and remediation.

22. In addition to the requirements of the IRP Section of the [ISM](#), system specific IRPs are to document:

- a. the types of incidents anticipated;
- b. the most appropriate action(s) to minimise the harm of each anticipated incident, and processes for managing incidents that were not anticipated or are outside the capability of first responders;

- c. the conditions under which a system can and cannot be shut down or isolated;

Example: A system with high availability requirements might have adverse effects on critical operations or personal safety if shut down.

- d. alternative methods of harm minimisation if the system cannot be isolated; and
- e. connected systems that might be affected as a result of an incident, including points of contact for those systems.

23. Actions undertaken during the first response phase are to be documented for use in later incident management phases.

Reporting and Triage Phase

24. All security incidents in Defence are to be reported in accordance with:

- a. DSPF Principle 10 – *Assessing and Protecting Official Information*;
- b. DSPF Principle 77 – *Security Incidents and Investigations*;
- c. System IRPs and any relevant Standard Operating Procedures (SOPs), and
- d. [Privacy Act 1988](#).

25. System or capability owners are to report cyber security incidents to ASD in accordance with the Reporting Cyber Security Incidents section of the [ISM](#), and copies of any such reports provided to the First Assistant Secretary Security and Vetting Services (FAS S&VS).

26. If an ICT security incident affects multiple agencies, the Defence ITSA is to coordinate management activities with counterparts in those agencies.

27. Security incidents that do not cause harm could indicate a weakness in a control. These incidents are to be recorded to assist with continual improvement and improve security performance.

Example: Unsolicited email may be blocked by gateways in large volumes. As they have not reached their intended recipient and do no harm in their own right, they do not need to be reported individually. However they should be recorded in aggregate in order to inform trend analysis of potential malicious activity.

28. Security incidents where data breaches of personal information are likely to result in serious harm, could also indicate a weakness in a control. These incidents must be reported to the Privacy Office in addition to all other mandatory reporting.

Remediation and Recovery Phase

29. The objective of the remediation and recovery phase is to return affected systems to their normal operation or state prior to the incident, consistent with any requirement to maintain evidence for use as part of an investigation.

30. Evidence must be collected, protected and preserved during the remediation process in accordance with Defence Investigative Standards and DIA directions.

31. If the integrity of a system is compromised, it must be returned to a trusted state before continuing to process Defence information.

Example: *If the integrity of a system is compromised by a malicious code infection, it may need to be rebuilt using trusted images and backups.*

32. In the event of a data spill, remediation may require the sanitisation or destruction of electronic storage media. When required this must be performed in accordance with the Media Security section of the [ISM](#).

33. Any authenticators that are suspected to have been compromised as part of the incident must be changed in a manner that is not predictable given knowledge of the compromised authenticators.

34. Further remedial activities can be found in the Managing Cyber Security Incidents section of the [ISM](#).

35. Where cyber security incidents have been reported to ASD, remediation must be performed in accordance with any advice from ASD.

Analysis and Lessons Learned Phase

36. Analysis of incident data is to be used to inform improvements to system Security Risk Management Plans (SRMPs) and SOPs. It is recommended that this analysis consider:

- a. the adequacy of existing processes;
- b. the degree to which processes are followed;
- c. the degree of exposure to similar incidents; and
- d. whether or not the incident, or any resulting investigation, has highlighted the need for additional logical, physical or personnel security controls.

37. The occurrence of an incident that was not previously identified in an IRP should be analysed for inclusion in future versions of the plan. It is recommended that this analysis consider:

- a. the means by which the incident was detected, and whether or not this is a reliable way to detect future occurrences;

- b. the suitability of first response activities;
- c. the suitability of reporting mechanisms; and
- d. whether or not this type of incident could affect any other Defence systems. If another Defence system is affected, the ITSA is to be notified to enable the risk to be managed.

Investigations

38. Formal investigation of incidents must only be conducted by a Defence Investigative Authority (DIA). The DIAs responsibilities are specified in DSPF Principle 77 – *Security Incidents and Investigations*.

39. Although other areas of Defence may provide advice or support to a DIA, their actions must only be performed under the authority of the DIA.

40. A system manager may receive a request from a Defence Investigative Authority to provide activity logs for use in an investigation.

Roles and Responsibilities

Chief Information Officer (CIO)

41. As the capability manager for the Single Information Environment (SIE), the CIO is responsible for setting the strategic direction of the SIE. This includes the management of information systems security incidents.

Chief Information Security Officer (CISO)

42. The CISO is responsible for:

- a. ensuring that incident management processes are integrated into the normal operation of the SIE;
- b. providing data on information security incidents as part of Defence security performance reporting; and
- c. Liaising with the FAS S&VS and Service Executive Security Advisors (ESAs) to ensure that information systems security is integrated with broader protective security strategies, policies, and plans.

Information Technology Security Adviser (ITSA)

43. The Defence ITSA is responsible for:

- a. liaising with counterparts in other agencies affected by an incident; and
- b. Coordinating ITSMs to remediate security incidents, in accordance with established procedures or direction from the relevant DIA.

Information Technology Security Managers (ITSM)

44. ITSMs are responsible for:
- a. ensuring that any identified security incidents are reported;
 - b. supporting DIAs by facilitating requests for information; and
 - c. conducting remedial activity as directed by system owners, the ITSA or a DIA.

Information Technology Security Officer (ITSO)

45. ITSOs are responsible for:
- a. conducting first response activities in accordance with system management SOPs in order to minimise the harm caused by a security incident;
 - b. reporting any incidents identified during the course of their duties; and
 - c. complying with instructions from a relevant DIA. This may include provision of technical advice to the DIA, provision of system logs or other artefacts or conducting remedial activity to address the incident.

Defence Intelligence Security

46. [DIS](#) is responsible for:
- a. planning for, detecting, and remediating security incidents within their area of responsibility; and
 - b. reporting identified incidents to the FAS S&VS.

System Owners

47. System owners are responsible for:
- a. ensuring systems are covered by IRPs as part of the suite of system documentation considered during certification and accreditation;
 - b. monitoring the effectiveness of security controls and refining the controls or their configuration based on identified incidents;
 - c. ensuring security incidents are remediated in order to return a system to normal operation in accordance with established procedures or direction from the ITSA, a DIA or an ESA; and
 - d. refining security risk management plans, SOPs and incident response plans as a result of lessons learnt from security incidents.

System Managers

48. System managers are responsible for:
- a. operating information systems in accordance with plans and procedures approved during system accreditation;
 - b. monitoring systems under their control for events that may indicate a security incident;
 - c. reporting any detected incidents;
 - d. supporting investigations as directed by a DIA;
 - e. performing remedial activity in accordance with established procedures or as directed; and
 - f. enacting security controls to prevent further occurrences, if required.

Certification Authorities

49. Certification authorities are responsible for:
- a. assessing system specific incident management processes documented in SRMPs, SOPs and IRPs Plans against applicable policy requirements and identifying any deficiencies;
 - b. providing technical advice to system owners on methods to improve incident management; and
 - c. factoring documented incident management processes into recommendations for the accreditation authority.

Accreditation Authorities

50. Accreditation authorities are responsible for:
- a. ensuring certification activities have been adequately performed; and
 - b. deciding whether or not to accept the risk(s) of operating a system.

System Users

51. System users are responsible for:
- a. using information systems in accordance applicable procedures;
 - b. reporting any security incidents they become aware of; and
 - c. complying with instructions from the DS&VS, DIA, or entities acting on behalf of DIA.

Privileged Users

52. In addition to the responsibilities of a system user, privileged users are responsible for:
- a. minimising the use of their privileges in order to limit the impact of a security incident;
 - b. noting their level of privilege when reporting a security incident; and
 - c. performing system administration tasks in support of incident remediation as directed by the system manager.

Key Definitions

53. **Data Spill.** The spillage of information onto a system not accredited to handle it. This can include higher classified information found on less classified networks, and breaches of need-to-know requirements where users are exposed to data they are not authorised to access.
54. **Event.** An occurrence that may have security implications and potential for harm to Defence information, capability, resources, reputation or people. All security incidents are events, but not all events are security incidents.
55. **Information Communications and Technology (ICT).** Encompasses any medium used to record, process, store and transfer information. This includes:
- a. data storage devices (e.g. magnetic disk/tape, compact disks/digital video disks, flash memory, etc.);
 - b. technology used for transferring or communicating information; and
 - c. operating systems, hardware and software applications used to operate networks and systems.
56. **Incident Management.** The process of addressing a security incident across its entire lifecycle.
57. **Information System (or ICT) Security Incident.** Also referred to as cyber security incidents within the ISM, these are unwanted or unexpected events that:
- a. are caused by, or impact on, an ICT system or its supporting infrastructure; and
 - b. may cause harm to Defence information capability, resources, reputation or people.
58. **Incident Response.** Actions taken after the detection of a security incident to minimise the harm caused.

59. **Major Security Incident.** A Major security incident is any deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of official information or assets. Examples include:

- a. the loss of material classified SECRET or above, or significant quantities of material of a lower Protective Marking;
- b. actual or suspected hacking into any information and communications technology (ICT) system;
- c. compromise of security keys or combination locks;
- d. actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored; or
- e. repeated incidents involving the same person or work area where the combination of the incidents warrants an investigation.

60. **Minor Security Incident.** A Minor security incident is an accidental or unintentional action involving failure to observe protective security policy mandatory requirements or procedures within the DSPF. Examples include:

- a. access passes or identification documents lost or left insecure; or
- b. security classified material not properly secured or stored.

61. **Security Incident.** Any event that prejudices security and/or breaches security regulations. Security incidents might be deliberate, negligent or accidental, and are often the result of a failure to comply with security policy.

Further Definitions

62. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Security Incident Management
Control Owner	ITSA
DSPF number	Control 24.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Security Incident Management
Related DSPF Control(s)	Protective Marking and Protecting Official Information Release of Official Information Physical Security Security Incidents and Investigations Escorting Security Protected or Classified Assets

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Business Impact Levels and Aggregation

General principle

1. Defence will protect information systems through the implementation of personnel, logical and physical security controls determined by Business Impact Level (BIL) assessments.

Rationale

2. BILs provide a consistent approach to assessing the business impacts arising from the loss or compromise of confidentiality, integrity or availability of Australian Government resources. They provide the level of detail needed to assess the business impacts for a wide range of Australian Government responsibilities and give clear, understandable definitions of business impact;
3. BILs enable consistent risk-based decisions to be made by providing a standardised measure for determining the degree of impact to Defence; and
4. BILs are especially useful when managing information security where aggregation and the distinction between BILs for confidentiality, integrity and availability need to be carefully managed to ensure appropriate security measures are applied.

Expected outcomes

5. Defence information systems and, when necessary, sub-components are categorised using BILs;
6. Defence and Defence Industry information systems that store, process or communicate Official Information are assigned BILs for confidentiality, integrity and availability;
7. BILs are used:
 - a. to determine and inform the minimum level of protection required for information systems;

- b. to select and implement appropriate personnel, logical and physical security controls;
 - c. to inform information system certification and accreditation decisions;
 - d. as a primary mechanism for determining an information system's criticality rating;
8. Defence identifies information systems that have an increased likelihood of having their confidentiality, integrity and availability compromised due to:
- a. the value and/or volume of information held;
 - b. the capability provided by the information system; or
 - c. the context and environment in which the information system operates; and
9. Defence will ensure additional security controls and protective measures are implemented for those information systems, as appropriate.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Accreditation Authority (must be SES 1/1* or above)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Accreditation Authority (must be SES 1/1* or above)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Accreditation Authority (must be SES 1/1* or above)	Appointed Group or Service Cyber Security Advisor. Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	SES 2/2*	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence Chief Information Security Officer (CISO) will be the appropriate escalation point
Extreme	SES 3/3*	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems Business Impact Levels and Aggregation
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 25
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 25.1
Control Owner	Information Technology Security Advisor

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Protective Marking of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information ICT Certification and Accreditation Physical Transfer of Information and Assets Physical Security Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government information security management guidelines—Australian Government security classification system – provides guidance to assist agencies to identify the value of information and in turn apply a suitable protective marking; Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information and material – provides guidance on procedures for applying protective markings and information handling procedures; and Australian Government Information Security Manual – sets out the standard governing the security of Australian Government ICT systems.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Information Systems Business Impact Levels and Aggregation

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Business Impact Levels and Aggregation
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 25.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Business Impact Levels and Aggregation
Related DSPF Control(s)	Assessing and Protecting Official Information ICT Certification and Accreditation Physical Transfer of Information and Assets Physical Security Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Media Protection Security

General principle

1. Defence personnel are to ensure that all media that contains, or has contained, official information is managed appropriately to protect against unauthorised access and to protect the confidentiality, integrity and availability of the information held within.

Rationale

2. Removable media (i.e. thumb drives, DVDs, and CDs) represent unique security challenges due to its rapidly evolving nature and the ability for devices to capture, record, process and transmit large amounts of information in almost any conceivable format.

Expected outcomes

3. Defence personnel and persons engaged under contract are to ensure that all media that contains (or has processed) official, privacy, or Protectively Marked information within the SIE is protected and managed in accordance with the DSPF.

4. All media used within the Single Information Environment (SIE) is to be afforded a level of protection commensurate with the Protective Markings of information processed or stored and will be used in a way that will not compromise the Official Information or the security of Information and Communication Technology (ICT) systems.

5. The use of portable ICT assets and removable media will be risk managed in accordance with Australian Government requirements detailed in the Information Security Manual (ISM).

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Advisor Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Media Protection Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 26
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 26.1
Control Owner	ITSA

Related information

Government Compliance	PSPF Core Requirements: Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Foreign Release of Official Information Mobility Device Security Information Systems Security Incident Management Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government information security guidelines – Australian Government security classification system – provides guidance to assist agencies to identify the value of information and, in turn, apply suitable protective markings. Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and materiel – provides guidance on procedures for applying protective markings and information handling procedures. Australian Government Information Security Manual – sets out the standards governing the security of Australian Government ICT systems.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Media Protection Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the Control Owner of this enterprise-wide Control.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Advisor Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

2. Policy for using mobility devices outside of the office and, conducting remote access to Defence systems from both privately owned and Defence controlled devices may be found in:
 - a. DSPF Principle 22 – *Mobility Device Security*; and
 - b. DSPF Principle 30 – *Remote Access to Defence Systems*.

Accreditation of Mobility Devices and Removable Media

3. The ICT accreditation authority must approve the acceptable use and permitted configuration for devices, based on the policy requirements detailed in the Information Security Manual (ISM) and DSPF Principle 23 -ICT Certification and Accreditation.
4. Details of this use and configuration are to be provided for users in a system-specific Standard Operating Procedure (SOP).
5. The SOP or Defence Instruction developed during the accreditation process is to state the Protective Marking for the device in each functional state, according to the level of protection that is effective in that state.

Example: The SOP or Defence Instruction for a secure phone with embedded (Australian Signals Directorate (ASD)-approved encryption technology may specify that it is OFFICIAL when hardware is powered off and SECRET when in standby mode, screen locked or operational.

6. If removable media or other connectivity such as USB-connectivity is to be enabled on a mobility device that is approved for connection to a classified network, then the ICT accreditation authority is to confirm the device offers the same level of auditing and access control over its interfaces as offered by the network.

Example: A commercial Global Positioning System (GPS) unit is to be added to a network's approved device whitelist; it is necessary to determine that it won't be possible to use the device's removable media to subvert data transfer audit controls on the network.

7. Defence controlled devices are not to be connected to any other network or device unless they are specifically accredited to be.

Example: A Defence laptop supplied for remote access may be connected to the Internet.

Tracking and Recording of Mobility Devices

8. For mobility devices with an 'actual' classification of 'PROTECTED' and above, the Commander or Manager, or where appointed the Equipment Manager, is to record the location and issue in a suitable form, such as an asset register.
9. Where a mobility device is issued to an organisation for shared use, it is the Commander or Manager's responsibility to ensure that temporary loans and transfers are recorded.

Conduct of Data Transfers

10. The use of removable media and mobility devices to transfer information to, or from, SECRET and above systems presents an increased risk of compromise to both the information held on the system and the system itself. Inappropriate data transfers can impact on the confidentiality of information stored or processed by systems, as well as the integrity or availability of the system itself. It is therefore imperative that data transfer procedures are adhered to in all instances. Compromise may occur through inappropriate use, for example, using a removable media device to:

- a. copy Official Information from a system for the purpose of informing external actors; or
- b. propagate viruses that infect Defence ICT systems and collect Official Information for the purpose of espionage.

11. The use of removable media for data transfer on systems classified SECRET and above must be strictly limited and supported by an endorsed business case and risk assessment in accordance with the ISM.

12. Defence business cases **must** be endorsed by a SES band 1/O7 or their designated delegate.

13. In the case of Defence Industry Security Program (DISP) members, the position(s) and level(s) within a company that may endorse a business case with respect to those companies' networks may be negotiated with the ICT accreditation authority and must be included in the system's accreditation documentation.

14. In order to ensure individual accountability for the conduct of data transfers, every data transfer to, or from, systems classified SECRET and above are to be audited in accordance with ISM Controls. Auditing may occur via electronic logging or via a manual system.

15. In accordance with the [ISM](#), data transfers between Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) systems and foreign systems must:

- a. be reviewed by two people, one of whom is not the originator of the information to be transferred; and

Exclusion: Where the transfer is conducted via an accredited gateway it is excluded from this requirement. Protection of AUSTEO and AGAO information in these circumstances is the primary responsibility of the author of the information, and is supported by technical monitoring measures in the gateway.

- b. undergo key word scanning (scanning is to be configured to include metadata such as deleted text).

16. Rewriteable media should not be used to conduct data transfers to, and from, systems classified SECRET and above in accordance with the [ISM](#). The recommended media for this purpose is write once optical media.

Note: This is done to assist in the prevention of malware/viruses propagating to classified networks via removable media.

17. Removable media with an 'actual' classification of SECRET and above is to be recorded in a Classified Document Register (CDR) or a Data Transfer Register. This ensures the files and the media are physically accountable even if encrypted.

Note: This additional accountability is especially relevant for encryption schemes that use shared keys that permit multiple users access. In these circumstances, the loss of encrypted media during transit does not guarantee that the information is secure from trusted insiders who have the means to decrypt the information. If loss is detected then audit logs can be checked to see if it was subsequently accessed.

Limiting Data Held on Mobility Devices and Removable Media

18. Removable media are not to be used for permanent data storage, except as required by System Administrators for backup and disaster recovery purposes. Information held on mobility devices and removable media is not backed up and will not be archived unless the user transfers the information onto corporate systems such as the SIE. Users of these devices are responsible for backing up and archiving data held on mobility devices and removable media.

Exclusion: This only applies where a backup data synchronisation regime is not place.

19. In order to limit the potential information compromise from the loss or theft of mobility devices and removable media, all users are to limit data stored on these devices to that which is essential to their immediate activity. It is further recommended that:

- a. mobility devices and removable media have their user data storage areas overwritten before being reassigned to another user; and

Note: Multi-pass secure deletion software is recommended for these purposes. Such software may not meet sanitisation requirements of the ISM but can significantly reduce the risk of other cleared users accessing remnant data.

- b. users review the content of their mobility device and removable media at regular intervals; unnecessary data is to be removed from the device or media.

20. The accumulation of classified removable media or mobility devices that are no longer required is a serious security risk. It is recommended that organisations audit their mobility devices and removable media holdings annually and return or destroy devices/media that are surplus to operational requirements in accordance with the disposal section below.

Physical protections for Mobility Devices and Removable Media

21. All users are to follow removable media procedures documented in the system SOP or Defence Instruction. If a SOP or Defence Instruction has not been supplied for the system then users are to follow the procedures contained in the [ISM](#) Media Security section which contains policy for the labelling, storage, handling, sanitisation and destruction of media.
22. Some removable media (such as micro Secure Digital (SD) cards) are too small to label with any meaningful security markings. The use of such media is strongly discouraged unless there is a clear operational requirement to do so. In such cases, the handling and protection of these media is to be specifically addressed in SOPs or a Defence Instruction. Consideration may be given to:
- purchasing media incorporating embedded security features that can be recorded; and
 - applying suitable tamper evident mechanisms, such as seals, to the device containing the media and treating the media and device in combination as a classified item.
23. The handling and protection of Official Information (including mobility devices and removable media) is required to comply with the procedures for handling and protecting Official Information during use, storage, transfer and transmission as outlined in the DSPF Principle 10 – *Assessing and Protecting Official Information*.
24. Physical storage measures for ICT equipment may be reduced by using ASD-approved encryption that reduces the 'handle-as' classification of electronic devices and media to a lower classification.

Example: Where a High Grade Silicon Data Vault (HGSDV) encrypted laptop uses ASD-approved encryption to reduce the device from 'SECRET' to 'OFFICIAL', a safe is not required to store the device when powered off, but the device still needs to be protected from theft.

25. Where suitable ASD-approved encryption is not in use or is not active, mobility devices and removable media is to be stored, transferred and handled in accordance with the 'actual' Protective Marking.
26. Mobility devices and removable media are at greatest risk when being transferred outside secure facilities. In accordance with [ISM](#) controls, ASD-approved encryption should be used for all removable media.

Disposal of Mobility Devices and Removable Media

27. Incorrect disposal of mobility devices and removable media introduces a significant risk that Non-Volatile Media containing Official Information may be compromised. The hard disk or flash memory in mobility devices can contain large quantities of Official Information. Therefore, any applicable disposal plan for the device **must** be followed.

28. Normally, a device is disposed of by the equipment manager; however, if the device has no equipment manager and a disposal plan has not been developed, the commander or manager becomes responsible for carrying out media sanitisation/destruction to the standards specified in the [ISM](#) Media Security section.
29. Controlled Cryptographic Items (CCI) are marked with a CCI sticker. CCI have specific accountability and disposal requirements. CCI are to be returned to the relevant COMSEC custodian when no longer required.
30. Removable Media that has stored Official Information that is not authorised for public release must be declassified or destroyed.
31. Sanitisation/destruction must meet the requirements outlined in the [ISM](#) Media Security section.

Note: Care is to be taken when using Security Construction and Equipment Committee (SCEC) approved optical disk shredders. Older optical disk shredders may remove only the first layer of a multi-layer optical disk leaving the second deeper layer intact. In the case of Blue-Ray disks this can leave up to 25GB of data recoverable from the disk. Other common mistakes include shredding the wrong side of the disk, in the case of writable disks (CD-RW, DVD±RW, Blu-Ray R etc.) the data is written to the printed label of the disk. The label 'top' of the disk is to be destroyed.

32. Media protected by ASD-approved encryption is sanitised/destroyed in accordance with the media's 'handle-as' classification. Where the media has an 'actual' classification of 'SECRET' or above, sanitisation/destruction is to be recorded in the accompanying CDR or data transfer log entry.
33. When a DISP member uses their own computing and other electronic equipment in order to process official information that is not authorised for public release, including Dissemination Limited Material, the equipment is subject to the DSPF and [ISM](#). On termination of a contract, or when the equipment is disposed of, the equipment **must** be sanitised to 'OFFICIAL' in accordance with the requirements of the ISM Media Security section.

Note: Some hardware cannot be declassified to 'OFFICIAL' without the complete destruction of the device or its components. In these instances declassification is conducted using an ISM-approved destruction method (that reduces the resulting waste product to 'OFFICIAL'). Alternatively, it may be surrendered to the Commonwealth.

Privately Owned Mobility Devices and Removable Media

34. Refer to DSPF Principle 22 – *Mobility Device Security* for details on the use of privately owned mobility devices within Defence.
35. Refer to DSPF Principle 30 – *Remote Access to Defence Systems* for details on the use of privately owned mobility devices for remote access within Defence.
36. Privately owned mobility devices and removable media that have inadvertently been contaminated with sensitive or classified material must be sanitised in accordance with the [ISM](#). In order to avoid contamination, it is

recommended that a Defence owned mobility device or removable media be used where there may be a potential for the accidental contamination of the device with sensitive or classified information.

Cordless Phones

37. [ISM](#) section Telephones and Telephone Systems contains the mandatory standards for the use of cordless phones. Defence Voice Services approve the use of cordless phones and answering machines on Defence telephony networks.

Mobile Phones and Other USB Powered and Rechargeable Devices

38. Refer to DSPF Principle 22 – *Mobility Device Security* for details on the use of mobility devices within Defence.

Media Sanitisation

39. All media containing Defence Official Information must be sanitised before the Media changes ownership, is re purposed to a lower classified network, or disposed of at end of life.

Removable Media Management and Control

40. Defence personnel and persons engaged under a contract are required to ensure that any removable media within their custody and used in conjunction with the Defence networks is managed and controlled in accordance with the following:

- a. The removable media is not to be used in conjunction with the Defence Networks;
- b. Only the minimum quantity of removable media necessary to satisfy their Defence Networks data transfer requirements is to be held;
- c. All removable media items are to be classified to at least the highest Protective Marking ever stored on the media, or since the media was last declassified/sanitised;
- d. Where AUSTEO information has been stored on the removable media, the Protective Marking of the media will not be downgraded for the life of the media;
- e. All removable media items are to be labelled with a Protective Marking according to its classification;
- f. Registered media items are to be mustered at random intervals not exceeding six (6) months;
- g. All removable media are to be transported in accordance with the relevant requirements of DSPF Principle 71 – *Physical Transfer of Official Information and Assets*; and

- h. All removable media are required to be disposed of / destroyed at the end of their required life in accordance with the relevant requirements of DSPF Principle 10 – Assessing and Protecting Official Information.

Single Information Environment –‘PROTECTED’ and Below Administration

41. All items of fixed storage media (e.g. hard disk drives, remote management cards) utilised within SIE equipment (server, workstation, etc.) that is classified as ‘PROTECTED’ or below are to be labelled with a Protective Marking of “WARNING - This item to be handled as ‘PROTECTED’, NOT for release and to be destroyed at end of life” when deployed for use.
42. An Information System Security Register (ISSR) is to be maintained for each site. All SIE Server hard disk drives within a site are to be registered within the site ISSR using the manufacturer’s serial number as the item Reference Number, and noting the drive’s location, server and asset number within the item remarks.
43. SIE hard disk drives, when removed from SIE equipment (server, workstation) that is classified as ‘PROTECTED’ or below – including network attached storage or storage area networks – are to be deemed as having been contaminated by a data spill during their operational lives. This is unless it can positively be confirmed otherwise. Accordingly, the hard drives are to be reclassified and re-labelled as “PROTECTED CONTAMINATED”, at a minimum, and handled accordingly.

Single Information Environment –‘SECRET’ and Above Administration

44. All items of fixed storage media (e.g. hard disk drives, remote management cards) utilised within SIE ‘SECRET’ and above equipment (server, workstation, etc.) are to be labelled with a security marking of ‘SECRET AUSTEO’ when deployed for use.
45. Holdings of ‘SECRET’ and above classified media (both fixed and removable) and equipment are to be mustered and audited:
- a. annually – 100% of holdings;
 - b. monthly – spot checks of holdings; and
 - c. on any changeover of media / equipment custodian(s) – 100% of holdings.
46. A Classified Media Register (CMR) is to be maintained for each site (using an XC040 – Classified Document Register). All SIE ‘SECRET’ and above hard disk drives within a site are to be registered within the site Classified Media Register using the manufacturer’s serial number as the item Reference Number, and noting the drive’s location, workstation/server, and asset number within the item remarks. All hard disk drives are to be labelled with a CMR label detailing the CMR and line item references.

47. SIE hard disk drives, when removed from a 'SECRET' workstation or server (including network attached storage or storage area network), are to be deemed as having been contaminated by a data spill during their operational life unless it can positively be confirmed otherwise. Accordingly, the hard drives are to be reclassified and re-labelled as 'SECRET AUSTEO' CONTAMINATED.

Off-line Handling

48. Site CMRs are to be updated to reflect the current storage location of the hard disk drives.

Off-line Handling – 'PROTECTED' CONTAMINATED

49. As soon as practicable after relabelling, 'PROTECTED' CONTAMINATED hard disk drives are to be transferred to the nearest suitable Defence 'SECRET' facility pending relocation for destruction. Transfers are to be undertaken in accordance with DSPF requirements for SAFEHAND (movement and accounting). This will involve acquittal of the drives from the ISSR.

50. All movement of 'PROTECTED' CONTAMINATED hard disk drives are to be under the direction and coordination of the ICT Regional Engagement Office and undertaken in accordance with DSPF SAFEHAND requirements.

Off-line Handling – 'SECRET AUSTEO' CONTAMINATED

51. As soon as practicable after relabelling, 'SECRET AUSTEO' CONTAMINATED hard disk drives are to be transferred to the nearest suitable Defence facility pending relocation for destruction. Transfers are to be undertaken in accordance with DSPF requirements for SAFEHAND (movement and accounting). This will involve acquittal of the drives from the site CMR.

52. All movement of 'SECRET AUSTEO' CONTAMINATED hard disk drives are to be under the direction and coordination of the ICT Regional Engagement Office and undertaken in accordance with DSPF SAFEHAND requirements.

Storage

53. Central and Regional SIE administration personnel are to make arrangements for the provision of security containers at each SIE site within their responsibility for the storage of SIE backup media and other system administration media. In doing so, SIE administration personnel are to ensure that secure storage for media is adequate to satisfy the following:

- a. **Physical security standards.** Security containers for SIE backup and other system administration media are required to be compliant with the standards applicable to the classification of the media as identified in DSPF Principle 72 – *Physical Security*.
 - (1) Security Containers for DSN backup media Protectively Marked 'SECRET AUSTEO' ('TOP SECRET' by aggregation) are required to be compliant with the standards applicable to 'TOP SECRET' material in conjunction with DSPF Principle 72 – *Physical Security*.
- b. **Space.** The secure storage is large enough to accommodate:
 - (1) all backup media for site;
 - (2) all systems administration media for site; and
 - (3) to the maximum extent possible provision of space for off-site storage of backup media for other sites within the Central Office Service Provider's responsibility.

Re-use

54. Hard drives reclassified to 'PROTECTED' CONTAMINATED may be redeployed for re-use within the SIE.

55. 'SECRET' CONTAMINATED hard disk drives are not to be considered for sanitisation and declassification for re deployment within lesser classified systems.

56. 'SECRET AUSTEO' hard drives may be scrubbed and redeployed within 'SECRET' or higher classified systems.

57. SIE server hard disk drives and data spilled hard disk drives are not to be considered for sanitisation and declassification for re-deployment within lesser classified systems.

58. Hard drives reclassified to 'SECRET AUSTEO' CONTAMINATED are not to be redeployed for re-use within the 'SECRET' environment. Hard drives reclassified to 'SECRET AUSTEO' CONTAMINATED may be redeployed for use within Defence 'TOP SECRET' networks.

59. Items of SIE equipment other than hard drives with permanent memory used for the storage of equipment network addresses, identities, remote access accounts and passwords (e.g. management components of network equipment, server remote access cards) are to be managed as per SIE hard disk drives. Such items of equipment are not likely to be contaminated by a data spill and hence are exempt from the requirements detailed above regarding management of 'PROTECTED' CONTAMINATED or 'SECRET AUSTEO' CONTAMINATED at the 'SECRET' level.

60. Central and Regional SIE administration personnel are to be responsible for managing all removable media associated with its SIE support activities. Such removable media includes (but is not limited to):

- a. SIE build media – software media (sensitive and classified) disseminated for the purposes of building and configuring SIE infrastructure;
- b. Backup media;
- c. Data Transfer media; and
- d. Media utilised for sundry administration activities.

61. All items of removable media are to be labelled with a security classification marking.

62. Backup media are to be Protectively Marked to the highest classification of the data written to the media and labelled accordingly.

Note: Sites that are considered to have data holdings warranting higher protection due to aggregation are to be certified and accredited in accordance with DSPF Principle 73 – Physical Security Certification and Accreditation.

63. Data transfer media are to be marked as per the highest Protective Marking of Official Information that has been stored on that media.

64. All movement of removable media is to be undertaken in accordance with the requirements of DSPF Principle 71 – *Physical Transfer of Information and Assets*. Movement of media classified 'SECRET' or higher is to be appropriately recorded in the relevant site CMRs.

65. A Classified Media Register is to be maintained for each site using an XC040 – Classified Document Register.

66. All items of removable media associated with 'SECRET' and above support activities that are classified 'SECRET' or higher are to be registered within the site CMR. Where an item of removable media is marked with a manufacturer's serial number that identification is to be used as the item Reference Number within the CMR entry.

67. All registered items of removable media are to be labelled with a CMR label detailing the CMR and line item references.

Disposal

68. No items of removable media associated with SIE support activities are to be considered suitable for public disposal.

69. Full backups are to be transferred to the custody of the regional Information Technology Security Officer (ITSO) for storage after 12 months of system being decommissioned in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information*.

70. Items of removable media contaminated by data spills are to be handled and stored at the level of the highest Protective Marking of data the media was exposed to, and disposed of in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information*.

71. All other items of removable media associated with SIE support activities classified PROTECTED or higher are to be transferred to the custody of the ITSO or delegate for destruction. Items transferred for destruction are to be clearly marked as being for destruction and are to be pre-prepared with destruction certificates so to minimise the need for nugatory accounting of items.

Control of Access

72. All access to site backup and other system administration media is to be under the positive control of the Central Office Service Provider. Backup and systems administration removable media is not to be secured within cabinets or vaults where ready access may be gained by other individuals utilising the storage space.

73. The storage should include provision for separate storage of:

- a. separate backup media series used for servers storing designated Closed Community of Interest material. Storage space for this material is to be under the positive control of only SIE administration personnel specifically approved for access; and
- b. media (backup or otherwise) impounded as part of handling security incidents or other departmental inquiries. Storage space for impounded media is to be under the sole positive control of the ITSO or delegate

74. Central and regional administration personnel are to maintain and promulgate for each SIE site within their responsibility, local procedures regarding control of access to secure storage for systems administration related removable media. As a minimum these procedures are required to incorporate the following:

- a. “Unescorted Access Lists” are to be maintained for security containers used for storage of backup media and other systems administration media;

- b. All personnel identified for unescorted access to security containers used for storage of SIE backup and other systems administration media are to be approved for privileged access to the SIE;
- c. Security containers holding SIE backup and other systems administration media are to be secured at all times;
- d. Where security containers for SIE backup and systems administration media are secured using key-locks, container keys are to be managed in accordance with the requirements detailed above for SIE server racks and network cabinets;
- e. Where security containers for SIE backup and systems administration media are secured using combination-locks, the combination is to be recorded for each container;
- f. For Central SIE administration personnel, container combinations are to be secured within wafer sealed envelopes, in the custody of the Regional ICT Security Manager;
- g. Container keys / combinations are to be required to only be releasable to SIE administration and support personnel identified on the “Unescorted Access List” for the container;
- h. Individuals not identified on the “Unescorted Access List” for security containers holding SIE Backup media are not to be provided any access to those containers nor media; and
- i. A copy of the procedure is to be maintained as part of the site security information within the security elements of the SIE Configuration Management database.

Roles and Responsibilities

ICT Accreditation Authority

75. With regard to media protection, the applicable ICT accreditation authority is responsible for:
- a. accrediting the portable ICT asset either as a stand-alone device or as a component of a system;
 - b. the removable media types and the conditions of use. These details will be provided to users in the form of SOPs or issued as Defence Instructions. A Defence Instruction may be issued to provide an umbrella policy across a number of systems, this approach helps to prevent repetition in individual system SOPs;

- c. all data transfer mechanisms to, and from, the system or device including, but not limited to, air-gapped data transfers, gateways and other connections. Instructions for the conduct of data transfers will be provided in the form of SOPs or issued as Defence Instructions and will cover the types of devices permitted for use, the systems to and from which data transfers may be conducted, and the procedures to be used to conduct data transfers. Accreditation of data transfer solutions will confirm that requirements contained in the [ISM](#) Data Transfers section are met or relevant;
- d. ensuring dispensations are in place;
- e. procedures for securing portable ICT assets and removable media during operation, storage and transit, against the requirements specified in the [ISM](#); and
- f. disposal procedures for classified portable ICT assets and removable media against the requirements specified in the [ISM](#).

76. 'TOP SECRET' areas including Sensitive Compartmented Information Facilities (SCIF) are mandatory portable ICT asset prohibited areas under the DSPF Control 72.1 – *Physical Security*. Within these areas the SCIF accrediting authority is responsible for accreditation of portable ICT asset policy and procedures with respect to those areas.

System Owner

77. The System Owner is responsible for the provision of an ICT system. Where portable ICT assets are procured through a Whole-of-Defence support contract, an Equipment Manager is to be appointed by the System Owner.

78. System Owners and/or Equipment Managers are responsible for:

- a. developing a through life support plan for the portable ICT asset;
- b. gaining and maintaining ICT accreditation for the device in accordance with DSPF Principle 23 – *ICT Certification and Accreditation*; and
- c. ensuring that all Defence-owned assets, whether on issue or transfer to individuals or stored pending issue, are accounted for.

Commanders and Managers

79. With respect to those areas of a base or facility that are not subject to mandatory portable ICT asset prohibitions enforced by an accreditation authority (for example TOP SECRET areas), a Commander or Manager may choose to implement additional portable ICT asset prohibited areas within their base or facility to address identified security risks.

80. Where a Commander or Manager chooses to implement additional portable ICT asset prohibited areas they are responsible for:

- a. conducting a risk assessment;
- b. development and approval of Security Standing Orders (SSOs) that include local policy on the operation and use of portable ICT assets in prohibited areas. Refer to DSPF Principle 72 – *Physical Security* for more information.

Information Technology Security Officers (ITSOs) and Information Technology Security Managers (ITSMs)

81. ITSOs or ITSMs may be appointed to assist the System Owner, or the Commander or Manager; to fulfil their ICT security responsibilities.

82. The decision to appoint an ITSO or ITSM is taken based on the complexity of ICT tasks to be performed. The use of the title ITSM reflects that specialist training or skill is required to perform the duties. When this is not the case it is more appropriate to name the position as a Security Officer.

83. ITSM positions were previously known as Information System Security Officers/Liaison Officers.

84. It is recommended that security duties be delegated in writing as responsibility always rests with the relevant position unless it is formally delegated. Examples of duties that may be delegated include:

- a. providing advice to Commanders and Managers regarding the use of portable ICT assets and removable media;
- b. maintaining a record of the location or private issue of portable ICT assets held by the organisation (an asset register may be used for this purpose);
- c. recording user details (name, device accessed and time of login) for portable ICT assets that use shared passwords (for example, those in a training laptop pool); and
- d. assisting users to sanitise, destroy or transfer for disposal, used electronic media which is no longer required (including hard disk drives, removable disk drives, and other removable media).

System Users

85. With regard to media protection, System Users are responsible for complying with DSPF Principle 22 – *Mobility Device Security* and DSPF Principle 26 – *Media Protection Security*, SOPs and Defence Instructions issued with mobile ICT devices and removable media.

Note: If users are unsure of how to securely store or operate a mobile ICT device or media, they are to seek support through the relevant IT Service Desk, Security Officer or ITSM.

Key Definitions

86. **Media.** A generic term for hardware that is used to store information.

a. **Volatile Media.** A type of media that is designed to lose information when power is removed.

Example: Random Access Memory (RAM) in a laptop computer.

b. **Non-Volatile Media.** A type of media that retains information when power is removed.

Example: The Hard Disk Drive (HDD) in a desk top computer.

c. **Removable Media.** Non-Volatile media that can be easily removed from a system and is designed for removal.

d. **Fixed Media.** Digital storage media not designed to be removed from the device during normal operation.

87. **Defence Controlled Device.** A device is under Defence control if it is owned by Defence or is subject to any agreement that legally binds the owner of the device to comply with all DSPF and ISM security policies. Defence controlled devices include security classified assets owned by DISP members.

Example: A DISP member supplies their own computer to process 'SECRET' information. DISP membership contractually obliges the company to comply with all Commonwealth policies and the DSPF.

Further Definitions

88. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Media Protection Security
Control Owner	ITSA
DSPF Number	Control 26.1
Version	3
Publication date	3 August 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Media Protection Security
Related DSPF Control(s)	Foreign Release of Official Information Mobility Device Security Information Systems Security Incident Management Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Update of language to reflect Defence Admin Policy; update protective marking to OFFICIAL
3	3 August 2020	AS SPS	Protective Marking update to align with PSPF –including removal of 'CONFIDENTIAL'



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Data Transfer Security

General principle

1. Defence and Defence industry are to ensure that Official information is transferred in a secure manner and are only received by the intended recipient.

Rationale

2. Defence needs to regularly transfer Official Information, Protective Marked assets to Defence and non-Defence locations both in Australia and overseas with secure means of transfer to reduce the risk of loss or compromise.

Expected outcomes

3. Data is shared in accordance with agreements or arrangements between the parties concerned.
4. Information is protected during its transfer.
5. The 'need to know' principle is considered in conjunction with the 'need to share' principle before transferring any information.
6. The security measures required to protect classified information and security-protected assets during transfer are determined.
7. Data transfers are accomplished via Information and Communication Technology (ICT) systems wherever possible.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Executive
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive
Extreme	Chief Information Officer (CIO)(responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems Data Transfer Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 27
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 27.1
Control Owner	Information Technology Security Advisor

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Access to Information, and Safeguarding Information from Cyber Threats. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Security for Projects Foreign Release of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Offshore and Cloud Based Computing
Implementation Notes, Resources and Tools	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Information Systems Data Transfer Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Executive
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive
Extreme	Chief Information Officer (CIO)(responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

Preferred Use of ICT systems for Official Information

2. It is recommended that transfer of Official Information is conducted over accredited ICT systems and networks, rather than by physical transfer. For further information on physical transfers, see the DSPF Principle 71 – *Physical Transfer of Information and Assets*.

Note: The transfer of a media device, such as a thumb drive or laptop, is considered a physical transfer.

3. Defence personnel are to ensure the intended recipient has the appropriate 'need-to-know' and the required level of security clearance before information is transferred, in accordance with the [Protective Security Policy Framework \(PSPF\) Information Security Management Guidelines](#).

4. Data should only be transferred to a system with a higher classification system when there is a legitimate business need. The data must be scanned for malicious content with up to date virus/malware definitions before being transferred.

5. If transferring data from a higher classified system to a system of lower classification the data is to be sanitised and redacted to ensure that the content is suitable for the destination systems classification. The transfer device used should not currently hold or have previously held data of a higher classification.

6. Commanders and Managers are to have in place formal exchange policies, procedures and controls to protect the exchange of information.

7. All activity relating to the import and export of information via removable media is to be recorded within system audit trails and monitored.

Information Security Checking Requirements

8. All Defence personnel and persons engaged under a contract should complete the following security checks on information being transferred to ensure that it is appropriate to release:

- a. **Malicious content checking.** All Data being imported and exported within the Single Information Environment (SIE) is to be scanned for viruses and other malicious content as part of the transfer process. The detection of a virus or other malicious software is to be reported in accordance ;
- b. **Approved File Types.** System Users are only to transfer approved file types to/from removable media across approved gateways with external systems. The detection of an illegal/unapproved file type will result in transfer of the identified file being blocked; and
- c. **Data Spillage.** System Users are to ensure the classified information is not inadvertently released.

Example: Many office automation packages retain the content of previous work (e.g. in tracked changes). To ensure classified information is not inadvertently released, System Users should use the “Save as” function to create a new copy of that document in a format that does not support hidden text (Rich Text Format, RTF, is recommended).

Release of Classified Material

9. Any release of information, including to other Australian Government, industry and foreign government systems, is to be compliant with DSPF Principle 10 – *Assessing and Protecting Official Information* and DSPF Principle 15 – *Foreign Release of Official Information*.

10. The release of classified material includes the presentation of briefings or demonstrations using the SIE that include the display of classified software or information.

USB Drives

11. These devices are for data transfer purposes only; they are not to be used as a storage medium.

Defence Approved USB Thumb Drives

12. Only Defence approved USB thumb drives are to be used within the SIE unless exclusion has been granted by ITSA/ITSM – ICT Security Branch (ICTSB). A list of Defence approved thumb drives can be found on the Directorate ICT Asset Management (DIAM) web portal.

USB Mass Data Transfer Service

13. Mass transfers may be performed using external hard drives. A Defence approved data transfer account will be required.

Decommissioned USB Thumb Drives

14. All decommissioned USB devices are to be disposed of in accordance to ICT disposal policy DEFLOGMAN, Part 2, Volume 5, Chapter 10.

Roles and Responsibilities

Commanders and Managers

15. Commanders and Managers are responsible for:
- ensuring that Official Information, Protectively Marked assets are handled, packaged and transferred in accordance with DSPF Principle 71 – *Physical Transfer of Information and Assets*; and
 - reviewing/approving Defence approved USB Device requests for their staff.

Fleet Management

16. Fleet management are responsible for:
- consulting with ITSM – ICT Security Branch on ICT security requirements for USB devices;
 - the procurement and management of Defence approved USB devices; and
 - assisting Regional ICT Security Manager to dispose of decommissioned USB devices.

System Owners

17. System Owners shall determine the security measures required to protect classified information and security-protected assets during transfer. Refer to DSPF Principle 71 – *Physical Transfer of Information and Assets*.

System Users

18. System Users are responsible for ensuring they only use Defence approved USB devices for data transfer within the SIE. No other USB devices (including charging personal mobile ICT devices) are to be connected to the SIE without approval from ITSM or their delegate.

Key Definitions

19. **Classified Asset.** A security-protected asset that meets the criteria for classification see DSPF Principle 10 – *Assessing and Protecting Official Information* for further details.
20. **Classified Information.** Official Information that meets the criteria for classification under the [Australian Government Security Classification System \(AGSCS\)](#).
21. **Media.** Media is a generic term for the components of hardware that are used to store information in digital form. Removable media can include (but is not limited to) floppy disks, hard disks, USB thumb drives, CDs, DVDs, etc.
22. **Official Information.** Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and persons engaged under a contract. It includes:
- Documents and papers;
 - Data;
 - The software or systems and networks on which the information is stored, processed, or communicated;

- d. The intellectual information (knowledge) acquired by individuals; and
- e. Physical items from which information regarding design, components or use could be derived.

23. **USB Thumb Drives.** USB Thumb drives is the term used to generally describe all forms of USB devices that, subject to being listed on the Defence approved USB devices list, can be connected to ICT resources within the SIE in order to establish a temporary drive for data transfer.

Further Definitions

24. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Data Transfer Security
Control Owner	ITSA
DSPF Number	Control 27.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information System Data Transfer Security
Related DSPF Control(s)	Assessing and Protecting Official Information Security for Projects Foreign Release of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Offshore and Cloud Based Computing

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Log Management

General principle

1. Defence must develop and implement an event logging strategy covering logging facilities, including availability requirements and the reliable delivery of event logs to secure centralised logging facilities.

Rationale

2. Logging events from critical systems, applications and services within the single information environment can help detect, attribute and respond to compromise. It also supports accountability.

Expected outcomes

3. Defence systems are configured to enable sufficient logging and audit capabilities to detect cyber security incidents, attempted intrusions and unusual usage patterns that are protected from modification and unauthorised access, and whole or partial loss within the defined retention period; and
4. Defence is to retain event logs for a minimum of 7 years in accordance with the National Archives of Australia's (NAA) Administrative Functions Disposal Authority.

Escalation Thresholds

5. The Information Technology Security Advisor (ITSA) has set the following general threshold for risks managed against this *Defence Security Principles Framework (DSPF) Enterprise-wide Control* and the related *DSPF Principle and Expected Outcome*.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems Log Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 28
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 28.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. <u>Australian Government Information Security Manual (ISM)</u> <u>Legislation:</u> <u>Archives Act 1983</u>
Read in conjunction with	N/A
See also DSPF Principle(s)	Information Systems (Logical) Security ICT Certification and Accreditation Information Systems Security Incident Management Security Incidents and Investigations
Implementation Notes, Resources and Tools	<u>Australian Government information security management guidelines – Australian Government security classification system</u> – provides guidance to assist agencies to identify the value of information and, in turn, apply a suitable protective marking <u>Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material</u> – provides guidance on procedures for applying protective markings and information handling procedures <u>Australian Government Information Security Manual</u> – sets out the standard governing the security of Australian Government ICT Systems

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Log Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The ITSA has set the following general threshold for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor. Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point.
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

Event Logging Strategy

3. Event logging strategies allow Defence to increase security posture by ensuring the accountability of all user actions and minimising the likelihood of undetected malicious behaviour. Audits of event logs will help detect, attribute and respond to any violations of information security policy, including cyber security incidents, breaches and intrusions.
4. The CISO is responsible for developing an event logging strategy covering:
 - a. logging facilities, including availability requirements and the reliable delivery of event logs to logging facilities;
 - b. the list of events associated with a system or software component to be logged; and
 - c. event log protection and retention requirements.
5. A system's Accreditation Authority should be consulted in the development of an event logging strategy.

Events to be Logged

6. All systems that handle Official Information, accept network connections, or make access control (authentication and authorisation) decisions should record and retain audit-logging information including:
 - a. all privileged operations;
 - b. successful and failed elevations of privileges;
 - c. security related system alerts and failures;
 - d. user and group additions, deletions and modification to permissions;
 - e. unauthorised access attempts to critical systems and files; and
 - f. events for any system that requires authentication:
 - (1) logons;
 - (2) failed logon attempts; and
 - (3) logoffs.
7. Examples of additional events that can be logged can be found within the Event Logging and Auditing section of the [ISM](#) as well as from your Accreditation Authority's Information Technology Security Officer (ITSO).

8. For each event logged, Defence business applications, systems, and networks within the Defence Single Information Environment (SIE) must log the following event detail:

- a. date and time of the event;
- b. relevant users or process;
- c. event description;
- d. success or failure of the event;
- e. event source e.g. application name; and
- f. ICT equipment location/identification.

Formatting, Storage and Documentation

Formatting

9. System owners **must** consult with their appropriate Accreditation Authority's ITSOs prior to developing their localised event logging strategy and mechanisms. This consultation should occur as early as possible in the system development lifecycle.

10. Logging is to be configured in a manner to ensure that process failures are raised as incidents with the appropriate Service Desk.

11. Systems should support the formatting and storage of event logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

- a. operating system event logs collected by a centralised log management system;
- b. logs in a well-documented format sent via https post, syslog, syslog-ng, or syslog-reliable network protocols to a centralised log management system;
- c. logs stored in a database that itself generates audit logs in compliance with the requirements of this document; and
- d. other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, Stroom Event Logging Schema and IDMEF.

Storage

12. Event logs must be stored independently of the system being monitored.

13. System owners that are responsible for systems that provide secure centralised logging facilities to other systems, should document availability and reliability specifications.
14. Defence personnel must ensure that all audit logging systems within the SIE use a centralised accurate time source to ensure time is consistent across the SIE.
15. Defence business applications, systems, and networks within the SIE **must** have a secure centralised logging facility that can be used to correlate and protect event logs from multiple sources. This includes:
 - a. the establishment or identification of a secure centralised logging facility;
 - b. that systems are configured to save event logs to a secure centralised logging facility as soon as possible after each event occurs;
 - c. the establishment or connection to an accurate time source, and use it consistently across systems to assist with the correlation of events;
 - d. that existing event logging facilities must be used where possible to correlate and protect events such as those logged or recorded by the Security Information and Event Management (SIEM) solution; and
 - e. that System Owners should consult with their Accreditation Authority's Information Technology Security Officers (ITSOs) to determine the appropriate centralised logging facility to use.

Documentation

16. All event logs must be documented to adequately describe the activity that the event is recording. The documentation must extend to the definition of individual fields and the meaning of their possible values.
17. Log files should be backed up daily unless otherwise stipulated in accreditation documentation.
18. Event logs should be retained for the life of the system, in accordance with the [Archives Act \(Cth\) 1983](#). An archiving system is to be implemented to ensure that log files are archived on a regular basis, in a manner that maintains their integrity and held for the period specified for that system.
19. Activity logs must be protected against disclosure, modification, fabrication and destruction and preserved in accordance with the [Archives Act 1983](#).
20. Users that are the subject of log entries **must** not be able to delete, destroy or modify logs.
21. Any legitimate activity that affects the integrity or availability of logs must be formally requested through the ITSA to CISO and if approved documented accordingly.

22. Any unauthorised modification or destruction of system log files is a security incident and must be reported in accordance with:

- a. DSPF Principle 19 – *Information Systems (Logical) Security*;
- b. DSPF Principle 24 – *ICT Security Incident Management*; and
- c. DSPF Principle 77 – *Security Incidents and Investigations*.

23. Log files containing sensitive system information or personal data are to be accessible only by those with a legitimate need to know and their contents are not to be disclosed without approval of the Information Technology Security Manager (ITSM) within, or delegated by, the appropriate Accreditation Authority.

Auditing

24. The appropriate ITSM within, or delegated by, the appropriate Accreditation Authority, is to conduct event log auditing as part of security operations and compliance to ensure potential violations are quickly identified and addressed.

25. Privileged users are responsible for supporting their appropriate ITSM within, or delegated by, the appropriate Accreditation Authority and System owners for assisting Defence in conducting Audit reviews, analysis and reporting of Audit events.

26. Privileged users must report all Audit processing failures to the their commander and/or manager and, if the failure is expected to last greater than 48 hours, their appropriate ITSM within, or delegated by, the appropriate Accreditation Authority.

Exclusions

27. With respect to Event log retention, Defence business applications, systems, and networks within the SIE should retain domain name service (DNS) and proxy logs for at least 18 months.

Roles and Responsibilities

Chief Information Security Officer (CISO)

28. With regards to Information systems log management, the CISO is responsible for:

- a. developing system event log strategies for Defence,
- b. consulting with the Accreditation Authority in the development of system event Log strategies, and
- c. approving requests that will affect the integrity or availability of system logs that are not aligned with Defence event log strategies.

Information Technology Security Advisor (ITSA)

29. With regards to Information systems log management, the ITSA is responsible for advising and supporting the CISO on the development and implementation of system event log strategies for Defence.

Information Technology Security Manager (ITSM)

30. With regards to Information systems log management, the ITSM is responsible for:

- a. ensuring all activity monitoring and system audit logs are periodically monitored for activity including but not limited to:
 - (1) unauthorised access, modification, and/or removal of log data; and
 - (2) unauthorised and/or inappropriate use of ICT resources within the SIE; and
- b. approving release of sensitive system log information to third parties.

Information Technology Security Officers (ITSOs)

31. With regards to information systems log management, ITSOs are responsible for providing system owners with security advice on log management within the SIE and reporting any reported ICT systems non-compliance against this policy.

Accreditation Authority

32. With regards to information systems log management, the Accreditation Authority is responsible for advising CISO on security related requirements in relation to the development of system event log strategies for Defence.

System Owners

33. With regards to information systems log management, system owners are responsible for ensuring that new applications, systems and network devices within the SIE are designed and implemented in accordance with the requirements of this policy.

Privileged Users

34. With regards to information systems log management, privileged users are responsible for ensuring that no ICT system log specified in this policy is deleted from any ICT system without prior approval from Defence ITSA or their delegate. This includes but is not limited to:

- a. deleting system logs to free up storage space within retention periods;

- b. configuring systems to overwrite retainable log data that will be lost inside retention periods; and
- c. reporting to their commander and/or manager about Defence ICT resources that don't comply with this policy.

Key Definitions

35. An **audit or event log** should provide a quantifiable record of a person's, or non-person entity's (NPE), interaction with a system, whether the interaction is successful or not, or if the access is inferred (i.e. searching). It must record the time, system details including which system component is generating the event, locations (logical and physical), the entities involved, the type and method of access and identify the information accessed or searched for. Event logs may be directly related to the access of a systems' primary information, or indirectly, by effecting change in a supporting or control enforcing component (e.g. adding a user into an access group in an Active Directory, enabling extended network access via a firewall change).

36. **Auditing.** The analysis of logged events in order to identify or investigate anomalies.

37. **Logging.** The collection of information about systems events.

38. A **system**, for the purposes of event logging, is an ICT based capability where entities can affect the Confidentiality, Integrity or Availability (CIA) of information or process under management. A system typically comprises a core set of applications that provides a means for users to effect the system's information or processes. These applications are either bespoke or locally integrated 'off-the-shelf' software. The applications themselves run on an infrastructure 'stack' to support requirements such as data stores (e.g. RDBMS), operating environment (e.g. operating system) or control enforcing infrastructure such as Identity and Access Management (IdAM), firewalls and network management. It is noted that IdAM, firewalls and network management capability may be provided as an external service. A system will have well-defined management and security boundaries that identify how information can be effected and how information transits those boundaries, inbound or outbound.

39. **System Log.** A file that contains events that are captured by the operating system components. These events are often predetermined by the operating system itself. System log files may contain information about device changes, device drivers, system changes, events, operations and more.

40. **System Data.** Comprises the primary information under management as well as IdAM information (such as users, groups, roles and access attributes), configuration management information to support the applications and infrastructure management information for any system specific infrastructure.

Further Definitions

41. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Log Management
Control Owner	ITSA
DSPF Number	Control 28.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Log Management
Related DSPF Control(s)	Information Systems (Logical) Security ICT Certification and Accreditation Information Systems Security Incident Management Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Vulnerability and Patch Management

General Principle

1. Defence will monitor newly identified Information and Communications Technology (ICT) vulnerabilities, prioritise patch deployment activities and develop appropriate risk mitigation strategies for Defence information systems that are unable to be patched within the specified timeframes.

Rationale

2. Security Patch Management is a critical aspect of maintaining the integrity of information systems. Security updates, or patches, are published by vendors to remediate identified vulnerabilities in operating systems, applications, firmware, and device drivers. Timely application of security updates is important and effective processes to protect Defence ICT systems from known vulnerabilities.

Expected Outcomes

3. Defence assets are monitored for vulnerabilities, and likelihood of threats and impact which are documented and used to determine risks.
4. Processes are established to receive, analyse and respond to vulnerabilities disclosed to Defence from internal and external sources (e.g. internal testing, security bulletins, security researchers).
5. Management plans are developed and implemented, and scans are performed in order to detect vulnerabilities.
6. Newly identified vulnerabilities are mitigated within the stated timeframes of the ISM, unless granted a deferral for non-compliance.
7. Defence develops remediation strategies for unpatched system vulnerabilities.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Adviser. NB: In the event that an appointment of a Group or Service Cyber Security Adviser has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive NB: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Information Systems Vulnerability and Patch Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 29
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 29.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Security for Capability Planning Defence Industry Security Program Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Security Incident Management Security Incidents and Investigations
Implementation Notes, Resources and Tools	• Australian Government Information security management guidelines – Australian Government security classification system – provides guidance to assist agencies to identify the value of information and, in turn, apply a suitable protective marking • Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material – provides guidance on procedures for applying protective markings and information handling procedures • The Australian Government Information Security Manual (ISM) assists in the protection of information that is processed, stored or communicated by Defences' systems • The Strategies to Mitigate Cyber Security Incidents complements the advice in the ISM • The Essential Eight Maturity Model complements the advice in the Strategies to Mitigate Cyber Security Incidents

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Vulnerability and Patch Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The ITSA has set the following general threshold for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	ITSA	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Controls

Vulnerability Management

3. Defence will develop and implement strategies to mitigate Cyber Security Incidents within the Defence Single Information Environment (SIE) by implementing risk mitigation strategies, as a minimum security baseline, in accordance with the [Australian Signals Directorate \(ASD\)'s Essential Eight Strategies to Mitigate Cyber Security Incidents](#).
4. Prior to the implementation of [ASD's Essential Eight Strategies to Mitigate Cyber Security Incidents](#), System Owners should identify the following:
 - a. which systems require protection (i.e. which systems store, process or communicate Official Information or other information with a high availability requirement);
 - b. which adversaries are most likely to target their systems (e.g. cyber criminals, nation-states or malicious insiders); and
 - c. what level of protection is required (i.e. selecting mitigation strategies to implement based on the risks to business activities from specific cyber threats.)
5. Any risk mitigation activities shall be implemented in priority of:
 - a. preventing Malware Delivery & Execution:
 - (1) application whitelisting;
 - (2) patch Applications; and
 - (3) configure Microsoft Office Macro settings.
 - b. limiting the extent of Cyber Security Incidents:
 - (1) restrict administrator privileges;
 - (2) patch operating systems; and
 - (3) implement multi-factor authentication mechanisms.
 - c. recovering Data and System Availability:
 - (1) ensure daily backups are performed.
6. Once the initial security baseline is established, System Owners should continue to develop and implement the [ASD's Essential Eight Strategies to Mitigate Cyber Security Incidents](#) throughout the systems lifecycle as new vulnerabilities are identified.

7. All vulnerabilities identified in operating systems, applications, drivers and hardware devices will be patched within the stated timeframes of the [Information Security Manual \(ISM\)](#), unless granted a deferral for non-compliance from the ITSA through Information Technology Security Manager (ITSM). All efforts to remediate non-compliance are to be taken to ensure no unacceptable risks are introduced into the Single Information Environment (SIE) through lack of effective Vulnerability management.

8. System Owners shall monitor the systems under their control for newly identified vulnerabilities and ensure they are patched within the specified timeframes stated in the ISM. If a system cannot be patched within the specified timeframes, then a Deferral must be requested. All risks associated with unpatched systems (excluding approved Deferrals granted from the ITSA through ITSM) shall be escalated in accordance with the escalation thresholds in this policy.

Note: The Deferral process is only to be granted for exceptional circumstances where patching a system may cause severe technical issues or could introduce greater risks to the system than the risk being mitigated. Deferrals are only to be granted for a limited amount of time to allow System Owners time to resolve any underlying technical issues and are not intended to remain in force throughout the system lifecycle.

9. The Information Technology Security Officer (ITSO) shall conduct periodic Vulnerability assessments, in consultation with the ITSM and System Owners, to assist with identifying new vulnerabilities and mitigate them within the stated timeframes of the [Information Security Manual \(ISM\)](#) unless granted a Deferral from the ITSA through ITSM.

10. The ITSO, as directed by the Defence ITSM shall further investigate any reported security vulnerabilities to systems and conduct a risk assessment to determine the associated risks, and countermeasures that should be employed to mitigate those risks to a manageable level.

11. The ITSO shall forward a final report to the System Owner, ITSM and the accrediting authority for consideration and guidance regarding system vulnerabilities that are not able to be adequately addressed.

12. Defence ITSM shall conduct periodic audits of the SIE to ensure system patches have been deployed in a timeframe which is commensurate with the risk posed to information or systems. Defence ITSM is to ensure Vulnerability audits include:

- a. Vulnerability scans;
- b. the assessment of threats, vulnerabilities, likelihood, and impacts to determine risk;
- c. the development of Vulnerability management plans to mitigate system vulnerabilities;

- d. the development of security patches within the stated timeframes of the ISM; and
- e. the development risk mitigation strategies in accordance with the [ASDs Essential Eight Strategies to Mitigate Cyber Security Incidents](#).

Application Whitelisting

13. System Owners shall implement application whitelisting on all known Defence systems to prevent non-approved software applications (including malicious code) from being executed.

Patch Management

Patching and Updating

14. In accordance with the [ASD's Essential Eight Strategies to Mitigate Cyber Security Incidents](#) patch management of applications and operating systems is an essential part of Vulnerability management and fundamental to the security of any Information and Communications Technology (ICT) system. However, an untested patch could potentially impact the normal operation of a system.

15. The balance of timeliness versus thorough testing is to be planned, documented and considered as part of the certification and accreditation process arising from the absence of application and operating system security patches within the Defence SIE.

Monitoring Patch Availability

16. The Defence ITSM is to ensure that processes are established to monitor vendor sites and other relevant sources to identify new patches as soon as they become available so that they can be assessed.

Exposure Assessment

17. When new patches become available to fix security vulnerabilities, an assessment is to be performed by the System owner to determine if the patch poses an extreme, high, moderate or low.

18. If the results of the assessment indicate moderate or high risk of exploitation, a high priority is to be given to the testing and deployment of the patch; or

19. If the results of the assessment indicate a low risk of exploitation, a low priority is to be given to the testing and deployment of the patch.

20. A risk assessment, based on threats, vulnerabilities, likelihood, and impacts to determine risk is to be determined and mitigated against patching timeframes. If the Vulnerability cannot be patched within the specified timeframes then the System Owner will escalate the issue in accordance with the risk tolerance threshold table.

Patch Testing

21. Prior to the deployment of any patch into the SIE production environment, the patch is to be tested in a non-production environment (e.g. Development or Test environment) to identify any potential risks.
22. If a non-production environment is not available, then testing is to be performed on a small pilot group of non-critical systems instead.
23. If patch testing adversely impacts the affected product, then the patch is not to be considered for deployment.

Scheduling of Patch Deployments

24. To achieve a balance between ensuring minimal business disruption is caused by the deployment of patches to production systems, and the need to quickly address security vulnerabilities identified in accordance with the ISM, patches identified by the Exposure Assessment as being:
 - a. Extreme Risk must be patched or mitigated within 48 hours (ISM Control: 1144; Revision: 8; Updated: Sep-17);
 - b. High priority must be patched or mitigated within two weeks (ISM Control: 0940; Revision: 7; Updated: Sep-17); or
 - c. Moderate or Low priority must be patched or mitigated within one month (ISM Control: 1472; Revision: 0; Updated: Sep-17).

Note: Microsoft regular updates are conducted on a monthly basis as part of the Defence patching cycle unless the vendor advises an 'extreme risk' level associated with the newly identified Vulnerability – in which case it must be patched within 48 hours in accordance with emergency patch processes.

Approval for Deployment

25. Prior to patches being deployed to the SIE production environment, approval is to be sought via the Defence Change and Release Management Processes.

Deployment of Patches

26. Patches are to be implemented during the change windows approved in the Change Request.

Post Implementation Validation Testing

27. Once the patch has been deployed, sufficient testing is to be performed of the affected product to validate that no adverse impacts have been caused to the normal functions provided by the affected product.

Defence Security Patch Management Process

28. The following links provide process workflows and compliance assessment criteria:

- a. Patch Management Plan;
- b. Patch Management System Lifecycle;
- c. Patch Management Process;
- d. Patch Management Compliance Assessment; and
- e. Patch Management Compliance Assessment Checklist.

Disable Untrusted Microsoft Office Macros

29. System owners shall disable untrusted Microsoft Office macros on Defence systems to prevent adversaries from using untrusted macros to download malware in order to access sensitive information.

Restrict Administrative Privileged

30. Privileged access to Defence operating systems and applications shall be restricted based on user duties and limited to System Administrator only tasks.

Example: Using a Privileged account for reading emails and web browsing the internet.

31. Regular revalidation for the need for privileges shall be conducted to ensure users access privileges remain aligned with the 'Need to Know' and 'Least Privileges' security principles.

User Application Hardening

32. System Owners shall block web browser access to Adobe Flash Player (uninstall if possible) to prevent users from executing untrusted Flash, Java, and web ads on defence systems.

Daily Backup of Important Data

33. To ensure information can be accessed again following a cyber security incident or technical failure (e.g. after a successful ransomware incident) System Owners must perform daily backups of important new/changed data, software and configuration settings, stored disconnected, and retained for at least three months. System Owners shall also perform backup restoration tests initially, annually, and when IT infrastructure changes.

Multi-Factor Authentication

34. To make it harder for adversaries to gain access to sensitive information, System Owners should implement Multi Factor Authentication (MFA), including remote access, for all users when they perform a privileged action within the Defence SIE.

Roles and Responsibilities

Chief Information Security Officer (CISO)

35. With regard to information system Vulnerability and patch management, the CISO is responsible for developing Defence-wide Vulnerability assessment and system monitoring strategies and capabilities.

Information Technology Security Advisor

36. With regard to information system Vulnerability and security patch management, the ITSA is responsible for approving non-compliance deferral requests from System Owners.

Information Technology Security Manager (ITSM)

37. With regard to information system Vulnerability and security patch management, the ITSM is responsible for:

- a. coordinating or conducting periodic ICT security Vulnerability and risk assessments of ICT environments;
- b. ensuring that vendor sites are monitored to identify new patches that have been released for products used within the SIE;
- c. an assessment is performed to identify if the Vulnerability it fixes poses a high, moderate or low risk of being exploited if not patched;
- d. supporting ITSA and System owner in reviewing system non-compliance deferral requests before being submitted to ITSA for approval; and
- e. maintain and regularly examine the Patch Exemption Register to ensure patch exemptions are still applicable and patch management is being undertaken efficiently.

Information Technology Security Officer (ITSO)

38. With regard to information system Vulnerability and security patch management, the ITSO is responsible for:

- a. conducting Vulnerability assessments and taking actions to mitigate threats and remediate vulnerabilities; and

- b. notifying the System Manager and ITSA of any identified Vulnerability that may prejudice the security of the system.

Compliance Manager

39. With regard to information system Vulnerability and security patch management, Compliance manager is responsible for providing ICT security advice, assistance and mitigation guidance to System Owners and broader Defence community including Computer Incident Response Team capabilities, ICT system certification and Vulnerability assessment for Defence SECRET and below systems.

System Owner

40. With regard to information system Vulnerability and security patch management, the System Owner is responsible for:

- a. ensuring that the appropriate ICT security mitigations are designed and integrated into the system based on [ASD's Essential Eight Strategies to Mitigate Cyber Security Incidents](#) and system's requirements; and
- b. monitoring and maintaining the security configuration of the system ensuring that patches are tested and applied in a timely manner to maintain the standard of the system security.

System Managers

41. With regard to information system Vulnerability and security patch management, the System Manager is responsible for advising the System Owner of any known vulnerabilities, non-compliances, unmanaged risks or other issues affecting the security of the system.

Equipment Manager

42. With regard to information system Vulnerability and security patch management, the Equipment Manager is responsible for developing a through-life support plan covering Vulnerability and patch management.

System Manager and Technical Support Staff

43. With regard to information system Vulnerability and security patch management, the System Manager and technical support staff are responsible for:

- a. ensuring the patch is tested to determine if its installation may have any adverse impacts on the operation of their business application and/or SIE infrastructure;
- b. ensuring a Patch Exemption request is raised for all Patches that would cause operational impact to their business application; and

- c. ensuring Patch remediation activities are undertaken to ensure patches that have an approved exemption are deployed within reasonable timeframes.

Key Definitions

44. **Application Whitelisting.** A whitelist only allows selected software applications to run on computers. All other software applications are stopped, including malware.
45. **Patch.** A patch fixes security vulnerabilities in software applications. Adversaries will use known security vulnerabilities to target computers.
46. **Multi-Factor Authentication (MFA).** Is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically: Something you know, like a passphrase. Something you have, like a physical token. And/or something you are, like biometric data. Having multiple levels of authentication makes it a lot harder for adversaries to access your information.
47. **Single Information Environment (SIE).** Encompasses the information and communications technology infrastructure of Defence along with the people and management systems that deliver that infrastructure and its related services. It is a capability that consists of the data/information used by Defence for business and military operations and the means by which it is created, managed, manipulated, stored and disseminated in and across all Defence security domains. The scope includes all Defence assets, personnel and capabilities involved in the exchange of data such as fixed, mobile, standalone and deployable networks, user devices and their support services, including Defence services hosted on external servers.
48. **Untrusted Microsoft Office Macros.** Microsoft Office applications can use software known as “macros” to automate routine tasks. Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled.
49. **Vulnerability.** In the context of information security, Vulnerability is a weakness in system security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system’s security policy.
50. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Vulnerability and Patch Management
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 29.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Vulnerability and Patch Management
Related DSPF Control(s)	Security for Capability Planning Defence Industry Security Program Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Security Incident Management Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	ITSA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Remote Access to Defence Systems

General principle

1. Defence will ensure there are appropriate security controls on the use of remote access to prevent unauthorised access to Defence information.

Rationale

2. Defence personnel and persons engaged under contract may be required to work offsite. While remote access capabilities give users the flexibility to perform their duties away from the office (refer to DSPF Principle 70 – *Working Offsite*), appropriate controls need to be in place to prevent the technical compromise of Official Information.

Expected outcomes

3. The provision of remote access services is limited to authorised Defence personnel and persons engaged under contract, with authorisation from the relevant authority to do so.
4. Remote access users are made aware of their responsibilities to protect Official Information when conducting Defence work offsite.
5. Users requiring remote access are provided this through approved systems.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor. Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point.
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	Chief Information Officer (CIO)(responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Remote Access to Defence Systems
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 30
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 30.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	PSPF Core Requirements: Safeguarding information from cyber threats; assessing and protecting Information; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Security for Projects Information Systems (Physical) Security Information Systems (Personnel) Security Offshore and Cloud Based Computing Overseas Travel Working Offsite
Implementation Notes, Resources and Tools	Australian Government Information Security Manual – sets out the standard governing the security of Australian Government ICT systems - Defence Remote Electronic Access & Mobility Service (DREAMS)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CISO	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Remote Access to Defence Systems

Control Owner

1. The Defence Information Technology Security Advisor (ITSA) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The Defence ITSA has set the following general threshold for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	Group/Service managed systems
Low	CIOG Information and Communication Technology (ICT) Security Branch EL1	EL1/O-5 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Defence Information Technology Security Advisor (ITSA)	EL2/O-6 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Advisor.
High	Head of Information Communications and Technology Operations (HICTO)	Appointed Group or Service Cyber Security Executive.
Extreme	Chief Information Officer (CIO)	Group Head or Service Chief

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

3. Defence permits remote access to some of its Defence ICT systems, networks, infrastructure and applications via accredited remote access solutions. In some circumstances it may also supply users with a standalone device such as a laptop to conduct off-site work. Remote access permits authorised users to conduct off-site work on a variety of devices. Approvals for remote access are conducted when the account/device is requested and remain in effect until the account/device is surrendered or the user changes positions.

Note: The granting of remote access approval to Defence networks does not extend to permitting the removal of hardcopy information PROTECTED or above. Whenever information with a 'handle-as' classification of PROTECTED or above needs to be stored at home, a home-based work agreement is required.

Remote access approvals

4. Before granted remote access to a user, the area provisioning the capability **must** gain the approval of an appropriate delegate in accordance with the roles and responsibilities section of this DSPF policy.

5. Users **must** only use Defence secure gateways to remotely access Defence networks. Refer to the Australian Government Information Security Manual (ISM) – *Guidelines for Gateways (Gateway architecture and configuration)*.

6. Users **must** only use their own Defence Standard User account to access the Defence Protected Network (DPN) via Defence approved remote access solutions (eg Defence Remote Electronic Access and Mobility Services (DREAMS) or the Defence Protected Laptop (DPL)).

7. When accessing Defence networks through remote access solutions, users should ensure that Defence official information is protected in accordance with:

- a. DSPF Principle 70 – *Working Offsite*;
- b. DSPF Principle 44 – *Overseas Travel*.

8. Defence issued remote access devices/tokens **must not** be used for any other purpose other than what the Defence remote access device was issued for. If a Defence issued remote access device/token is lost, stolen, or suspected to have been compromised a security incident is to be reported as soon as possible. Refer to DSPF Principle 77 – *Security Incidents and Investigations*.

9. Foreign nationals **must not** be granted remote access to Defence networks that process, store or communicate nationally sensitive or classified information.
- a. Consideration will be given to FVEY (Five Eyes) Foreign nationals who are embedded or on exchange posting with the Australian Defence Force (ADF). DSPF Control 40.1 – *Personnel Security Clearance* provides detail regarding foreign nationals.
 - b. A dispensation from this control for non-FVEY Foreign nationals will be considered, by the Defence ITSA, on a risk basis when supported by a Group Head or Service Chief endorsed risk assessment and business case.

Remote access processing restrictions applicable to systems administrators

10. Users **must not** be permitted under any circumstances to perform system administration via any remote access solution (including DREAMS), unless the system has been capability accredited to do so. This includes use of/entering privileged access credentials for directory services (e.g. Active Directory) and/or Application privileged credentials.

Restrictions on ICT equipment used for off-Site work and remote access

11. Public computing devices (untrusted public connections) are extremely vulnerable to exploitation. They are assumed to be compromised and actively collecting information by hardware and software techniques such as keyboard logging, screen scraping or remnant data access from memory. These techniques are widespread and are often used to collect valuable commercial information from public computers. These techniques are used to capture encrypted information when it is displayed or entered in unencrypted form.

12. As a result of the risk of using public devices the Protective Security Policy Framework (PSPF) provides direction prohibiting the use of such devices. Therefore, users **must not** use public devices to:

- a. Process, store or communicate any Defence official information which has not already been authorised for public release;
- b. perform remote access to Defence systems.

Note: Note: This restriction includes all forms of access using public computers, including using remote access systems, or reading material on a DVD, encrypted thumb drive or other removable media.

13. Users **must not** process, store or communicate Official Information on privately-owned devices or upon web based email or storage capabilities, for example Hotmail, Gmail, Dropbox, or Google Drive. The use of privately-owned devices to access DREAMS or VERA has been approved by Defence and are permitted as these capabilities are configured to ensure strong virtual separation of the session from the physical host to prevent data loss.
14. Defence members are permitted to store or process Official Information on personal devices where this pertains to records that contain their Personally Identifiable Information and relate to their employment with Defence such as Job Offers, Salary Nominations, Payslips, eVetting Packs.
15. In accordance with the ISM – *Guidelines for Enterprise Mobility (Privately-owned mobile devices)*, privately-owned devices **must not** be used for remote access to information and systems classified SECRET and above. Also refer to DSPF Principle 70 – *Working Offsite*.
16. Users with a requirement for SECRET and above, remote access **must** use an accredited Defence controlled remote access device and receive approval by an appropriate delegate in accordance with DSPF Principle 70 – *Working Offsite* and the *Roles and Responsibilities* section below.
17. Remote access devices used to process information SECRET or above **must** use:
- a. ASD-approved encryption to reduce the 'handle-as' classification to OFFICIAL;
 - b. handle and store the device in accordance with its actual classification.

Work-from-home

18. Users may take home hardcopy OFFICIAL Information Management Markers (IMM) marked information, such as an OFFICIAL: Sensitive document, provided that it is stored from casual unauthorised access whilst at home using a locked commercial filing cabinet or locked secure briefcase, over which the employee maintains positive control.
19. There are no circumstances where an employee can 'informally' remove PROTECTED and above hardcopy material in order to take it home. Whenever information with a 'handle-as' classification of PROTECTED or above needs to be stored at home, a home-based work agreement is required.
20. Users working offsite, and performing official duties (ie: Defence members posted to overseas locations), are permitted to do so providing the requirements for working offsite have been met. Refer to DSPF Principle 70 – *Working Offsite* for additional requirements.

Example: Even where an employee has a DREAMS account and can use this to work from home on up to PROTECTED softcopy material the employee cannot take a hardcopy of PROTECTED or above documents home, even if it is only overnight.

Remote access to Defence systems from outside Australia

21. There is an increased risk when accessing Defence networks remotely from locations outside Australia. Use of remote access solutions, (by authorised Australian national Defence personnel), from within the borders of a Five Eyes partner nation, will generally be considered acceptable as long as users observe the travel security principles outlined in DSPF Control 22.1.

22. When travelling overseas on official travel and prior to approving remote access from locations other than Australia, consideration **must be** given to the contemporary threat (travel advice). DSPF Control 44.1 – Annex A to Overseas Travel – *Overseas Travel Briefing and Debriefing Guides (Stage 3)* requires personnel to obtain travel advice for the location(s) being visited or transited. User's travelling to a Non-FVEY country are only permitted to use remote access within an Australian government controlled environment. This may include an Australian Embassy/Consulate/High Commission and/or Defence establishment.

23. If returning from travelling overseas with mobile devices to high/extreme risk countries, personnel are to:

- a. reset user credentials used with devices, including those used for remote access to Defence systems;
- b. monitor accounts for any indicators of compromise, such as failed login attempts, and report any suspicious activity as a security incident.

24. Refer to DSPF Principle 70 – *Working Offsite* and DSPF Principle 22 – *Mobility Device Security* or additional requirements.

Roles and Responsibilities

Group Heads and Service Chiefs

25. Group Heads and Service Chiefs are responsible for approving off-site work that involves remote access for SECRET systems, as it relates to their responsibilities in accordance with DSPF Control 23.1 Annex A.

26. This responsibility may be delegated no lower than SES Band 1/O-7.

Defence Information Technology Security Advisor (ITSA)

27. ITSA is the Control Owner. In addition the ITSA is responsible for:

- a. coordinating the efforts of Systems Owners, System Managers and cyber security elements across Defence in order to ensure the strategic intent and direction of the Defence CISO is achieved;
 - b. liaising with peers in other agencies on technical security matters; and
 - c. management of cyber security advice, guidance and reporting on significant cyber security risks in Defence, including Defence's overall information security and cyber security posture.
28. Where policy does not exist the Defence ITSA will provide final determination on the matter.

Executive Security Advisers

29. Executive Security Advisers (ESAs) are responsible for assessing the security arrangements and managing the accreditation for home-based work arrangements for Defence personnel and external service providers employed in single-service units.

Commanders, Managers and Contract Managers

30. Commanders, managers, and contract managers are responsible for:
- a. approving remote access to systems up to PROTECTED; and
 - b. ensuring all requests for Privileged User Remote Access, have been assessed and authorised by the Risk Owner if and when required.

System Owners

31. System owners are responsible for ensuring Defence ICT systems, networks, infrastructure and applications incorporate security measures for audit trails and activity logging to ensure the accuracy and integrity of the data captured or held.

Defence Industry Managers

32. Defence industry managers are responsible for gaining the approval for offsite work for any affected staff from or through the relevant Defence Contract Manager before permitting offsite work to be conducted using Defence information.

System Users

33. System users **must** only use approved Defence remote access solutions to remote access Defence ICT systems, networks, infrastructure and applications.

Privileged User

34. Privileged users are responsible for the conduct of network administration functions and **must not** use remote access via Defence Remote Access solutions.

Key Definitions

35. **Australian Signals Directorate (ASD) approved encryption.** Any cryptographic functionality that is implemented for an ICT system, asset or device to reduce its handle-as classification is to be done in accordance with any product specific advice, all relevant requirements of the ISM, and any relevant Australian Communications- Electronic Security Instructions (ACSI) series publications.

36. **Defence Controlled Device.** A device is under Defence control if it is owned by Defence or is subject to any agreement that legally binds the owner of the device to comply with all DSPF and ISM security policies. Defence controlled devices include security classified assets owned by Defence Industry Security Program (DISP) members.

***Example:** A DISP member supplies their own computer to process SECRET information. DISP membership contractually obliges the company to comply with all Commonwealth policies and the DSPF therefore the device is under Defence control.*

37. **External Access.** Access to Defence resources, by a partner organisation using a logical private network.

38. **Foreign National.** A person who is not an Australian citizen.

39. **Foreign System.** A system that is not managed by, or on behalf of, the Australian Government.

40. **Gateway.** Gateways securely manage data flows between connected networks from different security domains.

41. **Offsite Work.** Work undertaken in any location that would not be recognised as a usual workplace or one where Defence would not normally conduct day-to-day official business. Examples of this type of work may include work undertaken at home, during official travel, in a hotel or conference centre, or by a Defence employee at a Defence contractor's premises. It does not include work conducted on operations and exercises (with the exception of approval processes for the conduct of classified work in accommodation areas such as barracks.) Refer to *DSPF Principle 70 – Working Offsite*.

42. **Privileged User.** A user who can alter or circumvent a system's security measures. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security measures. A Privileged User can have one or more of the following abilities or accesses:

- a. the ability change key system configuration settings;
- b. the ability to change or circumvent security controls;
- c. access to audit and security monitoring information;
- d. access to data, files and accounts used by other users, including backups and media;
- e. access to troubleshoot a system.

43. **Remote Access.** Access to a system that originates from outside a Defence network and enters the network through a gateway, including over the internet. Remote access is characterised by:

- a. the provision of an information and communications technology (ICT) device that implements Australian Signals Directorate (ASD)-approved encryption in order to permit offsite work on official information that is not for public release;
- b. accessing a system or desktop session of any classification from an external network via an accredited gateway.

44. **Security domain.** A system or collection of systems operating under a consistent security policy that defines the classification, releasability and special handling caveats for information processed within the domain.

45. **Privately Owned Device and Public Devices.** Home computers, portable ICT devices, laptops, phones and removable media or any other form of computing device that is owned by an individual or a company and is not subject to Defence control. This is also known as a trusted private connection.

46. **Public Site.** Any place where neither the employee nor Defence can exert physical control over the local environment. This is also known as an untrusted public connection. Example: Hotel conference rooms, public transport, internet cafes, airport lounges etc.

47. **Security risk.** Any event that could result in the compromise, loss of integrity or unavailability of information or resource, or deliberate harm to people measured in terms of its likelihood and consequences.

48. **System User.** A user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass security measures.

49. **System.** A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.

50. **System Administration.** System administration refers to the management of one or more hardware and software systems.

51. **System Owner.** The executive responsible for a system and is identified in the accreditation documentation.

52. **Elevated Privileges.** Elevated privileges is when a user is granted the ability to do more than a Standard User. A System User is someone that has “zero administrative” privileges in any capacity

Further definitions

53. Further definitions for common PSPF terms can be found in the Glossary.

54. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

55. Australian Government Information Security Manual- Supporting information- Glossary of cyber security terminology.

Annexes and attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Remote Access to Defence Systems
Control Owner	Defence Information Technology Security Advisor (ITSA)
DSPF Number	Control 30.1
Version	6
Publication date	07 March 2023
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Remote Access to Defence Systems
Related DSPF Control(s)	Classification and Protection of Official Information Security for Projects Information Systems (Physical) Security Information Systems (Personnel) Security Offshore and Cloud Based Computing

	Overseas Travel Working Offsite

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	Defence ITSA	Launch
2	9 April 2020	AS SPS	Inclusion of dispensation DEFGRAM 147/2020
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	03 August 2020	AS SPS	update of dispensation DEFGRAM 147/2020 to DEFGRAM 315/2020
5	30 October 2020	AS SPS	Removal of expired dispensation DEFGRAM 315/2020 (expired 30 October 2020)
6	07 March 2023	Defence ITSA	Inclusion of remote access from outside Australia and Foreign Nationals use of remote access.



Defence Security Principles Framework (DSPF)

Defence Research, Innovation & Collaboration Security

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Principle. To view the full Principle, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Document administration

Identification

DSPF Principle	Defence Research, Innovation & Collaboration Security
Principle Owner	First Assistant Secretary Defence Security (FAS DS)
Control Owner	Chief Defence Scientist
Version	1
Publication date	14 March 2023
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 31.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	06 January 2023	DSTG	Approved by FAS DS for release on 14 March 2023.



Defence Security Principles Framework (DSPF)

Defence Research, Innovation & Collaboration Security (DRICS)

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

Annex A – *DRICS Rationale and Context*

Annex B – *DRICS Guidance*

Annex B – Appendix 1 – *DRICS Process Workflow*

Document administration

Identification

DSPF Control	Defence Research, Innovation & Collaboration Security
Control Owner	Chief Defence Scientist
DSPF Number	Control 31.1
Version	2
Publication date	14 July 2023
Releasable to	Need-to-Know
General Principle and Expected Outcomes	Principle 31
Related DSPF Control(s)	Defence Industry Security Program Personnel Security Clearance Temporary Access to Classified Information and Assets Physical Security Physical Security Certification and Accreditation Security Incidents and Investigations Escorting Security Protected or Classified Assets
Implementation Notes, Resources and Tools	DRICS Supporting Documents and Templates http://drnet.defence.gov.au/DST/DRICS/Pages/DRICS.aspx

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	06 January 2023	DSTG	Approved by FAS DS for release on 14 March 2023.
2	14 July 2023	DSTG	Typographical, grammatical and font changes.



Defence Security Principles Framework (DSPF)

Annex A: DRICS Rationale and Context

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Annex A – DRICS Rationale and Context
Annex Version	1
Annex Publication date	14 March 2023
Releasable to	Need-to-Know
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Research, & Innovation Collaboration Security (DRICS)
DSPF Number	Control 31.1
Implementation Notes, Resources and Tools	DRICS Supporting Documents and Templates http://drnet.defence.gov.au/DST/DRICS/Pages/DRICS.aspx

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	06 January 2023	DSTG	Approved by FAS DS on 6 January 2023



Defence Security Principles Framework (DSPF)

Annex B: Guidance

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

Appendix 1 – DRICS Process Workflow

Document administration

Identification

DSPF Annex	Annex B – Guidance
Annex Version	1
Annex Publication date	14 March 2023
Releasable to	Need-to-Know
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Research, & Innovation Collaboration Security (DRICS)
DSPF Number	Control 31.1
Implementation Notes, Resources and Tools	DRICS Supporting Documents and Templates http://drnet.defence.gov.au/DST/DRICS/Pages/DRICS.aspx

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	06 January 2023	DSTG	Approved by FAS DS on 06 January 2023



Defence Security Principles Framework (DSPF)

Appendix 1 to Annex B: DRICS Process Workflow

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Document administration

Identification

DSPF Appendix	Appendix 1 to Annex B: DRICS Process Workflow
Appendix Version	1
DSPF Annex	Annex B: Guidance
Annex Publication date	14 March 2023
Releasable to	Need-to-Know
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Research, Innovation & Collaboration Security (DRICS)
DSPF Number	Control 31.1
Implementation Notes, Resources and Tools	DRICS Supporting Documents and Templates http://drnet.defence.gov.au/DST/DRICS/Pages/DRICS.aspx

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	06 Jan 2023	DSTG	Approved by FAS DS on 06 Jan 2023



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Personnel Security Clearance

General principle

1. Only those people recognised as eligible, suitable and trusted will obtain and retain access to Australian Government resources (people, information and assets).

Rationale

2. An assured and trusted workforce of security cleared personnel is a critical protective security control. It underpins the effectiveness of many other controls and efficient business practices.

Expected outcomes

3. The Australian Government Security Vetting Agency (AGSVA) will conduct personal security vetting for Defence personnel, Contractors, Consultants and Outsourced Service Providers.
4. In accordance with the Protective Security Policy Framework (PSPF), the personal security vetting process will be used to assess the eligibility and suitability of an applicant to hold and maintain a clearance.
5. Defence, Government, industry and foreign partners will confidently give access to classified information and assets to Defence personnel, Contractors, Consultants, and Outsourced Service Providers holding a security clearance.
6. Security clearance holders, managers and security officers will report: changes of circumstances; suspicious, ongoing, unusual or persistent contact; and any other significant incidents which may impact on the clearance holder's suitability to hold a clearance.

Escalation Thresholds

7. Departure from PSPF policy requirements.

Risk Rating	Responsibility
Low	Assistant Secretary Vetting (ASV) or authorised delegate
Moderate	ASV
Significant	Defence Security Committee (DSC) – through ASV
High	DSC – through ASV
Extreme	Will not be accepted. Must treat, including by avoiding the risk (i.e. ceasing the relevant activity)

8. Approval or changes to Eligibility Waivers.

Risk Rating	Responsibility
Low	Group Head/Service Chief or authorised delegate
Moderate	Group Head/Service Chief or authorised delegate
Significant	Group Head/Service Chief or authorised delegate
High	Secretary – through First Assistant Secretary Security and Vetting Service (FAS S&VS)
Extreme	Will not be accepted. Must treat, including by avoiding the risk (i.e. ceasing the relevant activity)

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Personnel Security Clearance
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 40
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 40.1
Control Owner	Assistant Secretary Vetting (ASV)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Eligibility and suitability of personnel; Ongoing suitability and management of personnel; and Separating personnel Legislation: <u>Privacy Act 1988 (Cth)</u> <u>Freedom of Information Act 1982 (Cth)</u> <u>Public Service Act 1999 (Cth)</u> <u>Australian Citizenship Act 2007 (Cth)</u>
Read in conjunction with	DSPF Governance and Executive Guidance DSPF Controls, Processes and Instructions PSPF Mandatory Requirements
See also DSPF Principle(s)	Assessing and Protecting Official Information Information Systems (Personnel) Security Contact Reporting Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	• <u>PSPF – Eligibility and suitability of personnel</u> • <u>PSPF – Ongoing assessment of personnel</u> • <u>PSPF – Separating personnel</u> • Military Personnel Policy Manual

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	20 June 2019	FAS S&VS	PSPF alignment update
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Personnel Security Clearance

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document administration

Identification

DSPF Control	Personnel Security Clearance
Control Owner	Assistant Secretary Vetting (ASV)
DSPF Number	Control 40.1
Version	4
Publication date	22 June 2023
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Personnel Security Clearance
Related DSPF Control(s)	Classification and Protection of Official Information Information Systems (Personnel) Security Contact Reporting Access Control Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	02 July 2018	ASV	Launch
2	20 June 2019	ASV	PSPF alignment update
3	31 July 2020	ASV	Inclusion of CDI as PV Sponsor; Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	22 June 2023	ASV	Addition of form number to paragraph 103(d) and removal of paragraph 104



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Temporary Access to Classified Information and Assets

General principle

1. For urgent operational or business needs, people without the necessary security clearance may be granted limited and controlled, temporary access to classified information and assets. The approval of such access does not constitute the granting of a security clearance.

Rationale

2. Access to classified information and assets requires individuals to have an appropriate clearance and need to-know.

3. If an individual requires access for legitimate reasons, that access may be granted on a temporary, limited and controlled basis.

Expected outcomes

4. Temporary access to classified resources is only approved for urgent operational or business reasons, not as a substitute for sound personnel security management or appropriate workforce planning.

5. Temporary access provisions are only used for situations that involve access to classified information or assets.

6. Defence does not provide temporary access to caveat, CODEWORD or compartmented information at any classification.

7. Temporary access is strictly supervised and confined to information or assets that are essential to the requirement for which the temporary access was approved.

8. Temporary access to ICT networks is not approved unless it can be strictly confined to information that is essential to operational or business needs.

9. Approval for access to ICT networks involving SIGNIFICANT and HIGH risks are to be implemented by Assistant Secretary ICT Security (ASICTS) in the Chief Information Officer Group as the Control Implementer.

10. Any misuse of temporary access provisions is reported as a security incident.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander, or Manager
Moderate	EL2/0-6 or equivalent in relevant Group/Service
Significant	AS SPS ASICTS for ICT systems access only
High	Defence Security Committee (DSC) – through AS SPS ASICTS for ICT systems access only
Extreme	DSC through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Temporary Access to Classified Information and Assets
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 41
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 41.1
Control Owner	Assistant Secretary Policy and Services (AS SPS)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security governance for contracted service providers; Security governance for international sharing; Classification of information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems; and Eligibility and suitability of personnel. Legislation: <u>Members of Parliament (Staff) Act 1984 (Cth)</u> <u>Privacy Act 1988 (Cth)</u> <u>Freedom of Information Act 1982 (Cth)</u>
Read in conjunction with	Australian Government Security Classification System (AGSCS)
See also DSPF Principle(s)	Assessing and Protecting Official Information Foreign Release of Official Information Defence Industry Security Program Personnel Security Clearance Identity Security. Physical Transfer of Information and Assets Physical Security Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	<u>Australian Government physical security management protocol</u> Australian Security Intelligence Organisation (ASIO), Security Equipment Guides (SEGs) are available to ASAs from the GovDex Protective Security Community Information Security Manual (ISM) Control 0441

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	12 August 2019	AS SPS	To reflect the appointment of ASICTS as Control Implementer for Significant and High risk ICT systems access.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Temporary Access to Classified Information and Assets

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner for this Enterprise-wide Control.

Control Implementer

2. AS SPS has formally designated Assistant Secretary ICT Security (ASICTS) in the Chief Information Officer Group (CIOG) as the Control Implementer for ICT systems access for SIGNIFICANT and HIGH risk. ASICTS will manage all approvals for temporary access to ICT systems in accordance with the Escalation Thresholds below.

Escalation Thresholds

3. The AS SPS has set the following general thresholds for risks managed against this DSPF Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS ASICTS for ICT systems access
High	Defence Security Committee (DSC) – through AS SPS ASICTS for ICT systems access
Extreme	DSC through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Controls

Temporary Access

4. Temporary access allows limited, supervised access to specific security classified information and assets to meet an operational or business need. Commanders and Managers are to supervise and monitor the classified information and assets accessed under these arrangements.
5. Temporary access is to be strictly confined to the specific classified information or assets required to meet the operational or business need. An inability to accurately identify and record the specific classified documents, files or assets that will be accessed not only limits the ability to conduct a risk assessment but suggests that unrestricted access is required and hence the use of Temporary access provisions is inappropriate. In these circumstances, a clearance should be sought for ongoing access.
6. Temporary access is not a security clearance and cannot be used in lieu of a security clearance to provide assurance for reasons other than access to specific classified assets (information or physical).

Note: 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. Defence policy requires that these positions are identified as Designated Security Assessment Positions (DSAP) and the occupant holds an appropriate Australian Government security clearance.

Note: Defence policy mandates that Defence personnel hold a minimum security clearance of Negative Vetting 1 (NV1) prior to having independent access to bulk weapons. Temporary access cannot be used to satisfy this requirement.

Note: A Defence employee requires an NV1 to be allowed unescorted access to a security zone within a building. Temporary access is not a security clearance and therefore cannot be used to allow access to the security zoned area.

Temporary Access, Caveats, DLM and Need-to-Know

7. Access to information requires that a person has a 'need-to-know' and the appropriate security clearance. Temporary access provisions only address security clearance requirements, they do not alter a person's need-to-know.

8. The approval of Temporary access cannot alter the effect of caveats. Approved Temporary access does not grant access that would otherwise be limited by caveats.

Note: The Australian Government Protective Security Policy Framework (PSPF) prohibits the use of Temporary access provisions to enable access to Caveat, CODEWORD and Compartmented information.

Example: An Australian Defence Force member has a current Negative Vetting 2 clearance and is in the process of upgrading to Positive Vetting (PV). Temporary access provisions cannot be used to grant this individual Temporary access to Caveated, CODEWORD, or Compartmented information.

Types of Temporary Access

9. There are two types of Temporary access 'Short Term' and 'Provisional' for managing limited access to classified information and resources. Each type of access encompasses specific limitations and prerequisites. See [Australian Government Personnel Security Protocol](#).

Requirements and Constraints on Temporary Access

10. Temporary access will only be approved when there is no other current clearance holder available that can carry out the duties required. If a current clearance holder is available but cannot carry out the duties, this will be documented in the risk assessment and be considered by the approving authority. See [Australian Government Personnel Security Protocol](#).
11. In addition to limitations applied within the [Australian Government Personnel Security Protocol](#), Temporary access:
- a. is not to be approved:
 - (1) to permit access to any material classified TS unless the person requiring the access holds an Australian Government Negative Vetting Level 1 clearance;
 - (2) retrospectively to avoid managing a security incident resulting from unauthorised or incidental access to classified material; or
 - (3) if the clearance holder has been subject to an adverse security clearance decision at the level of the requested Temporary access, or is currently under review for cause (e.g., clearance downgraded due to security concerns, or higher level clearance previously denied on security grounds.)

- b. Temporary access is only to be approved:
- (1) by Defence Personnel. Defence industry cannot approve Temporary access on behalf of the Australian Government; and
 - (2) if the scope of the approved information access can be defined and the ownership of the information is understood.

12. Temporary access is only available to persons who either currently hold, or are eligible to be considered for an Australian Government security clearance.

13. Temporary access is not available to foreign nationals who hold a foreign government security clearance that is recognised through a Security of Information Agreement/Arrangement (SIA).

Example: A foreign national has a recognised clearance that allows them to see *PROTECTED* material. As they have a recognised foreign clearance, they cannot be approved for Temporary access to *SECRET* material.

14. If a foreign national has been granted an Australian Government security clearance on the basis of successfully approved eligibility waivers, they may be considered for Temporary access if required (this does not include Temporary access to Top Secret (TS) information.)

ICT Systems Access

15. The approval of Temporary access does not permit unrestricted access to Defence ICT networks. If Temporary access is required to ICT resources, [Information Security Manual \(ISM\) control 0441](#) requires that the account holder's access is either restricted to only the information that is required for the specified duties, or is continually supervised by another appropriately cleared system user.

16. Normal user access on systems such as the Defence Restricted Network (DRN) and Defence Secret Network (DSN) grant access to very large volumes of information on web sites and shared drives, the risk of granting access to this material is accepted for those with a security clearance at the required level but is considered too great for those that have not completed the security clearance process.

17. ASICTS in CIOG is the Control Implementer for ICT systems access requests involving SIGNIFICANT and HIGH risk. Therefore, requests for access involving these risk thresholds can be made to for approval.

- a. CIOG mandates that if unrestricted ICT access is required, approval is to be processed as a minimum of SIGNIFICANT risk for the DRN and as a minimum of HIGH risk for the DSN, or similarly classified networks, before access is granted.

Members of Parliament (Staff) Act 1984 (MOPS Act) Staff

18. For information regarding the granting of Temporary access to MOPS Act staff, see Australian Government Personnel Security Protocol, '*Temporary Access for MOPS Act staff*'.

19. The following table identifies the approving authorities for Temporary access.

Table 1: Authority to Approve Temporary Access

Access To	Type of Temporary Access	
	Short Term	Provisional
Information requiring a PV as a prerequisite to access	Unavailable	Unavailable
Caveat / CODEWORD / Compartmented material of any classification	Unavailable	Unavailable
TOP SECRET excluding CODEWORD (refer Note 1)	Group Head, Service Chief or approved delegate in consultation with AGSVA	Minimum of SES Band 1/07 (or approved delegate) in consultation with AGSVA
SECRET and below excluding CODEWORD	Commander, Manager or Contract Manager in consultation with AGSVA Senior Australian Defence Force Officer (SADFO) (only for SAFEbase related emergencies)	SADFO (only for SAFEbase related emergencies)

Note 1:

TOP SECRET excluding Caveat, CODEWORD and Compartment -Note 1: Clearance subjects are to hold an Australian Government security clearance at minimum of Negative Vetting Level 1 for access to this level of material under Temporary access arrangements. (for MOPS Act staff, see [Australian Government Personnel Security Protocol](#) '*Temporary Access for MOPS Act staff*')

Note: Chief Joint Operations (CJOPS) discharges these responsibilities in respect of personnel on overseas operations.

Processing Temporary Access Requests

20. The area approving Temporary access will assess the risks associated with doing so, specify risk monitoring requirements and identify the responsible appointment. The assessment of risk is to be in accordance with PSPF [Personnel Security Guidelines – Agency personnel security responsibilities](#): Temporary access risk assessments.

21. The Commander or Manager (or their delegate) of the area seeking Temporary access for an employee are to:

- a. prior to processing a request for Temporary access, consult with AGSVA (and the Department of Finance in relation to MOPS Act staff) to determine if an applicant for Temporary access has any pre-existing clearance conditions or restrictions recorded on their Personnel Security File that would prevent Temporary access from being approved. This consultation should be initiated through the security officer of the requesting area;
- b. consult with other areas in Defence and/or other agencies if the Temporary access will result in access to their information;
- c. prepare and staff a business case requesting Temporary access from the appropriate authority (refer Table 1 – Authority to Approve Temporary Access);
- d. make the decision to deny or approve requests for Temporary access for e. which they are the nominated delegate;
- e. formalise the arrangement in writing with the applicant, including advising the applicant of the information that can be accessed under these arrangements and their responsibilities with regard to confidentiality and the protection of the information;
- f. record the details of access in the security register;
- g. ensure ongoing monitoring of approved Temporary access to ensure that it is strictly confined to the identified information and assets essential to the operational and business need for which the access was approved;
- h. report any inappropriate or unauthorised access as a security incident in accordance with DSPF Principle 77 – Security Incidents and Investigations; and
- i. review the duties and responsibilities of the position and if required:
 - (1) upgrade the position's security clearance requirement; and
 - (2) initiate a security clearance upgrade for the individual.

Note: Contract Managers discharge these responsibilities in respect of the persons engaged under a contract that they manage.

22. If the steps in the above paragraphs cannot be performed due to the urgent and immediate requirement to grant access in an emergency situation these steps are to be undertaken as soon as is practical following the granting of access.

Temporary Access Denied

23. Temporary access decisions are not final security clearance decisions as they are based on incomplete information that does not allow for a full assessment of the whole person. Therefore a decision not to grant, or to withdraw Temporary access, does not indicate that a person will necessarily be found unsuitable to hold a security clearance by the AGSVA, even if AGSVA has identified concerns during the application for Temporary access. Subsequent investigation by AGSVA during the full security clearance process may identify mitigating factors or reveal new information.

Key Definitions

24. **Australian Government Security Vetting Agency:** AGSVA is a branch of the Defence Security and Vetting Service (DS&VS) that provides independent security clearance vetting services and advice to non-exempt government agencies (including Defence).

25. **MOPS Act staff:** Staff employed by an Australian Government Minister under the Members of Parliament (Staff) Act 1984 (Cth).

26. **Ongoing access:** Access to classified information or assets for longer than three months, or regular access for shorter periods constitutes Ongoing access. This requires an individual to have the appropriate security clearance and need-to-know.

27. **Temporary access:** A temporary arrangement that in some circumstances provides limited access to security classified information to people who are yet to be issued with an appropriate security clearance. There are two types of Temporary access: Provisional access and Short Term access.

28. **Provisional access:** A form of Temporary access that can be approved after a person submits all information required for a security clearance, but before the clearance is finalised to allow that person to access security classified information on a limited basis only.

29. **Short Term access:** A form of Temporary access used where access to security classified information is required by a person who does not have the appropriate security clearance.

30. **Limited Higher Access (obsolete term):** This term refers to an older form of Temporary access and should no longer be used, except when referring to old arrangements.

31. **Emergency Access (obsolete term):** This term refers to an older form of Temporary access and should no longer be used, except when referring to old arrangements.

Further Definitions

32. Further definitions for common PSPF terms can be found in the [Glossary](#).
33. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Temporary Access to Classified Information and Assets
Control Owner	Assistant Secretary Security Policy and Services
Control Implementer	Assistant Secretary ICT Security
DSPF Number	Control 41.1
Version	31 July 2020
Publication date	X Month 20XX
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Temporary Access to Classified Information and Assets
Related DSPF Control(s)	Assessing and Protecting Official Information Foreign Release of Official Information Defence Industry Security Program Personnel Security Clearance Identity Security Physical Transfer of Information and Assets Physical Security Access Control Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	12 August 2019	AS SPS	To reflect the appointment of ASICTS as Control Implementer for Significant and High risk ICT systems access.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Identity Security

General principle

1. Individuals' identities will be verified and, where necessary, protected in relation to association with particular roles and capabilities.

Rationale

2. Proof of identity assists Defence to mitigate risks associated with unauthorised persons accessing Defence establishments or information and reduces the likelihood of fraud.
3. Defence protects the identities of personnel associated with sensitive capabilities to maintain operational security of that capability and the safety of the individual and their family.

Expected outcomes

4. Defence maintains proof of identity processes, requiring individual identities to be verified in accordance with Defence People Group's 'Identity Management Framework';
5. Information relating to Protected Identities is secured appropriately;
6. Defence personnel and persons engaged under a contract are made aware of their roles and responsibilities in relation to Protected Identities;
7. Individuals assigned Protected Identity status conduct themselves in a way that maintains their own personal protection; and
8. Defence personnel and persons engaged under a contract report all such unauthorised disclosures as a security incident.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary People Policy and Employment Conditions (AS PPEC)
High	Defence Security Committee (DSC) – through AS PPEC
Extreme	Defence Security Committee (DSC) – through AS PPEC

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Identity Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 42
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 42.1
Control Owner	AS PPEC

Related information

Government Compliance	PSPF Core Requirements: Entity physical resources; and Eligibility and suitability of personnel. Legislation: ASIO Act 1979, Part V section 92 Crimes Act 1914, Part IAC Assumed Identities Intelligence Services Act 2001, Part 6, section 41 Defence (Inquiry) Regulations 1985
Read in conjunction with	Verification of Identities will be addressed by Defence People Group's Identity Management Framework in 2018. Controls surrounding Protected Identities are addressed in DSPF Control 42.1 – <i>Protected Identities</i>
See also DSPF Principle(s)	Assessing and Protecting Official Information Information Systems (Personnel) Security ICT Certification and Accreditation Personnel Security Clearance Overseas Travel Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	Defence People Group's 'Identity Management Framework' Defence Form XP168 -Report of Security Contact Concern. Defence process for granting honours and awards (including the process for individuals with protected identities). Defence 06.1.4 The Administrative Inquiries Manual, Chapter 7: scoping and planning a Court of Inquiry. National Identity Security Strategy 2012. National Identity Proofing Guidelines 2014.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Protected Identities

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

Annex A – Process For Granting Honours and Awards

Document administration

Identification

DSPF Control	Protected Identities
Control Owner	AS PPEC
DSPF Number	Control 42.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Identity Security
Related DSPF Control(s)	Assessing and Protecting Official Information Information Systems (Personnel) Security ICT Certification and Accreditation Personnel Security Clearance Overseas Travel Physical Security Certification and Accreditation Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS PPEC	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex A to Protected Identities – Process for Granting Honours and Awards

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendices and Attachments

This DSPF Annex has no Appendices and Attachments.

Document administration

Identification

DSPF Annex	Protected Identities
Annex Version	2
Annex Publication Date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identity Security
DSPF Number	Control 42.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS PPEC	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Overseas Travel

General principle

1. Defence seeks to protect its people and information from threats or loss arising from official or private overseas travel.

Rationale

2. International travel may expose Defence Personnel and persons engaged under a contract to threats which could compromise national security and personal safety. Such threats may not be present in Australia and may therefore not be anticipated by travellers. For this reason it is crucial that travellers are briefed before travel to raise awareness of their destinations security environment, to ensure that adequate precautions are taken.

Expected outcomes

3. Defence Personnel and persons engaged under a contract are expected to:
 - a. notify relevant Departmental authorities of their travel plans in a timely manner;
 - b. be aware of security risks relevant to their travel destination;
 - c. be aware of additional security risks they may expect if they are a Sensitive Compartmented Information access holder;
 - d. protect official information (if being carried or accessed for official travel);
 - e. report suspicious contacts, security incidents or security concerns to their Security Officer (SO) and DS&VS security via submission of an XP168 (Suspicious contact) and XP188 (Security Incident Report), and the Australian Signals Directorate if a member of a Defence Intelligence Agency);
 - f. ensure that official visits to allied facilities are conducted in accordance with bilateral security responsibilities and hosting country business processes;

- g. use their Australian passport to exit and return to Australia if they are holders of a Positive Vetting clearance (unless granted specific permission to do otherwise); and
- h. remain aware of their security responsibilities (as per the DSPF) during travel.

Note: Certain countries, including the United States of America and Canada, have moratoriums and minimum lead times for processing official travel visit requirements. Defence Security & Vetting Service (DS&VS) Clearance Support Team (CST) can be contacted for further advice.

- 4. Defence Personnel and persons engaged under a contract are not to make false declarations regarding their employment. If required, the traveller is to list their status as “government employee” or “contractor”.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SP

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Overseas Travel
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 44
Version	4
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 44.1
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Eligibility and suitability of personnel; and ongoing assessment of personnel. Legislation: <u>ASIO Act 1979 (Cth)</u> <u>Work Health and Safety Act 2011 (Cth)</u>
Read in conjunction with	N/A
See also DSPF Principle(s)	DSPF 10 – <i>Classification and Protection of Official Information</i> DSPF 15 – <i>Foreign Release of Official Information</i> DSPF 45 – <i>Contact Reporting</i> DSPF 71 – <i>Physical Transfer of Information and Assets</i> DPSPF 77 – <i>Security Incidents and Investigations</i>
Implementation Notes, Resources and Tools	<u>DFAT Smartraveller</u> website Security forms and tools available on the DS&VS Security Toolkit: 1. Overseas Travel Briefing and Debriefing (Web form AB644) 2. Overseas Travel Defensive Briefing Guide 3. DSN country-specific threat advice Security of Information Agreements and Arrangements (SIAs) Defence Intelligence Security (DIS)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	August 2019	FAS S&VS	See DSPF Amendment List 1
3	30 May 2020	FAS S&VS	Deletion of references to DFAT Smartraveller registration and DSM and minor grammar updates
4	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Overseas Travel

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the Control Owner for this Enterprise-wide Control.

Escalation Thresholds

2. AS SPS has set the following general thresholds for risks managed against this Defence Security Principles Framework (DSPF) Control, and related Principle and Expected Outcome.

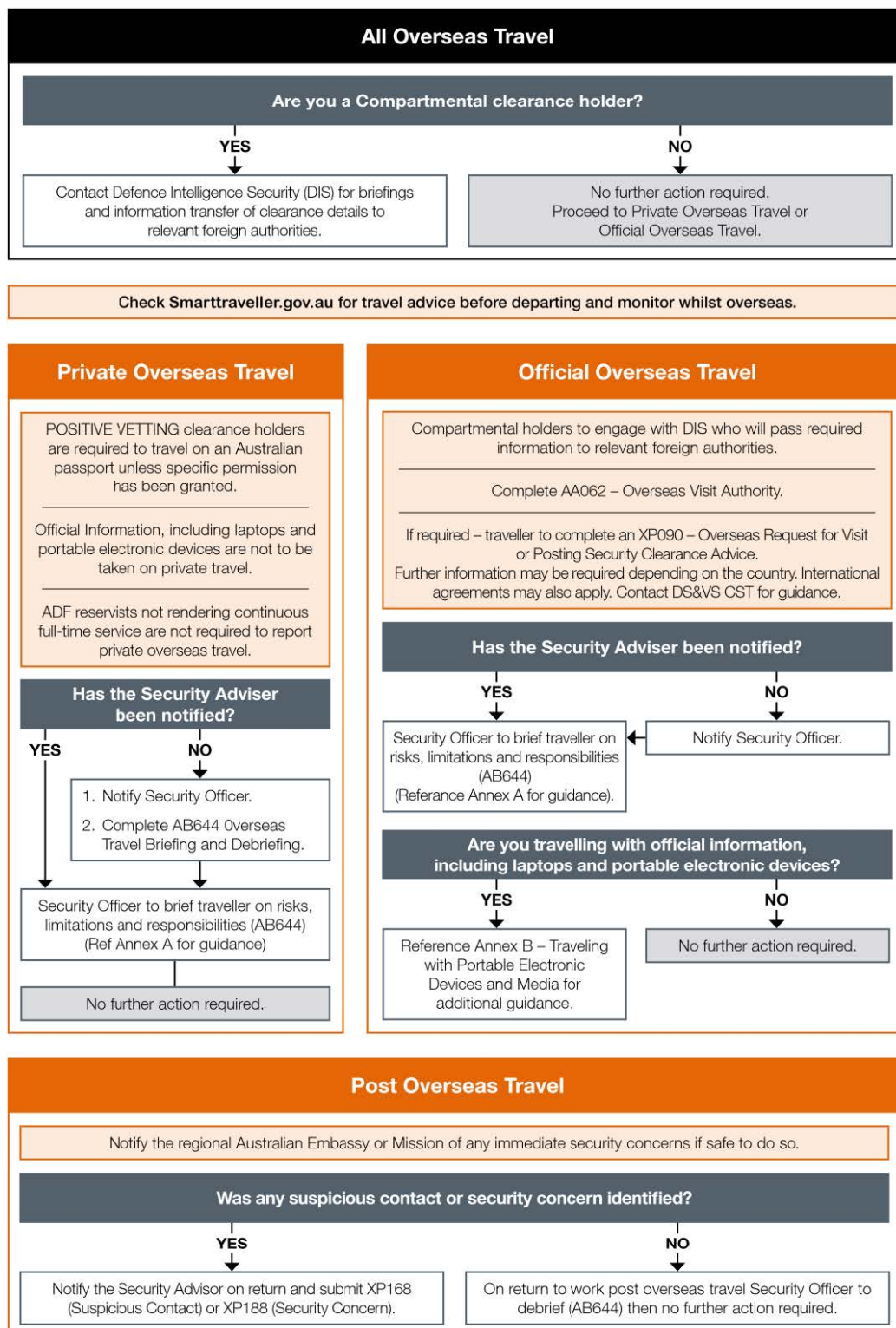
Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

3. Figure 1 outlines the Overseas Travel security process.

Note: the AA062 – Overseas Visit Authority is to be completed for official travel; and the AB644 – Overseas Travel Briefing and Debriefing is to be completed for personal travel.

Figure 1: Overseas Travel Security Process



Roles and Responsibilities

DSVS Clearance Support Team, Australian Signals Directorate Security and Executive Security Advisers

4. The Defence Security & Vetting Service (DS&VS) Clearance Support Team (CST), Australian Signals Directorate (ASD) Security and the Group and Services Executive Security Advisers (ESAs) are responsible for providing overseas security travel advice and compliance requirements.
5. The CST is responsible for end to end clearance processing, including referring Defence personnel and persons engaged under a contract security clearance details to foreign governments, and confirming foreign national security clearance details in accordance with Security of Information Agreements and Arrangements (SIA).
6. ASD Security is the compartment sponsor of Defence personnel and persons engaged under a contract, and is responsible for notifying foreign government's details (if held) of a traveller's Sensitive Information Compartments (SIC).

Commanders and Managers

7. Commanders and Managers are responsible for processing and approving overseas travel requests and for ensuring that all Defence personnel and persons engaged under a contract travelling overseas are aware of their security responsibilities in accordance with the DSPF.

Security Officers

8. The Security Officer (SO) is responsible for administering necessary administrative action to ensure compliance with the DSPF on behalf of their Commander, Manager or Defence Industry Security Program member executive. Administrative actions include:
 - a. recording travel details from the form AA 062 Overseas Visit Authority (for official travel) or AB644 – Overseas Travel Briefing and Debriefing (for private travel) in the Security Register and maintaining a copy of the forms at unit level;
 - b. supporting Defence personnel and persons engaged under a contract in comply with their security responsibilities in accordance with the DSPF, including assisting compartmentally briefed personnel report intended travel to the relevant compartment controller via ASD Security or Communications Intelligence Security Officer (COMSO);
 - c. providing overseas travel briefings and debriefings, including following up as required anything noted in the completed post travel -Section 4 – Debrief form AB644 – Overseas Travel Briefing and Debriefing (for private travel); and

- d. confirming that (if required) an XP090 – Overseas Request for Visit or Posting Security Clearance Advice has been completed for official travel and sent to the DS&VS CST securityclearances@defence.gov.au within the required timeframe specified in the SIA.
9. In the absence of a SO, the Commander or Manager is to allocate an alternate SO to conduct the overseas briefings and debriefings.

Example: *If a traveller with a Negative Vetting 1 clearance, and no Sensitive Compartment Information brief has no SO available for the travel brief or debrief, the unit COMSO is a suitable alternate.*

Key Definitions

Further Definitions

10. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes

Annex A – Overseas Travel Briefing and Debriefing Guide

Annex B – Travelling with Portable Electronic Devices and Media

Document administration

Identification

DSPF Control	Overseas Travel
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 44.1
Version	3
Publication date	31 July 2020
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Overseas Travel
Related DSPF Control(s)	DSPF 10.1 – <i>Assessing and Protecting Official Information</i> DSPF 15.1 – <i>Foreign Release of Official Information</i> DSPF 45 (Principle) – <i>Contact Reporting</i> DSPF 71.1 – <i>Physical Transfer of Information and Assets</i> DSPF 77.1 – <i>Security Incidents and Investigations</i>

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	30 May 2020	AS SPS	Deletion of references to DFAT Smartraveller registration, minor grammar, removal of duplicated information and references to the DSM
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex A to Overseas Travel – Overseas Travel Briefing and Debriefing Guides

Briefings

1. Table 1 outlines the process for briefing a traveller prior to overseas travel.
2. Note: the AA062 –Overseas Visit Authority is to be completed for official travel; and the AB644 - Overseas Travel Briefing and Debriefing is to be completed for personal travel.

Table 1: Briefing Process Prior to Overseas Travel

Stage	Who does it	Description
1	Person travelling	Complete the form AB644 – Overseas Travel Briefing and Debriefing for personal travel; or the AA062 - Overseas Visit Authority for official travel. Send relevant form to their Security Officer as soon as they plan to travel. Contact the relevant agency Security Officer for specific compartmented briefings (if applicable).
2	Security Officer	Conduct an overseas travel briefing with the person travelling. Complete the pre-travel Security Officer section of form AB644. Confirm that the person travelling has had required compartment briefings.
3	Person travelling	Obtain travel advice for the country(ies) being visited or transited through from the Department of Foreign Affairs and Trade (DFAT) Smartraveller website.

Stage	Who does it	Description
4	Security Officer	Record travel details in the Security Register. Retain the completed form AB644 (for private travel) or AA062 (for official travel). Conduct a more detailed briefing if: 1) the person travelling has a high level of access; 2) DFAT has issued a Consular Travel Advisory Notice or Bulletin for countries being visited or transited through; or 3) the person is travelling with a Defence or Defence Industry Security Program laptop or Portable Electronic Device (PED) (also referred to as a Mobility Device), and is not protected by a <i>Laissez-Passer</i> (refer Definitions below.)
5	Security Officer and Traveller	If there are any contact or security concerns the Security Officer or the traveller are to submit an online XP188 with attached form AB644 (private) or AA062 (official) If relevant, report any change of circumstances to AGSVA via the myClearance portal.

Note: If the traveller is conducting Official Travel the Security Officer is to ensure they are briefed on their obligations regarding remote access to Defence systems from outside Australia, as per Control 30.1.

Debriefings

3. The table below outlines the process for debriefing a traveller returning from overseas.

Table 1 – Debriefing Process When Returning from Overseas

Stage	Who does it	Description
1	Person travelling	Complete the debriefing section of the form AB644 (private or official) with their Security Officer.
2	Security Officer	Conduct an initial debriefing using the debriefing section of form AB644 .
3	Person travelling	Complete and submit relevant online forms (if applicable) to report : • XP188 – Defence Security Report.
4	Security Officer	Retain copies of completed forms (AB644 and, XP188) at Unit/Facility level.

Issues Covered in Debriefings

4. Travel debriefing is a formal process to discuss events that occurred during the visit, and to identify events which could later be used to threaten the security of the individual. This is a discussion not an interrogation, and the returning traveller should not be questioned as such.
5. Debriefing discussions include:
6. Travel procedures:
 - a. **Visa** – How and by whom the visa was obtained? Were any probing questions asked about employment?
 - b. **Entry and exit procedures** – What occurred? Did officers/officials conduct any searches? Were documents examined out of sight? Was there any suspicious or concerning interactions with officers/officials? and
 - c. **Travel arrangements** – Was travel undertaken alone or with an organised party? Was there contact with officials or tour guides in the country and, if so, was there anything about their behaviour to indicate they may have had an intelligence function? Was any special attention directed to the traveller or to other members of the organised party?
7. Accommodation:
 - a. Where did the traveller stay?
 - b. How and by whom was the accommodation arranged?
 - c. Was there a choice in accommodation?
 - d. Did any hospitality staff appear to behave in an unusual manner? and
 - e. Were any occurrences of eavesdropping or searches of luggage or rooms observed?
 - (1) Was the traveller carrying official information?
 - (2) Was the official information appropriately stored and/or accompanied?
 - (3) Was the official information left unattended in the traveller's hotel room at any time during the stay? and
 - (4) Was the traveller's room cleaned or serviced while the traveller was absent?

8. Contact with local nationals:

- a. Was any approach made to the traveller for any of the following reasons or did any of the following occur:
 - (1) currency exchange;
 - (2) bartering, such as an offer to purchase or swap any of the travellers belongings;
 - (3) sexual soliciting; or
 - (4) requests to carry mail/packages?
- b. Was any excessive interest taken in the traveller's employment?
- c. Was there any unusual contact with any uniformed official?
- d. Drugs or suspected food/drink spiking?
- e. Did anyone propose continued contact post visit? and
- f. Were any invitations of any type extended?

Note: This is not a definitive list of questions to ask, or reasons local nationals may seek to make contact with travelling Defence personnel and persons engaged under a contract

9. Contact with other travellers or non-locals living in the country:

- a. Was there any contact with tourists who did not seem to be genuine (e.g. people in their tour group, other hotel guests, other attraction visitors etc.)?

Definitions

10. **Laissez-Passer** – A document issued by a national government or international treaty organisation to allow a government employee to act as a temporary diplomatic courier. The Laissez-Passer confers diplomatic immunity on the contents of a diplomatic pouch carried by the person to whom the Laissez-Passer is issued. The Laissez-Passer does not confer diplomatic immunity on personal hand luggage or other belongings. The Laissez-Passer and diplomatic pouch are issued to an individual and they are not transferable.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Overseas Travel Briefing and Debriefing Guides
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Overseas Travel
DSPF Number	Control 44.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	30 May 2020	AS SPS	Minor grammar and content changes
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	12 May 2023	AS SPS	Form link corrections; Defence logo updated; minor addition to <i>Contact with local nationals</i> section; inclusion of reference to Control 30.1.



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Overseas Travel – Travelling with Portable Electronic Devices and Media

Travelling Overseas with a 'Handle As' Classification of UNCLASSIFIED

1. When Defence personnel and persons engaged under a contract travel overseas on Defence business with a Defence laptop or Portable Electronic Device (PED), including removable media with an actual Protective Marking of OFFICIAL, OFFICIAL: Sensitive (O: S) or PROTECTED, the Defence laptop or PED is to be encrypted with an Australian Signals Directorate (ASD)-approved product accredited to reduce the 'handle as' classification to OFFICIAL.
2. In these instances approval for carriage overseas is to be sought from, and recorded by, the relevant Security Officer and is to only be given when the travel is for official Defence business purposes. Official Defence business purposes may include private travel if the individual has a confirmed condition of employment to be on call whilst away on private travel. These Defence laptops or PEDs are to be carried as hand luggage.

Travelling Overseas with an 'Actual' Classification of PROTECTED and Above

3. Defence laptops or PEDs including removable media with a classification of CONFIDENTIAL or above are to be transported utilising either Diplomatic Safe Hand or carried as hand luggage by the Defence member with a *Laissez-Passer* (see Definition below); refer to DSPF Principle 71 – *Physical Transfer of Information and Assets* for further guidance. This applies even if the Defence laptop or PED is encrypted with an ASD approved product to reduce its 'handle as' classification to OFFICIAL: Sensitive.

Storage Overseas

4. Physical access to a Defence laptop or PED may allow covert modification of the device to circumvent the cryptographic controls through techniques such as the installation of a hardware key logger. Defence personnel Contractors, Consultants and Outsourced Service Providers travelling overseas with a Defence laptop or PED are reminded that they are not to store classified or sensitive material in hotel rooms or hotel safes unless that material, including the Defence laptop or PED is stored in a tamper evident manner, refer to DSPF Principle 71 – *Physical Transfer of Information and Assets* for further guidance.

Requests to Search a Defence Laptop or PED

5. Most countries equate the random search of a laptop or PED with a random luggage search. Defence personnel and persons engaged under a contract are not exempt from such searches. They are to comply with the request for a search unless they are carrying a *Laissez-Passer* protecting the Defence laptop or PED.

Key Definitions

6. ***Laissez-Passer***: A document issued by a national government or international treaty organisation to allow a government employee to act as a temporary diplomatic courier. The Laissez-Passer confers diplomatic immunity on the contents of a diplomatic pouch carried by the person to whom the Laissez-Passer is issued. However, it does not confer diplomatic immunity on their hand luggage or other belongings. The Laissez-Passer and diplomatic pouch are issued to an individual and are not transferable.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Travelling with Portable Electronic Devices and Media
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Overseas Travel
DSPF Number	Control 44.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Contact Reporting

General principle

1. All Defence personnel and persons engaged under a contract should report contacts of security concern to assist in the identification of any attempts to cultivate Defence's people and/or acquire access to official, classified or sensitive materials.
2. All clearance holders are required to report defined contacts with foreign officials or other foreign nationals or any requests from foreign officials to access government assets or security classified information or resources.

Rationale

3. Foreign intelligence services and other threat actors devote considerable resources to obtain access to political, economic, scientific, technological, military and other information. This is not limited to classified information and often includes privileged information. Any compromise may be prejudicial to Australia's National Interest. Small pieces of information could contribute to an intelligence collection process. Accordingly, Defence personnel and persons engaged under a contract need to recognise that an 'innocent' conversation or 'contact' (e.g. e-mail, social media) can be part of human intelligence gathering.
4. The Australian Government Contact Reporting Scheme is managed by the Australian Security Intelligence Organisation (ASIO). The Scheme assists ASIO to identify activity directed against Australia and its interests including people who hold an Australian Government security clearance. ASIO uses this intelligence to assist in the formulation of threat assessment and security intelligence advice and to protect the national interest.

Expected outcomes

5. Defence Security and Vetting Service collects and assesses contact reports and coordinates the Defence input into the Australian Government Contact Reporting Scheme;
6. Defence personnel and persons engaged under a contract report suspicious, on-going, unusual or persistent contacts with foreign officials and other foreign nationals (see Implementation Notes, Resources and Tools below);.

7. Defence personnel and persons engaged under a contract report instances when an individual or group, regardless of nationality, seeks to obtain official information they do not require access to;
8. Defence personnel and persons engaged under a contract understand security threats to inform their reporting obligations; and
9. Security clearance holders understand their obligations under this principle and their responsibilities to report contact which causes security concern (See 'Read in Conjunction With' section below and DSPF Principle 40 – *Personnel Security Clearance*).

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Security Officer, Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Service or Group Security Authority or Director Security Intelligence and Threats
High	Assistant Secretary Security Threat and Assurance (ASSTA)
Extreme	Defence Security Committee – through ASSTA

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Contact Reporting
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	45
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	ASSTA

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Entity physical security. Legislation: <u>ASIO Act 1979</u> Standards: <u>Joint Directive 32/2014 – Association with Unlawful or Inappropriate Groups by Defence Personnel</u>
Read in conjunction with	<u>PSPF 5 - Reporting on security</u> <u>PSPF – Personnel Security</u>
See also DSPF Principle(s)	Personnel Security Clearance Identity Security Overseas Travel Counterintelligence Off-site Work Physical Transfer of Official Information, Security Protected and Classified Assets Security Incidents <u>and Investigations</u>
Implementation Notes, Resources and Tools	<u>DS&VS Security Portal</u> <u>Defence Form XP168</u> - Report of Security Contact Concern [available through DS&VS Security Portal, Defence Industry Portal and through USO]

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Counterintelligence

General principle

1. Counterintelligence (CI) activities identify and counteract the security risks posed by organisations or individuals engaged in espionage, sabotage, politically motivated violence (including terrorism), criminal activities or other threats to Defence. Defence undertakes CI activities with other intelligence, security and law enforcement agencies that are governed by legislation allowing CI investigations and operations.

Rationale

2. Defence personnel and persons engaged under contract have access to and knowledge of information that could compromise national security through accidental or deliberate disclosure. Defence CI informs the security standards mandated by Government and support the mitigation of risks arising from foreign intelligence services, politically motivated groups, terrorists and disgruntled staff. A robust CI capability will ensure Defence can identify and coordinate a response to threats to Defence.

3. Because of the nature of CI threats, notably from foreign intelligence services, and the sensitive compartmented measures needed to counter these threats, dedicated CI processes and capabilities are required.

Expected outcomes

4. All Groups and Services understand the threat to their people, information, assets and infrastructure and have measures to mitigate them. Where specific process or additional measures are identified to counter specific threats, advice may be provided by DS&VS.

5. Defence personnel and persons engaged under contract have access to timely and relevant security advice.

6. Defence personnel and persons engaged under contract report suspicious, on-going, unusual or persistent contacts with external parties through an XP168 Contact Report (see Implementation Notes, Resources and Tools below.)

7. DS&VS collects, assesses and investigates Contact Reports and, wherever necessary, forwards them to the Australian Security Intelligence Organisation and enacts suitable countermeasures.
8. DS&VS liaises and coordinates with other government agencies for nonoperational CI related activities to contribute to a whole-of-government security regime.
9. Joint Operations Command is responsible for coordinating operational CI activities.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Security Officer, Supervisor, Commander or Manager
Moderate	Service or Group Security Authority or Director Security Intelligence and Threats
Significant	Assistant Secretary Security Threat and Assurance (ASSTA)
High	Defence Security Committee – through ASSTA
Extreme	Secretary and Chief of Defence Force

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Counterintelligence
Principle Owner	First Assistant Secretary Security and Vetting Services (FAS S&VS)
DSPF Number	Principle 46
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	ASSTA

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Entity physical resources. Legislation: <i>Intelligence Services Act 2001</i> <i>Australian Federal Police 1979 (AFP) Act (Cth)</i> <i>Crimes Act 1914 (Cth)</i> <i>ASIO Act 1979</i>
Read in conjunction with	ADDP 2.1 Counterintelligence and Security
See also DSPF Principle(s)	Assessing and Protecting Official Information Personnel Security Clearance Security Awareness and Training Contact Reporting Physical Transfer of Official Information, Security Protected and Classified Assets Security Incidents and Investigations
Implementation Notes, Resources and Tools	ADDP 2.1 Counterintelligence and Security DS&VS Security Portal Defence Form XP168 – Report of Security Contact Concern [via DS&VS Security Portal] <i>ASIO Act 1979</i>

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Working Offsite

General principle

1. Security measures are in place, and practices are followed, to protect Official Information and assets from unauthorised access when the person using the information or assets is working away from their usual workplace.

Rationale

2. Defence personnel and persons engaged in contract may need to undertake duties outside their usual workplace.

3. When work is being performed outside the usual workplace, there is an increased risk of Official Information being accessed without authorisation – this may compromise national security, impact Defence capability, or have a negative effect on Defence's reputation.

Expected outcomes

4. Defence personnel and persons engaged under contract protect official information taken outside their usual workplace.

5. Offsite workplaces are properly assessed to identify any security vulnerabilities that need to be addressed before Official Information is used or stored there.

6. Defence personnel and persons engaged under contract follow security measures and practices to prevent unauthorised access by, or disclosure to, those who do not have the appropriate security clearance and a need-to-know.

7. Defence personnel and persons engaged under contract are aware of the increased security risks associated with working offsite.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Band 1/O-7 (or higher) in relevant Group/Service
High	Assistant Secretary Security Policy and Services (AS SPS)
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Working Offsite
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 70
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 70.1
Control Owner	AS SPS

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Robust ICT systems; Access to information; Entity physical resources; and Entity facilities. Legislation: <u>Work Health and Safety Act 2011</u> <u>WHS Regulations</u> <u>WHS Codes of Practice</u> Standards: <u>AS ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements</u>
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Audio-visual Security ICT Certification and Accreditation Personnel Security Clearance Contact Reporting Physical Transfer of Information and Assets Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	1. <u>PSPF – 15 Physical security for entity resources (Working away from the office)</u> 2. PSPF – 8 Sensitive and classified information 3. PSPF – <u>5 Reporting on security</u> 4. <u>Better Practice Checklist – 21. ICT Support for Telework</u> 5. PSPF – <u>3 Security planning and risk management</u> 6. Defence People Group Telework Policy 7. <u>Information Security Manual</u>

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Working Offsite

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The AS SPS has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group or Service
Significant	Band 1/O-7 (or higher) in relevant Group or Service
High	AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Introduction

3. Persons engaged under a contract undertaking approved offsite work within Australia, are to apply appropriate security controls in accordance with the DSPF and any applicable, referenced material.
4. This policy covers the security of Official Information and assets. It does not extend to Work Health and Safety (WH&S) matters.

Offsite Work

5. Offsite work includes work undertaken:
 - a. at the person's home (whether or not there is an approved Telework arrangement in place);
 - b. during official travel (for example in a hotel, on an aircraft, or in a conference environment); or
 - c. at a Defence contractor's premises.

Example: Mary reviews and drafts official documents and checks her Defence email whilst at her home; she does this on her own computer by logging into Defence Remote Electronic Access and Mobility Services (DREAMS) – which is an accredited gateway.

6. Prior to approving offsite work arrangements, the approving authority should take into account whether the location being used has been assessed for security vulnerabilities, and the extent to which those vulnerabilities may be mitigated. Refer to 'Approvals' (below) in this Control.

7. In addition to meeting security requirements, Defence personnel may require approval to undertake offsite work in accordance with the Defence Telework Policy.

Protecting Official Information

8. Defence personnel and persons engaged under contract are to ensure that Official Information is protected from unauthorised access. Refer to DSPF Principle 10 – *Assessing and Protecting Official Information*.

9. Defence personnel and persons engaged under contract must not allow people without the appropriate clearance, and a legitimate need-to-know, to access Official Information. The need-to-know principle applies at all times.

10. Where it is reasonable to assume uncleared people cannot see, hear or record the information, approval is not required before accessing the following Official Information offsite:

- a. Information that is OFFICIAL – in either hard copy or electronic (soft copy) format; and
- b. Information that is OFFICIAL:Sensitive or classified as PROTECTED – in soft copy only, via an accredited remote access system such as DREAMS, or via a device that has a 'handle-as' classification of OFFICIAL:Sensitive or lower. Refer to Key Definitions (below) for an explanation of handle-as classifications.

Example: Robin is travelling and working from his hotel room on a Defence laptop. He may access Official Information classified as PROTECTED when using DREAMS to access the Defence network, provided that uncleared people cannot see the information.

Hard Copy Documents

11. Approval in writing from a Commander, Manager or Contract Manager is required before Defence personnel and persons engaged under contract may remove OFFICIAL: Sensitive or higher (i.e. 'PROTECTED' and above) material from Defence premises to conduct offsite work.
- a. Refer to DSPF Control 71.1 – *Physical Transfer of Information and Assets* and DSPF Control 72.1 – *Physical Security* for policy related to the authorised removal of this material
 - b. Refer to DSPF Controls 10.1 – *Assessing and Protecting Official Information* and 72.1 – *Physical Security* for policy related to the minimum physical storage requirements for Official Information.
12. An auditable record of protectively marked documents and material removed from Defence premises is to be maintained. Material classified TOP SECRET and above must be recorded in an XC-40 Classified Document Register (CDR) in accordance with Annex E to Control 10.1 – *Assessing and Protecting Official Information*.
13. Whilst in transit, Official Information in hard copy (or on a device's screen) with a classification of PROTECTED or above must not be accessed or viewed in any setting where the information may be exposed to people without the appropriate clearance, and a legitimate need-to-know. The information is to remain secured in accordance with the DSPF Control 71.1 – *Physical Transfer of Information and Assets* at all times in such locations.

Example: It is a security breach to review hard copy PROTECTED documents whilst sitting in a café, a restaurant, on board a flight, etc.

Classified ICT Equipment and Media

14. Approval is required before Defence personnel and persons engaged under a contract may remove ICT equipment, or media with a 'handle as' classification of PROTECTED or above from Defence premises to conduct offsite work.
15. Encrypted ICT equipment or media with a 'handle as' classification may resume its actual classification once powered up, or when hibernating. Personnel must consider their environment and remain cognisant of their security obligations when using encrypted ICT equipment or media when working offsite. Refer to 'Actual and 'handle-as' security classifications for encrypted devices and media' in Key Definitions below and to any SOPs for the specific equipment.

Example: A Defence laptop with an actual classification of PROTECTED has its handle-as classification reduced to OFFICIAL by ASD-approved encryption. The laptop is put into hibernation mode at work and taken home prior to an offsite meeting the next day – this leaves the laptop unencrypted and its security must therefore be managed in accordance with its actual classification of PROTECTED.

Classified Conversations

16. Conversations involving classified information should not occur where persons without the appropriate clearance, and a legitimate need-to-know, may overhear or utilise other technological means to eavesdrop on or record the conversation.

Example: Although secure mobile phones with ASD-approved encryption allow the user to make classified calls from unsecured areas, this introduces the risk of eavesdropping on the people having the conversation.

17. Offsite classified conversations are to be protected from being overheard or recorded. See [PSPF 15 Physical Security for Entity Resources – Working away from the office](#) for guidance on the measures that can be used to reduce the threat of conversations being overheard or recorded.

18. Where classified conversations are conducted at home, e.g. on a secure phone, attention needs to be paid to the presence of uncleared persons.

Note: Be mindful of your surroundings, such as children overhearing classified conversations. Exposing them to classified information is a security risk. Similar precautions should be taken with smart home devices, such as Google Home or Alexa. These devices should be turned off.

19. Personnel **must not** continue with working offsite arrangements where there is an expectation that classified discussions occur regularly. Alternative working arrangements or expectations should be considered.

Note: There is an increased risk of Foreign Intelligence Services (FIS) targeting premises where classified conversations occur regularly.

Overnight Carriage

20. Overnight carriage of classified information is covered in DSPF Control 71.1 – *Physical Transfer Information and Assets*. Relevant material is to remain secured in a tamper-evident enclosure whilst in transit between secure locations, appropriate locations for overnight stops, or locations approved for offsite work.

Geo-location Security

21. Geo-location is the process or technique of identifying the geographical location of a person or device by means of digital information processed via the Internet.

22. In the rare event the location of an out of office trip is classified, location data is to be protected by:

- a. not using a mobile telephone (ID/SIMM cards could be used to track the device);
- b. turning off any GPS equipment or applications;

- c. disabling any application location services;
- d. not logging into any social networks; and
- e. not taking photos.

Note: Geo-location security may apply to operations and operational areas, requiring that their location remains unknown to those without both a need-to-know and a right-to-know. Further details will be covered in any Operational Security instructions.

Physical Storage Requirements for Offsite Work

23. Defence personnel and persons engaged under contract conducting offsite work are required to comply with procedures for handling and protecting Official Information during its use, storage, transfer and transmission. Refer to DSPF Control 10.1 – *Assessing and Protecting Official Information*, DSPF Control 71.1 – *Physical Transfer of Information and Assets* and DSPF Control 72.1 – *Physical Security*.

24. Whilst undertaking offsite work, ICT equipment and media is to be stored in accordance with the [Information Security Manual \(ISM\)](#) – ICT Equipment and Media chapter.

25. Accredited remote access systems, and products that implement ASD-approved encryption, may have the effect of reducing the actual classification of material to a lower 'handle-as' classification when the encryption is active.

Note: These protection measures will not work unless the encryption is activated. A device in standby power mode may not be protected, so users are to follow the device's Standard Operating Procedures (SOPs) and ensure it is in a secure state when left unattended.

Example: A Defence laptop is being used to process and store information up to the classification of SECRET and as such the laptop itself has a classification of SECRET. ASD approved encryption is used to reduce the device's 'handle-as' classification to OFFICIAL. A security container is not, therefore, required to store the device when it is powered off – although the device still requires normal protections from fire and theft. When the device is powered on or in hibernation mode then it resumes its classification of SECRET and should be stored accordingly.

26. If information or assets with a 'handle-as' or 'actual' classification of PROTECTED or above need to be stored at home, authorisation for offsite work is required from your commander/manager.

- a. Refer to DSPF Control 71.1 – *Physical Transfer of Information and Assets* and DSPF Control 72.1 – *Physical Security* for policy related to the authorised removal and secure storage of the material.

Disposal of Official Information

27. Defence personnel and persons engaged under contract working offsite are required to dispose of classified waste in accordance with DSPF Principle 10 – *Assessing and Protecting Official Information*. If classified waste cannot be disposed of appropriately when offsite, it is to be securely stored until it can be securely transferred to a facility where proper disposal may occur.

Reporting Security Incidents

28. When Defence personnel and persons engaged under contract working offsite become aware of any incident that may indicate or suggest that classified or official material has been compromised, tampered with or stolen, they are to immediately report this in accordance with the DSPF Principle 77 – *Security Incidents and Investigations*.

29. Any recommended remedial action arising from an incident must then be taken by the employee.

Example: A failed break and enter at a home-based work property may require investigation or additional security measures to be implemented even though there is no evidence of Defence material being targeted.

Approvals

Remote Access Approvals

30. Defence permits remote access to some of its ICT networks via accredited remote access solutions (e.g. DREAMS). Policy pertaining to the use of remote access is located in DSPF Control 30.1 -Remote Access to Defence Systems.

Note: The use of personal email accounts (such as Gmail, Hotmail and personal outlook accounts) and applications (such as Signal, Zoom and WhatsApp) cannot be used by personnel for the transmission or storage of Official Information, in accordance with Control 30.1 – Remote Access to Defence Systems. Refer to Control 10.1 – Assessing and Protecting Official Information for advice on protective markers and security classifications.

31. Defence personnel and persons engaged under contract must not use privately owned devices to process or store any Defence Official Information that has not been authorised for public release, as per DSPF Control 30.1 – *Remote Access to Defence Systems*.

Example: Alex is working from home using DREAMS. They are experiencing issues logging in to the DREAMS network and had a colleague forward Classified emails and documents to their Gmail account so they can continue working. This is a security breach.

32. Defence Personnel and persons engaged under contract must not reclassify information in order to allow it to be sent, or accessed from, offsite. Reclassifications are only to occur in line with DSPF Control 10.1 – *Assessing and Protecting Official Information*.

Example: Bob reclassifies a SECRET document to OFFICIAL in order to be able to access it remotely from home. This is a security breach and is not allowed.

Offsite Work Approvals -Physical

33. Offsite work requiring the physical handling, storage or destruction of Official Information or an asset with a 'handle-as' classification of PROTECTED or above, other than CODEWORD information, requires the approval of (at minimum) an SES Band 1/O-7 in the user's chain of command or the First Assistant Secretary Security and Vetting Service (FAS S&VS). This role cannot be delegated.

34. Approval from the originator must be provided when Defence is not the sole originator of the classified material.

35. Offsite work requiring the physical handling, storage or destruction of material classified TOP SECRET, or that carries a CODEWORD, requires the approval of DEPSEC SPI. This authority may not be delegated below SES Band 1/O-7, and additionally requires the prior approval of both ASIO and the originating agency.

36. The following questions are to be considered when approval for offsite work is being considered:

- a. Has a current Security Risk Assessment (SRA) been completed?
- b. Is there a real need to remove the classified material from Defence premises?
- c. Are there appropriate storage options at the offsite work site for the classified material being stored, handled or destroyed? This will require the approval authority to strike a balance between the requirements for offsite work with the physical security measures in place at the location.
- d. Have the ICT systems to be used been accredited to handle the highest classification of work to be conducted in accordance with DSPF Principle 73 – *Physical Security Certification and Accreditation*?
- e. Have Standard Operating Procedures (SOPs) for the transfer, handling, storage and destruction of Official Information at the home-based site been developed? and
- f. Has the employee been briefed by their Security Officer on the policies contained in the DSPF and any agreed SOPs?

37. Material is to remain in the personal custody of the individual and stored appropriately when not in use, in accordance with DSPF Control 72.1 – *Physical Security*.

Standard Operating Procedures (SOPs)

38. In addition to a formal agreement to undertake offsite work, it may be appropriate to develop SOPs – these may include:

- a. specifying the highest classification of work to be conducted by the employee off site including:
 - (1) classification of discussions allowed;
 - (2) classification of information processed on ICT systems; and
 - (3) classification of information stored, handled or destroyed;
- b. the requirement for a completed and current (no more than 24 months old) SRA covering the place where offsite work will occur;

Example: The security assessment should address security matters (including physical security) additional assessments may be required from a Work Health and Safety perspective.

- c. identifying the equipment that is to be supplied by either party or shared in order to perform the duties;
- d. any restrictions on equipment usage;

Example: Susie has carer responsibilities and has been provided a Defence laptop to be able to work from home. It is not permissible for her child to use the laptop to browse the internet even while supervised by Susie.

- e. whether ICT or physical certification and accreditation is required and where copies of the relevant certificate(s) will be held;
- f. whether Defence has the right to conduct compliance checks and determine how official resources are protected at the home-based site;
- g. procedures for the secure handling, storage and destruction of Official Information, including the provision of security containers suitable to store the maximum classification of information to be held;
- h. procedures for the disposal or return of classified waste;
- i. the requirement to report any security incidents at the premises to DS&VS;
- j. procedures for the transfer of classified material between other Defence or approved premises and the home-based site; and
- k. confirming the holder is prepared to accept responsibility for the safe custody of any material accessed while offsite.

Accreditation

39. For accreditation purposes, a home-based site is considered the same as any other Defence facility. Refer to the DSPF Control 73.1 – *Physical Security Certification and Accreditation* to determine if accreditation is required.
40. Physical accreditation of a home-based site is not required where:
- Official Information is only accessed in electronic form, the information's classification is PROTECTED or below (if using DREAMS), and the offsite device used to access the information is protected by an ASD-approved encryption that reduces the 'handle-as' classification to OFFICIAL or OFFICIAL:Sensitive when the device is not in use;
 - hard copies of information handled, stored or destroyed do not exceed the security classification of OFFICIAL.

Protecting Official Information at Events such as Conferences and Workshops

41. Official Information, compromised in any environment, has the potential to undermine Defence's reputation. Consideration should be given to the risks associated with having Official Information or material at any event, activity or meeting.
42. Security instructions should be developed before any event is held in a public venue or Zone One area involving security classified information, assets or other Official Information that has not been approved for public release.
43. Security instructions can be simple but need to be tailored to the event and based on a current SRA. Depending of the nature of the event, they should consider items including:
- entry and access control, including identification of staff and visitors, escort requirements, ratio of visitors to escorts;
 - the carriage/transfer of Official Information to and from the venue;
 - security clearances of facilitators, venue staff and escorts who may have access to classified material;
 - the storage and handling of Official Information that is not for public release, including disposal and reproduction;

Example: *Kylie uses the photocopier at a conference venue to copy Official Information that she needs to use for her presentation – this may leave a copy of the document in the machine's memory that could later be accessed by unauthorised people.*

- access control procedures;

- f. reporting process and requirements for security incidents;
 - g. security of equipment on display or in attendance;
 - h. the possibility of protest action or Foreign Intelligence Service collection activity (advice on these matters may be sought from DS&VS); and
44. In the case of CODEWORD material, the agreement of the relevant compartment controller must be gained prior to the material being taken to any offsite event.
45. If classified information is to be discussed in non-accredited areas, advice must be obtained from either DS&VS, or in the case of CODEWORD information, compartment controllers. Technical Surveillance Counter Measures (TSCM) may also be required. Refer to DSPF Principle 14 – *Audio-visual Security*. TSCM advice should also be obtained following any such discussions.
46. If classified information or assets need to be stored in a Zone One or Zone Two event site, for example overnight storage, advice should be obtained from the DS&VS regional office. Refer to DSPF Principle 72 – *Physical Security*.
47. For more general guidance on event security refer to [PSPF 15 Physical security for entity resources](#).

Roles and Responsibilities

Deputy Secretary Strategic Policy and Intelligence (DEPSEC SP&I)

48. DEPSEC SP&I is responsible for approving offsite work involving the handling, storage or disposal of information that is classified TOP SECRET or carries a CODEWORD.

CODEWORD Compartment Controllers

49. Compartment controllers are responsible for providing advice to DEPSEC SP&I with regard to the approval, or otherwise, of offsite work involving Official Information that carries any CODEWORD for which they have a compartment control responsibility.
50. For compartments managed on behalf of external agencies, compartment controllers are to liaise with those agencies on matters of shared security risk.

Executive Security Advisers (ESA)

51. Executive Security Advisers (ESA) are responsible for assessing the security arrangements for, and managing any accreditation of, home-based work arrangements for Defence personnel and persons engaged under contract employed in single-service units.

Commanders, Managers and Contract Managers

52. Commanders, Managers and Contract Managers are responsible for the approval of offsite work:

- a. where physical storage is required for OFFICIAL information;

Note: Commanders, Managers and/or Contract Managers cannot approve offsite work that requires physical storage of information with a 'handle-as' classification of PROTECTED or above.

- b. for remote access (such as DREAMS) to systems up to PROTECTED (this does not include hard copy documents).

Managers of person/s engaged under a contract

53. Managers of persons engaged under contract are to gain the approval for offsite work for any affected staff from or through the relevant Defence Contract Manager before permitting work from home to be conducted involving Defence information or assets.

Key Definitions

54. **Home.** A private dwelling, Defence supplied accommodation (including service accommodation in barracks and on exercise), or an approved alternative place of work.

Exclusion: For industry, where the private dwelling is the primary place of business it is considered as a facility and requires accreditation in accordance with DSPF Principle 73 – Physical Security Certification and Accreditation.

55. **Offsite Work.** Offsite work is work undertaken in any location not recognised as a usual workplace. This does not include work conducted on operations (with the exception of approval processes for the conduct of classified work in accommodation areas such as barracks) and does not cover Defence ICT support to Australian Defence Force (ADF) deployments.

56. **Home-based Site.** A security accredited private dwelling or other location that has been agreed between Defence and an employee as regular place of work.

57. **Home-based Employee.** An employee working at a home-based site.

58. **Home-based Work Agreement.** A formal agreement between an employee and Defence documenting the conditions of home-based work.

59. **Public Site.** Any place where neither the employee nor Defence can exert physical control over the local environment e.g. hotels, conference rooms, public transport, airport lounges etc.

60. **Defence Controlled Device.** A device is under Defence control if it is owned by Defence or is subject to any agreement that legally binds the owner of the device

to comply with all DSPF and ISM security policies. Defence controlled devices include security classified assets owned by Defence Industry Security Program (DISP) members.

***Example:** A DISP member supplies their own computer to process SECRET information. DISP membership contractually obliges the company to comply with all Commonwealth policies and the DSPF therefore the device is under Defence control.*

61. **Privately Owned Device.** A device where the end user has administrative control, responsibility and legal authority over the device's configuration. End users can exert control over these devices.

***Example:** A home computer or personal mobile phone. The end user can install their own virus detection software.*

62. **Public Device.** A subset of Privately Owned Devices where the end user has no administrative control over the device, they are not responsible for, and have no legal authority over, the configuration of the device.

***Example:** Internet kiosks and shared computers in hotels.*

63. **Australian Signals Directorate Approved Encryption.** Any cryptographic functionality that is implemented in accordance with all of the relevant requirements of the ISM Cryptography Section (including any product specific advice or in the Australian Communications Security Instructions (ACSI) series publications) in order to reduce the handling and storage requirements of the device.

64. **Actual and 'handle-as' Security Classifications for Encrypted Devices and Media.** Where ASD-approved encryption is applied to a device/media, that device/media has two different classifications. These are:

- a. the **actual classification**: the highest classification of information stored on or processed by the device/media, regardless of whether encryption has been applied; and

***Note:** This classification also applies whenever the device/media is in a keyed state, i.e. where the classified information is accessible in an unencrypted form.*

- b. the **'handle-as' classification**: the classification of the device/media when the classified information it contains is fully protected by encryption.

***Note:** This classification enables the device to be stored and physically transferred at a reduced classification due to the protection provided to stored information through the application of suitable ASD-approved encryption technology.*

Note: If ASD-approved encryption is not used, the actual and 'handle-as' classifications are the same, i.e. the highest classification of data stored or processed on the device/media.

Exclusion: Some ASD-approved technologies such as remote access solutions (e.g. DREAMS) have been evaluated to ensure that information is not recoverable from the hosting device once the session ends. In these instances the product's evaluation documentation will advise of the levels of protection offered.

Further Definitions

65. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Working Offsite
Control Owner	AS SPS
DSPF Number	Control 70.1
Version	5
Publication date	2 November 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Working Offsite
Related DSPF Control(s)	Assessing and Protecting Official Information Audio-visual Security ICT Certification and Accreditation Personnel Security Clearance Contact Reporting Physical Transfer of Information and Assets Physical Security Certification and Accreditation Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	9 April 2020	AS SPS	Foundational review; PSPF update; security classification alignment; update of terms defined in Defence Instruction: Administrative Policy; and update to align with flexible working arrangements during COVID-19 including dispensation Defgram 147/2020.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF
4	3 August 2020	AS SPS	Update of dispensation Defgram 147/2020 to Defgram 315/2020
5	30 October 2020	AS SPS	Removal of dispensation Defgram 315/2020 (expired 30 October 2020)



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Physical Transfer of Information and Assets

General principle

1. Defence is to ensure that Official Information, and security protected and classified assets, are transferred in a secure manner and are only received by the intended recipient.

Rationale

2. Official Information, and security protected and classified assets, are vulnerable to loss or compromise when being transferred, which may have negative impacts on Defence and wider Government.

Expected outcomes

3. Official Information, and security protected and classified assets, are:
- a. to remain secure and uncompromised during transfer;
 - b. only transported by authorised people or entities;
 - c. tracked during their physical transfer; and
 - d. received by the intended recipient.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Threat and Assurance (AS STA)
High	Defence Security Committee (DSC) – through AS STA
Extreme	DSC – through AS STA

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Physical Transfer of Information and Assets
Principle Owner	FAS S&VS
DSPF Number	Principle 71
Version	3
Publication date	22 September 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 71.1
Control Owner	Assistant Secretary Security Threat and Assurance (AS STA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Entity physical resources Other: Vienna Convention On Diplomatic Relations (1961) Articles 27 and 40
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Communications Security (COMSEC) Information Systems (Logical) Security Overseas Travel Working Offsite Physical Security Security Incidents and Investigations Explosive Ordnance Security Radioactive Sources Escorting Security Protected or Classified Assets
Implementation Notes, Resources and Tools	• PSPF 15 Physical Security for entity resources • ASIO, Security Equipment Guides (SEGs) are available from the GovDex Protective Security Community • Security Equipment Evaluated Product List (SEEPL) – refer also Security Toolkit: Security Equipment Guides • Defence Courier Service (DCS) contract user guide • Australian Radiation Protection and Nuclear Safety Agency Security of Radioactive Sources – Code of Practice

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF update of language to reflect Defence Admin Policy.
3	22 September 2020	FAS S&VS	Control Owner transferred to AS STA on 31 August 2020



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Physical Transfer of Information and Assets

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

Annex A – *Transport of Bulk Assets*

Annex B – *Developing a Movement Security Plan*

Document administration

Identification

DSPF Control	Physical Transfer of Information and Assets
Control Owner	ASSTA
DSPF Number	Control 71.1
Version	4
Publication date	22 September 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Transfer of Information and Assets
Related DSPF Control(s)	Assessing and Protecting Official Information Communications Security (COMSEC) Information Systems (Logical) Security Overseas Travel Working Offsite Physical Security Security Incidents and Investigations Explosive Ordnance Security Radioactive Sources Escorting Security Protected or Classified Assets

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy;
3	10 August 2020	AS SPS	BIL review for PSPF classification changes.
4	22 September 2020	AS SPS	Control Owner transferred to AS STA on 31 August 2020



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Physical Transfer of Information and Assets -Transport of Bulk Assets

General Requirements

1. Classified and high-risk unclassified assets are to be transported in accordance with the policy below based on their assigned Business Impact Level (BIL). Both classified and high-risk unclassified assets will have BILs assigned to them.
2. Where an asset has an assigned BIL which is higher than its corresponding classification due to higher integrity/availability factors, the appropriate BIL must be used to base transport measures upon. This is because measures based on the BIL will deal more adequately with the risk faced during transport due to the higher level of consequence of loss or damage to the asset.

Example: A high-risk unclassified asset has an assigned BIL of 4 (Extreme) due to the higher level of consequence to Defence if the asset were to be lost or compromised. As the BIL is higher than the sensitivity or classification of the asset, a more secure transport option, based on the higher BIL, is required.

Packaging

3. Classified and high-risk unclassified assets are to be packaged appropriately so that they are not exposed or damaged during transit. To achieve this, security-protected assets assigned a BIL of 3 (High) and above (classification of 'PROTECTED' and above) are to be packaged and sealed in a manner that ensures:
 - a. anonymity and security from viewing is achieved;
 - b. the packaging is tamper evident;
 - c. the asset is protected against damage;
 - d. the chance of loss is minimised; and
 - e. the opportunity for theft is reduced.

Note: The Supply Chain Branch of Joint Logistics Command can provide advice on appropriate methods of packaging and sealing.

Movement Security Plan

4. A Movement Security Plan (MSP):
 - a. must be developed for the transport of assets:
 - (1) assigned a BIL of 4 (Extreme) or 5 (Catastrophic); or
 - (2) classified 'SECRET' or 'TOP SECRET';
 - b. should be developed for the transport of assets:
 - (1) being transferred internationally;
 - (2) assigned a BIL of 3 (High); or
 - (3) classified 'PROTECTED'.
 - c. is recommended for assets assigned a BIL of 1 (Low) and 2 (Low-Medium). For guidance on how to develop an MSP, refer to Annex B of this Control.

Guarding and Escorts

5. The question of whether guards or escorts are required is to be addressed in the MSP. For further information regarding escorting, refer to the DSPF Principle 81 – *Escorting Security Protected or Classified Assets*.

Despatching and Receipting

6. Despatching and receipting of security-protected assets is to be in accordance with requirements within the Electronic Supply Chain Manual. For assets assigned a BIL of 3 (High) and above (classification of 'PROTECTED' and above), a signature (including the signatory's printed name and date of signature) is to be obtained on despatch and receipt. At every point where such assets are transferred, a receipt is to be provided by the gaining entity. Whatever receipting method is used, both issuing and gaining entities are to adhere to any applicable 'follow-on' actions described in the receipt.

Airport Screening

7. Assets being transported by air are generally screened for drugs, explosives and other prohibited and dangerous items. Some issuing entities may seek an exemption from screening due to the effect of screening on the nature of the asset. Issuing entities are to seek DS&VS approval for an airport screening exemption if they believe their asset falls into this category.

Transfer of Security Protected Assets by General Freight

8. BIL of 1 (Low) and 2 (Low-Medium): Security Protected Assets assigned a BIL of 1 (Low) and 2 (Low-Medium) may be transported by general freight if the requirements of paragraphs 3 and 6 above, have been satisfied.

9. It is recommended that a risk assessment determine whether there is a need for any additional security measures during transfer by general freight, such as but not limited to the use of:

- a. locks or security banding; and
- b. using SCEC-endorsed couriers instead.

10. BIL of 3 (High) and above: Security Protected Assets assigned a BIL of 3 (High) and above are to meet the following minimum requirements for transfer:

- a. by road: Assets are to be transported in a locked vehicle, or a secured container. If transport in a locked vehicle or container is not possible, sheeting or casing sealed with wire and SCEC-approved security seals are to be used;
- b. by rail: Assets are to be transported in a locked van. Assets with a BIL of 5 (Catastrophic) (classification of TOP SECRET) are to be dispatched in a separate locked and sealed van;
- c. by air: Assets are to be sent by either service aircraft or by SCEC-endorsed courier. Assets with a BIL of 5 (Catastrophic) (classification TOP SECRET) are to be dispatched by SAFEHAND in either a service aircraft or by SCEC-endorsed courier; and
- d. by sea: Assets are to be labelled 'LOCKUP STOWAGE' and carried in an appropriate locked and secured area/sealed container when transported by RAN or civilian ships.

11. Locking requirements: If the locking up of assets in vehicles or containers has been specified in paragraph 10, it is recommended that:

- a. commercial padlocks be used for assets with a BIL of 3 (High); and
- b. SCEC-approved padlocks be used for assets with a BIL of 4 (Extreme) and 5 (Catastrophic).

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Transport of Bulk Assets
Annex Version	3
Annex Publication date	10 August 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Physical Transfer of Information and Assets
DSPF Number	Control 71.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	10 August 2020	AS SPS	BIL review for PSPF classification changes.



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Physical Transfer of Information and Assets – Developing a Movement Security Plan

Developing a Movement Security Plan (MSP)

1. A MSP is used to document the risks and mitigation strategies involved in the movement of classified information or assets, including weapons or explosive ordnance. All movements are to be planned so they are effected as quickly as possible and the information and assets are protected from unauthorised access. Except for operational movements, planning is to allow six working days' notice for Defence preparation.

Note: *There is no set template or format for a MSP.*

2. A single MSP can be used to cover periodic movement of the consignment between the same parties at fixed departure and destination points. The route, time of departure and halting places are generally varied for each consignment.

Example: *It is not necessary to develop a MSP for each occurrence of a regular movement such as transporting weapons and explosive ordnance to a live-fire range.*

3. The MSP outlines the proposed security measures for the journey. It is recommended that the following details be included in an MSP:

- a. name of the issuing entity;
- b. name, address and phone contacts of the gaining entity;
- c. consignment details, including:
 - (1) description of the information or assets, including their security classification;
 - (2) unusual features requiring special handling or storage;
 - (3) measurements and weights;
 - (4) supervision of loading and unloading;

- (5) method of transmission of equipment keys; and
 - (6) arrangements for Customs inspection and sealing, if appropriate.
 - d. movement details, including:
 - (1) approximate dates;
 - (2) proposed method including details of the route, en route storage details and name of carrier, as appropriate;
 - (3) contingency plans (including a detailed response/recovery plan) in the event of a breakdown, accident, diversion or delay;
 - (4) actions taken or plans for addressing the risks identified in the risk assessment; and
 - (5) details of security guards or escorts; and
 - e. A clear outline of the steps to be taken when confronted with an unforeseen circumstance e.g. vehicle breakdown, an attack on the items being transported. This outline should include:
 - (1) possible risks, including likelihood; and
 - (2) mitigations including the steps to be taken to address the risks (e.g. setting up a piquet to protect weapons or ammunition, Commander to call the police, etc).
4. It is recommended that, during the drafting of an MSP, personnel should review current Defence Security and Vetting Service (DS&VS) threat advice that may affect the security of the freight, especially when SAFEBASE levels have been raised.
5. All MSPs for classified information or assets to be transported overseas are to be submitted to DS&VS for checking against the provisions of any Security of Information Agreements or Arrangements.
6. MSPs are to be approved by the relevant Commander or Manager responsible for the transport of the asset(s). Once approved, issuing entities are to provide a copy of the MSP to the relevant DS&VS regional office or Executive Security Adviser (ESA) for their awareness.

Notice of Movement

7. Once an MSP has been approved, the issuing entity is to prepare and send a Notice of Movement to the gaining entity so that they can prepare to receive the information or assets. The Notice of Movement will generally include the:

- a. equipment description and its security classification;
- b. security arrangements affecting the gaining entity (which may need to make special arrangement for the security of the equipment after receipt);
- c. methods of transportation;
- d. date and time of departure of the consignment;
- e. location at which the information or assets, and responsibility for it, will be handed over; and
- f. estimated date and time of arrival of the consignment.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Developing a Movement Security Plan
Annex Version	3
Annex Publication date	10 August 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Transfer of Information and Assets
DSPF Number	Control 71.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	10 August 2020	AS SPS	Further PSPF protective marking update; add hyperlinks



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Physical Security

General Principle

1. Defence facilities, people, official information, and security protected assets are protected from unauthorised access, sabotage, wilful damage, theft or disruption through a safe and secure physical environment.

Rationale

2. Application of physical security measures consistent with whole of Government requirements will:
- a. ensure a secure physical environment for storage and handling of official resources;
 - b. facilitate sharing of information and assets across Government, with allies and persons engaged under contract; and
 - c. maintain a safe and secure working environment for Defence personnel and persons engaged under contract.

Expected Outcomes

3. Appropriate security measures for the protection of resources and people are implemented, and underpinned by a high level of security awareness.
4. Security standards are applied and maintained consistently across the Defence enterprise at a level never lower than whole of Government ([Protective Security Policy Framework](#) (PSPF)) requirements.
5. The physical security environment is based on a thorough security risk review incorporating threat and risk assessments.
6. Implemented physical security controls do not breach relevant employer occupational health and safety obligations.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Threat and Assurance (AS STA)
High	Defence Security Committee (DSC) – through AS STA
Extreme	DSC – through AS STA

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: Chief of Joint Operations (CJOPS) or an authorised delegate can accept Significant to Extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.

Document administration

Identification

DSPF Principle	Physical Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 72
Version	3
Publication date	22 September 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 72.1
Control Owner	Assistant Secretary Security Threat and Assurance (AS STA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Role of accountable authority; Security planning; Security governance for international sharing; Entity physical resources; and Entity facilities.
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Information Systems (Physical) Security Working Offsite Physical Transfer Information and Assets Physical Security Certification and Accreditation Access Control
Implementation Notes, Resources and Tools	Australian Government, Physical security management protocol Australian Government, Security zones and risk mitigation control measures guidelines Australian Government, Business Impact Levels guidelines

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	22 September 2020	FAS S&VS	Control Owner transferred to AS STA on 31 August 2020



Defence Security Principles Framework (DSPF)

Physical Security

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The ASSTA has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Threat and Assurance (ASSTA)
High	Defence Security Committee (DSC) – through ASSTA
Extreme	DSC – through ASSTA

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.

Controls

General

3. The PSPF sets out minimum physical security controls required for protecting security-protected assets (refer to Key Definitions.) These controls provide a level of assurance that information originators and asset owners need to be confident that the information and assets they share with others will be protected in the same way and to the same level.
4. PSPF policy and guidance is at:
 - a. [Australian Government physical security management protocol](#);
 - b. Defence Security Toolkit -ASIO Technical Note 1/15 (Zones 2 -4);
 - c. Defence Security Toolkit -ASIO Technical Note 5/12 (Zone 5);
 - d. [Australian Government physical security management guidelines](#);
 - e. [Security zones and risk mitigation control measures guidelines](#);
 - f. [Physical security of ICT equipment, systems and facilities guidelines](#);
 - g. [Working away from the office guidelines](#); and
 - h. [Business impact levels guidelines](#).

Information Originators and Asset Owners

5. Originators of information and asset owners are to determine the appropriate Business Impact Level (BIL) to be applied to the confidentiality, integrity and/or availability for the information or asset. This process is to be in accordance with Business impact levels, refer to Protective Security Policy Framework (PSPF) [Physical security for entity resources](#), *Table 1 Business Impact Levels – compromise, loss or damage of physical assets*.
6. Where a BIL is assigned to the confidentiality of official information or an asset, a security classification is to be applied. Refer to DSPF Principle 10 – *Assessing and Protecting Official Information*.

Information and Asset Custodians

7. Information and asset custodians are responsible for securing security-protected assets in a manner that is compliant with the PSPF and appropriate for the BIL assigned by the information originator or asset owner.

Determining Physical Security Risk Mitigation Measures

8. Commanders and Managers, who are information and asset custodians, are to determine the most suitable Security Zone for the protection of security protected assets based on the classification or business impact level of the asset(s) (refer to Identification of Security Zones in this DSPF Control. Additional factors to consider when determining the required level of Security Zone include:

- a. specific requirements determined by the information originator / asset owner in accordance with any Defence Instruction or publication specifically related to the information or asset(s);
- b. the location of the information or assets within a base or facility;
- c. increased threats to Defence, a site or facility;
- d. the structure and location of an existing building or site; and
- e. additional physical protection systems (e.g. CCTV, access control systems, and alarms).

9. Where Commanders and Managers believe there is a need for physical security controls that exceed the minimum standard, this needs to be substantiated through a formal security risk management plan. This may include the need to store and handle the asset(s) in a higher Security Zone, or to apply stronger individual controls within the same Security Zone.

Note: It is recommended that information and asset custodians involve other relevant Commanders and Managers during the risk assessment process, such as the Base Support Manager (BSM). It may become apparent during the process that requested physical controls may already have been considered as part of Estate management, not be provided or be inappropriate given other controls already established on the base or facility. Mitigation measures may involve a physical re-location of an asset or unit within a base or facility to a more appropriate Security Zone.

10. Security Construction and Equipment Committee (SCEC)-approved security containers can be used to provide additional physical security controls. They are designed for storage of classified information/assets. They are not suitable for the storage of high risk unclassified assets. Due to their design these containers provide a high level of tamper evidence of covert attack and significant delay from surreptitious attack, but limited protection from forcible attack. For further information on selecting the appropriate security container refer to Table 1 in Annex A of DSPF Control 72 – *Physical Security*.

11. It is recommended that classified information be stored separately from other security-protected assets. This will:

- a. lower the likelihood of compromise of information if assets are stolen; and
- b. assist investigators to determine the reason for any incidents involving unauthorised access.

- c. Custodians with large quantities of security protected assets may use a Secure Room, strongroom or vault (including SCEC approved Instavaults), instead of containers to protect the information or assets. Secure Rooms are constructed to protect classified information from covert attack. Secure Rooms are constructed as Class A, Class B or Class C Secure Rooms, in accordance with ASIO Technical Notes 7/06, 8/06 and 9/06 respectively.

Note: Units are to seek advice from the Defence Security & Vetting Service (DS&VS) or the Executive Security Adviser (ESA) of the relevant Service before installing a commercial vault or strong room for the protection of security-protected assets.

12. Access to security-protected assets is to be based on a legitimate need to know, an appropriate security clearance and sanctioned by a policy, duty statement or directive. Where required, access is to be controlled to Defence bases, facilities, and security-protected assets.
13. Access control can be achieved through a mixture of physical security measures including, but not limited to -building construction techniques, security containers, perimeter, pedestrian and vehicle barriers, access control systems, locks and keying, and guards. All of these things are further defined using the Zone methodology described within the PSPF.
14. For further information on application of access control refer to the DSPF Principles for:
- a. Access Control;
 - b. *Assessing and Protecting Official Information*; and
 - c. *Personnel Security Clearance*.

Security Zones

15. Security Zones describe areas on a site that process, handle and store security-protected assets. They are designed to protect security-protected assets of a specific BIL.
16. The primary outcome of the Security Zone methodology is to establish scalable levels of protection from unauthorised or covert access to, and/or forcible attack on security-protected assets, depending on the business needs of the asset owner/custodian.

Identification of Security Zones

17. Facility owners, in consultation with system owners, asset custodians and other relevant stakeholders (such as Senior Australian Defence Force Officers (SADFO) and Heads of Resident Units (HRU)), are to identify those areas on a base or within a facility that process, handle and store security-protected assets and categorise those areas according to the Security Zone methodology described within PSPF guidelines (refer to [Physical Security for entity resources](#), Security zones).

18. The identification of areas as Security Zones is used for the purposes of base or site planning and differs from the certification and accreditation process. Where required, assistance may be sought from DS&VS or relevant ESA.

19. Once Zones have been identified and categorised, facility owners must seek certification and accreditation of those Zones by the appropriate authorities in accordance with DSPF Principle 73 – *Physical Security Certification and Accreditation*.

20. In an area of operations, it is recommended that the relevant Task Force Commander appoint an individual to identify and categorise those areas that process, handle and store security-protected assets.

21. Areas within a site that are not used to process, handle or store security-protected assets are not required to be categorised.

22. Security Zones are to be categorised according to:

- a. the level of access to people, information and assets provided by the security controls; and
- b. the minimum physical security controls used to treat identified risks in accordance with [Physical security for entity resources](#), Table 3 *Physical protections for security zones—level of assurance required for sharing of sensitive and security classified information*.

Example: The security of a facility is related to its design and level of access control. A facility that is constructed to a Zone Four standard, yet provides unfettered access to the public is not a Zone Four, it remains a Zone One area.

Portable Electronic Devices Prohibited Zone

23. Portable Electronic Devices (PEDs) are portable devices that can capture, process, store, record or communicate information electronically. Most PEDs are capable of internet connection via Wi-Fi or cellular data, and also contain media, which may be removable or fixed within the device (see ISM section 'Media Usage'.) Examples of PEDs, official or privately owned, that may be found within Defence include but are not limited to:

- a. laptops, tablets, eReaders, mobile phones, cameras, audio players/recorders;
- b. data transfer and format converters, that transfer information between peripherals without the use of an intervening computer, such as portable Wi-Fi hotspots, one touch backup drives, Serial Advanced Technology Attachment (SATA) hard disk to Universal Serial Bus (USB) converters. USB host transfer devices and wireless speakers; and

- c. cordless telephones such as Digital Electronic Cordless Telecommunications (DECT) phones, two way radios, and other wireless protocols including WiFi and Bluetooth.

24. Technological convergence has led to most devices incorporating the options of telephony, internet or other data connectivity. Whilst convenient, the security aspects of all functions, including the potential for covert access to microphones, cameras or media within a device will require consideration.

25. TOP SECRET areas **must** be designated as PED-prohibited areas ([ISM control 0346](#)).

26. SECRET areas **should** be designated as PED-prohibited areas ([ISM control 1169](#)).

27. Commanders and Managers may designate any area to be a PED-prohibited area if they determine the requirement through a risk assessment. The risk assessment should determine the types of PEDs and removable media that are to be prohibited in that area, taking into consideration secure areas and limited access areas, as well as areas that process and store private information.

***Example:** Mobile phones and cameras may be prohibited from a specific location such as an aircraft hangar.*

***Example:** Equipment capable of recording sound may be prohibited from an area where private counselling is held due to the risk of unintentionally recording private conversations.*

28. PED-prohibited areas are to be clearly sign posted. These signs are to:

- a. draw attention to the types of devices that are prohibited from the area; and
- b. advise the action that may be taken if unapproved devices are found.

29. Rooms or zones used for regular classified conversations, meetings, briefings, presentations etc. are to be certified and accredited for that purpose (refer to DSPF Principle 14 – *Audio-visual Security*.)

Facility Design and Development (including Greenfield Sites)

30. Project Managers responsible for developing construction security requirements in new facilities and retrofitting of existing facilities are to, in the early stages of planning, obtain security advice from DS&VS or the relevant ESA. Greenfield sites for new projects identified to process, handle and store security-protected assets are to be categorised and accredited using the Security Zone methodology described above.

Control Requirements

31. [Physical security for entity resources](#), Table 3 *Physical protections for security zones*, provides a combination of a performance-based and prescriptive specification which, when applied, will permit certification of the nominated facilities by the relevant accrediting authority.

32. The risk mitigation control requirements, which are outlined in [PSPF](#) policy: [Physical security for entity resources](#) and ASIO Technical Note 1-15 are the minimum prescriptions; they may not encapsulate all types of protection required for people and security-protected assets. Where bases or facilities face increased threats, for example terrorism, foreign interference, politically motivated violence, criminal activity etc., a risk assessment is to be conducted to determine additional prescriptions above the minimum for any zone.

Security Clearance Requirements for Access to Security Zones

33. Personnel security clearance requirements for each Zone differ and ultimately are dependent on the classification of any information or asset stored and handled within the Zone. A summary of PSPF security clearance requirements by Zone follows:

- a. Zones One and Two -determined by security risk assessment;
- b. Zone Three -if security classified official information or assets are held, all employees with ongoing access are to hold a security clearance at the highest level of the information/asset **they access in the Zone**; and
- c. Zones Four and Five -if security classified official information or assets are held, all employees with ongoing access are to hold a security clearance at the highest level of the information or asset **held in the Zone**.

Exception: Zones Three to Five -visitors do not require a specific security clearance as they will be escorted at all times within these Zones.

Alternate Storage Arrangements for Security Protected Assets

34. Where it is impractical to apply the controls as described in the guidelines, for security-protected assets, (i.e. the shape and size of the asset precludes it from being housed in a building) alternate measures are to be applied that:

- a. provide the equivalent level of protection to the requirement being varied;
- b. address any specific risk identified in a security risk assessment; and
- c. meet the business needs of the asset owner/custodian.

35. Where an asset is classified, it is to be stored in the same way as information of the same classification, refer to *PSPF policy: Physical security for entity resources*, above. Where it is operationally prohibitive or impractical to do so due to the nature of the asset and physical limitations of security containers, classified assets are to be stored in a secure facility that provides an equivalent level of protection afforded to information of the same classification. DS&VS or the relevant ESA can be contacted for advice.

36. Where it is impractical altogether to store classified assets in a secure facility, they are to be protected from unauthorised surveillance and theft. DS&VS or relevant ESA can be contacted for advice. Advice is heavily dependent on the asset and will involve measures to prevent:

- a. access by unauthorised persons;
- b. surveillance that could reveal classified information about the asset's characteristics or capabilities; or
- c. interception of any classified electronic emanations.

37. To prevent unauthorised surveillance of a classified asset it should:

- a. be covered in such a way that the shape of the item is disguised and, if possible, be out of sight from any public area; and
- b. be protected against an advanced technical intelligence attack by sophisticated surveillance equipment which could include, but is not limited to; optical, acoustic, seismic, magnetic, radar, image intensification, thermal imaging equipment or satellites.

38. If there is a risk of interception of non-communication electronic emanations from a classified asset, such as radars in weapons or surveillance systems, TEMPEST advice is to be obtained from the Australian Signals Directorate.

Storage of High-Risk Unclassified Assets

39. It is recommended that high-risk official assets be stored, where practical, in commercial safes and vaults designed to give a level of protection against forced entry commensurate with the BIL of the asset. Table 2 in Annex A to this DSPF Control, is to be used as a guide to selecting commercial safes and vaults for storing assets.

40. Alternate measures should be used that give the same level of intrusion resistance and delay for assets that cannot be secured in safes or vaults, such as large items or when it is operationally prohibitive (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this DSPF Principle.) It is recommended that personnel consult with a suitably qualified locksmith or vault manufacturer to determine the appropriate safe or vault for their needs.

41. Where it is impractical altogether to store high-risk official assets in a secure facility, they should be protected from unauthorised surveillance and theft. DS&VS or the relevant ESA can be contacted for advice.

Guarding and Patrol Requirements

42. Guards provide deterrence against loss of security-protected assets and can provide a rapid response to security incidents. Guards and patrols may be used separately or in conjunction with other security measures. The requirement for guards, their duties and the need for, and frequency of, patrols should be based on the level of threat and any other security systems or equipment that are already in place. This section is to be read in conjunction with DSPF Principle 75 – *Contracted Security Guards*.

Out-of-Hours Guarding

43. Out-of-hours guarding or patrols may be used instead of alarm systems in Zones Two to Three. These guards may be permanently on site or visit facilities as part of regular mobile patrolling arrangements. There is no requirement for guards to be used in a Zone One, unless a security risk assessment dictates otherwise.

44. Out-of-hours guarding or patrols may be used to supplement a SCEC-approved Type 1(A) SAS in Zones Four and Five, however they are not to be used as a permanent substitute/replacement for the alarm system itself.

Note: A SCEC-approved Type 1(A) alarm system is a mandated requirement for the certification of Zone Four/Five areas. Guards may be used as a temporary 'stop-gap' measure if the alarm system is non-operational.

45. Guards should hold security clearances at the highest level of information to which they may reasonably be expected to have incidental contact; refer to DSPF Principle 75 – *Contracted Security Guards* for further details.

Out-of-Hours Patrolling

46. Surveillance is to include after-hours inspection by mobile patrols. Mobile patrols that are used instead of an alarm system, where practical are to check all security cabinets, containers, assets and access points as part of their patrols. If it is impractical to physically check all these items, then the facility itself housing the items is to be physically inspected.

47. If security-protected assets are wholly protected by an operating security alarm system, then patrols of these items should be undertaken at intervals not exceeding 24 hours.

Note: This would generally be the case for Zones Four and Five, which by their nature, would be wholly protected by an operating security alarm system.

48. If security-protected assets are not wholly protected by an operating security alarm system, then patrols of these items should be undertaken at random intervals not exceeding:

- a. four hours for Zone Three, and
- b. based on a security risk assessment for all other Zones.

Note: BILs should determine the frequency of patrols during the risk assessment process. Assets with higher BIL may require shorter patrol time intervals than assets with lower BIL.

Security Zones in Areas of Operations

49. The fundamental principles of the Security Zone methodology apply equally to areas of operations. What may differ between operational and domestic Security Zones is the ability to rigidly apply security controls described within the guidelines. 'Defence in depth' and 'force protection' measures applied to an area of operations, may replace the relevant security control described in the guidelines if:

- a. it is operationally prohibitive or impractical to apply PSPF prescribed controls (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this DSPF Principle); and
- b. the control measures applied provide an equivalent level of protection to the security control being varied.

50. This can be considered part of the normal physical security variation process. Variations in areas of operations are to be approved by the relevant Task Force Commander.

Example: It is impractical to store an asset classified at SECRET in a Zone Three area in accordance with PSPF requirements (constructed to AS3555.1-2003 and surveilled by an AS 2201 Class 5 alarm system.) A variation may be approved to store and handle the asset in a tented area surrounded by barbed wire and permanently guarded by armed personnel, with back up able to attend in less than five minutes, as long as the fundamental access control principle of 'limited Defence personnel and contractor access with escorted visitors only' is applied.

Australian Defence Force Platforms

51. Australian Defence Force (ADF) platforms, due to varying designs, may not conform to the technical specifications described in the PSPF [Physical security for entity resources](#) guidelines and ASIO Tech Notes. Asset owners are to apply the variation methodology described within ASIO Technical Note 1-15.

Specific Handling Requirements for Security-Protected Assets

52. **Physical Transfer.** Security-protected assets are to be transported in accordance with DSPF Principle 71 – *Physical Transfer of Information and Assets*.

53. **Accounting.** Security-protected assets are to be accounted for in accordance with the requirements detailed in the Defence Logistics Manual (DEFLOGMAN) Part 2 Volume 5 Chapter 18 Data Quality Management Policy.

54. **Disposal.** Classified assets are to be disposed of in accordance with DSPF Principle 10 – Assessing and Protecting Official Information. High risk official assets are to be disposed of in accordance with the requirements of DEFLOGMAN Part 2 Volume 5 Chapter 10 Defence Disposal Policy and any Defence instructions specifically related to the asset.

55. **Loss.** The loss of a security-protected asset is a security incident and is to be reported and investigated in accordance with DSPF Principle 77 – *Security Incidents and Investigations* and CEI 6.3 Loss and Recovery of Public Property.

Note: Early reporting in accordance with DSPF Principle 77 – Security Incidents and Investigations may prevent further compromise and minimise the extent of damage arising from the security incident.

56. **Special Access Programs.** Additional requirements for the handling of security-protected assets relating to the Defence Special Access Program are detailed in DI(G) Admin 62-1 Defence Special Access Programs -Policy and Management.

Roles and Responsibilities

Project Managers

57. Project Managers, who are responsible for construction or refurbishment projects, are responsible for compliance with this DSPF part and the source material it references. For further information regarding project security, refer to DSPF Principle 11 – *Security for Projects*.

Facility Owners

58. Facility owners, including Base Support Managers (BSM), relevant Unit Commanders and Managers, and DISP member facility owners, are responsible for:

- a. the identification and categorisation of Security Zones for which they are responsible;
- b. base, facility or site planning;
- c. controlling access to bases and facilities through the use of appropriate physical security controls;
- d. identifying the need and commencing the processes for certification and accreditation; and

- e. ensuring that faculties meet the standards required for certification and accreditation and are maintained throughout the life of the accreditation period.

Note: *If the facility owner is a DISP member, that DISP member is responsible for these activities, however, risk ownership remains with the sponsoring Defence Service or Group.*

Asset Custodians

59. Asset custodians are responsible for:
- a. factoring the management of security-protected assets for which they are the custodian into their security risk management and planning, refer to the DSPF Governance and Executive Guidance;
 - b. the physical security procedures within the areas under their control;
 - c. ensuring that aggregated security-protected assets in their custody are appropriately protected in accordance with this DSPF part; and
 - d. ensuring that employees or persons engaged under contract working with aggregated security-protected assets are aware of, and comply with the requirements for protecting the asset as detailed in this DSPF Principle.

DISP Members

60. DISP members are responsible for maintaining accreditation of their facilities, including meeting the necessary physical security standards. Defence sponsors retain the security risk associated with outsourced activities and are to monitor DISP contractor processes to ensure physical security standards are maintained. For further information refer to DSPF Principle 16 – *Defence Industry Security Program*.

Contract Managers

61. Contract Managers are responsible for:
- a. the acceptance of physical security risks arising from the storage of official information and security-protected assets at persons engaged under contract facilities; and
 - b. ensuring that Defence assets are protected in accordance with this DSPF part when those assets are in the possession of persons engaged under contract.

Key Definitions

62. **Asset custodian.** The Commander or Manager responsible for the protection of asset(s) (including security-protected assets) upon issue to them by the asset owner.

63. **Asset owner.** The Group Head or Service Chief with responsibility and accountability for an asset for which responsibility has been assigned to them.
64. **Business Impact Level (BIL).** A standardised rating that forms part of a security risk management process and identifies the level of impact on Defence and the National Interest resulting from a compromise of confidentiality, loss of integrity or unavailability of individual or aggregated information and assets. Refer to the Australian Government physical security management guidelines, [Physical security for entity resources](#), *Table 1 Business Impact Levels—compromise, loss or damage of physical asset for further information*.
65. **Facility owner.** The person responsible for the operation of a facility.
66. **Official Information.** Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and persons engaged under contract, that includes:
- a. documents and papers;
 - b. data;
 - c. 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.
67. **Security Construction and Equipment Committee (SCEC).** A standing inter-departmental committee which reports to the Protective Security Policy Committee (PSPC). The SCEC is responsible for the evaluation of security equipment for use by Australian Government agencies, and for promulgating the Security Equipment Evaluated Products List ([SEEPL](#)).
68. **Security-protected asset.** A non-financial, reportable or accountable asset that requires greater than standard fire and theft protection due to either:
- a. being allocated a BIL of 2 (Low to Medium) or higher;
 - b. an unacceptable business impact that would result from the unauthorised modification (i.e. loss of integrity) of the asset, irrespective of whether that modification can be detected or not;
 - c. an unacceptable business impact that would result from the asset being unavailable (i.e. loss of availability) for a given period of time; or
 - d. being categorised as a weapon or explosive ordnance.

69. **Security Zones.** A methodology for physical security mitigation based on a security risk assessment. It is a multi-layered system in which physical security measures combine to provide security-in-depth to those areas on a site that protect assets which require more than normal fire and theft protection.

70. **Technical authority for physical security.** The arbiter for guidance, advice and decision making for technical matters relating to physical security specifications and standards required to achieve certification and accreditation.

71. **TOP SECRET area.** An area certified as a security zone (Zone 4 or 5) approved for handling and storing top secret material.

72. **Variation.** An approved alternate, substitute or risk-mitigated design that meets the intent of physical security standards or specifications.

***Note:** Physical security variations apply specifically to standards or specifications described in either ASIO Technical Notes or Defence-specific technical guidance presented in this DSPF part. They are used when it is impractical to meet the prescribed standard or specification.*

73. **Greenfield.** In the physical security context, a Greenfield site is a property that has not undergone an Australian Government security treatment.

Further Definitions

74. Further definitions for common PSPF terms can be found in the [Glossary](#).

75. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A — *Security Containers, Vaults and Safes*

Annex B — *Policy Transition from Security Rated Areas to Security Zones*

Document administration

Identification

DSPF Control	Physical Security
Control Owner	Assistant Secretary Security Threat and Assurance (ASSTA)
DSPF Number	Control 72.1
Version	3
Publication date	22 September 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Security
Related DSPF Control(s)	N/A

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	22 September 2020	AS SPS	Control Owner transferred to AS STA on 31 August 2020



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Physical Security – Security Containers, Vaults, and Safes

Security Containers for Official Information

1. Information originators are to determine the appropriate Business Impact Level (BIL) for official information in accordance with [Business Impact Levels guidelines](#).
2. The [core requirements for physical security](#) provide Whole of Australian Government guidelines on the physical controls required to protect assets (including information).
 - a. In accordance with the [Protective Security Policy Framework](#) (PSPF), Defence is required to select the minimum level of security containers or secure zones for storing official information where the compromise, loss of integrity or unavailability of the information has a business impact level. Table 1 should be used when selecting the minimum level of security containers or security zones. Information with an Information Management Marker (IMM) will have specific handling requirements detailed in a footer or cover page to the document. If these handling requirements exceed the requirements of this table, the higher requirement is to be applied.
 - b. Secured from unauthorised access means the information can be stored in containers other than a specified security container, for example -a desk drawer or cabinet. The information is to be stored discreetly and secured from casual access.
 - c. In exceptional circumstances to meet an operational requirement—for example, where TOP SECRET information cannot be returned to a Zone Five area—personnel may store TOP SECRET information for a period not to exceed five days in a Zone Three or Four area. Advice from ASIO-T4 should be sought before implementing arrangements for the temporary storage of TOP SECRET information outside a Zone Five area.

Table 1: Security Containers for Official Information

Classification / Business Impact Level	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
OFFICIAL Information the compromise, loss of integrity or unavailability of which would have a BIL of 1 (Low).	Locked commercial container	Secured from unauthorised access (see note b)	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 2 (Low to Medium). Or limited holdings of information with an OFFICIAL: Sensitive Information Management Marker (IMM) (see note a)	Security Construction and Equipment Committee (SCEC) Class C	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 2 (High). Or limited holdings of PROTECTED information	Ongoing storage not recommended, if unavoidable SCEC Class C	SCEC Class C	SCEC Class C	Container to be determined by a security risk assessment	Container to be determined by a security risk assessment

Classification / Business Impact Level	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 4 (Extreme). Or limited holdings of SECRET information	Not permitted	Not permitted (See note below for policy transition details)	SCEC Class B	SCEC Class C	SCEC Class C
TOP SECRET classified information the compromise, loss of integrity or unavailability of which would have a BIL of 5 (Catastrophic)	Not permitted	Not permitted	Not normally permitted. (In exceptional circumstances SCEC Class A) see 2.c. above	Not normally permitted. (In exceptional circumstances SCEC Class B) see 2.c. above	SCEC Class B

Note: Security classified material at the SECRET level currently stored in a Class A container within a Zone 2 must be relocated to a minimum Zone 3 by 1 August 2022.

Safes and Vaults for Protection of High Risk Official Assets

3. It is recommended that security-protected assets be stored, where practical, in commercial safes and vaults designed to give a level of protection against forced entry commensurate with the business impact level of the asset. In accordance with the PSPF, Defence is required to select the minimum level of security containers or security rooms for storing official information where the compromise, loss of integrity or unavailability of the information has a business impact level. Table 2 is to be used as a guide to selecting commercial safes and vaults for storing assets.

Note: For the purposes of transition, Table 2 references the former asset categories together with the business impact levels for high risk unclassified assets.

Table 2: Selecting Safes or Vaults to Protect High Risk Official Assets (GUIDANCE ONLY)

High risk unclassified assets / categorised assets	Zone One	Zone Two	Zone Three	Zone Four
High risk official assets the loss of which would have a BIL of 1 (Low) or SUPPORT assets	Locked commercial container	Locked commercial container	Determined by a security risk assessment	Determined by a security risk assessment
High risk official assets the loss of which would have a BIL of 2 (Low-Medium) or SENSITIVE and ATTRACTIVE assets	Commercial safe or vault	Determined by a security risk assessment	Determined by a security risk assessment	Determined by a security risk assessment
High risk official assets the loss of which would have a BIL of 3 (High) or IMPORTANT assets	Commercial safe or vault	Commercial safe or vault	Commercial safe or vault	Determined by a security risk assessment
High risk official assets the loss of which would have a BIL of 4 (Extreme) or MAJOR assets	AS 3809 high security safe or vault	AS 3809 medium security safe or vault	AS 3809 commercial safe or vault	Commercial safe or vault
High risk official assets the loss of which would have a BIL of 5 (Catastrophic)	Should not be held unless unavoidable	Should not be held unless unavoidable	AS 3809 high or very high security safe or vault	AS 3809 medium or high security safe or vault

Use of Security Containers

4. Commanders and managers must maintain a register of all security containers, combinations and keys. Each container must have a custodian who is responsible for its contents and controlling access to the container. Table 3 outlines the processes for the use of security containers.

Table 3: Use of Security Containers

Aspect	Procedure
Unlocked containers	When unlocked, the door is to be kept open, bolt returned to the locked position, and the key is to be removed, if applicable.
Closed doors or drawers	Are to be locked when the doors or drawers are closed.
Access to locks	Must be sealed on installation and after repair, so that access to the back of the lock is not possible.
Combination locks	Must not be opened in view of people who are not authorised to know the combination.
Labels	Are not to be placed near locks, bolts or hinges to ensure that signs of tampering or unauthorised entry are visible. Labels are not to give any indication of the contents of the container. 'Open/closed' labels are not to be used.
Keys	The security officer will: a. hold all duplicate keys when the container (including Class C rooms) is locked; and b. maintain a key register.

Movement

5. Prior to relocating a security container, the security officer must be advised. When relocating a security container, a risk assessment will determine if the container is to be completely emptied of all documents and if any labels attached to the inside are to be removed.
6. The locking pins **must** be reinserted if it is a Class A container.

Disposal

7. Before a container is returned to the store, it must be completely emptied of all documents and have a signed certificate attached to its body stating that it has been emptied and checked. The process is to include removing and replacing drawers to ensure that no classified items have been concealed behind or below drawers.
8. The key register **must** be updated to reflect the change. Additionally:
 - a. for a keyed lock container, keys will be removed and sent to the store separately with details of their container; or
 - b. for a combination lock container:
 - (1) the lock **must** be reset to the manufacturer's standard setting (usually 40-50-60 or as shown in the instruction book); and
 - (2) the combination **must** be marked on the outside of the container.

Note: Disposal must be conducted via a Defence approved disposal authority

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Security Containers, Vaults and Safes
Annex Version	4
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Security
DSPF Number	Control 72.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	6 July 2020	AS SPS	Table 1 Security Containers for Official Information in Zone 2 aligned with PSPF.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	18 September 2020	AS SPS	Transition policy for storage of SECRET information



Defence Security Principles Framework (DSPF)

Annex B to Physical Security – Policy Transition from Security Rated Areas to Physical Security Zones

Transition from Security Rated Areas to Physical Security Zones

1. The PSPF has amended the physical security methodology, replacing the former Security Rated Areas with Physical Security Zones. To facilitate a smooth transition between methodologies, the following policy is provided.

Existing Certification for Security Rated Areas

2. Table 1 has been developed for those areas holding a certification/accreditation certificate describing a 'Security Rated Area'; Refer DSPF Principle 73 – *Facilities Certification and Accreditation*.

3. If a certified/accredited Security Rated Area meets the requirements of Table 1 and holds a current accreditation certificate with no changes to the physical structure or supporting procedures, it may be deemed an accredited Physical Security Zone by the appropriate accreditation authority. All requests for an updated accreditation certificate must be supported by a statement that there has been no change to physical controls or an increase in threat since the original certification/accreditation was issued. If the accrediting authority agrees to the change, the accreditation certificate is to be updated to reflect the change to the Physical Security Zone methodology.

Table 1: Transitional Arrangements

If the Security Rated Area is:	And access control measures provide...	It equates to a Physical Security Zone of...
Public Access/Unsecure Area	Unfettered access to members of the public	Zone One
Accredited Intruder Resistant Area	Unrestricted Defence personnel and persons engaged under contract access; and Restricted public access	Zone Two
Accredited Partially Secure Area	Limited Defence personnel and persons engaged under contract access and escorted visitors only	Zone Three
Accredited Secure Area	Strictly controlled Defence personnel and persons engaged under contract access and escorted visitors only with an identified need to be there	Zone Four
Accredited TOP SECRET Areas	Strictly controlled Defence personnel and persons engaged under contract access and escorted visitors only with an identified need to be there	Zone Five

Interim Physical Security Zones

4. Some areas or facilities cannot be considered an official Physical Security Zone without completing a full accreditation process, refer DSPF Principle 73 – *Facilities Certification and Accreditation*. These include areas of facilities that:

- a. do not hold a current accreditation certificate;
- b. hold an accreditation certificate, but do not meet the minimum access control requirements; or

Example: The entirety of a building is considered a Secure Area, but its outer perimeter borders a public access area. During business hours, members of the public may access the foyers of the building, and there is unlimited access by Defence personnel and persons engaged under contract access to all common areas of the building (such as stairwells, elevators and open office environments.) Under the Physical Security Zone methodology, the entirety of the building can no longer be considered a Zone Four during business hours.

- c. are not current Security Rated Areas, but process, handle and store high-risk official assets.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Policy Transition from Security Rated Areas to Physical Security Zones
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Security
DSPF Number	Control 72.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Physical Security Certification and Accreditation

General principle

1. Defence conducts physical certification and accreditation processes to ensure that Defence's information, Security Protected Assets and infrastructure are protected by the necessary measures to meet identified security risks.

Rationale

2. The certification and accreditation process enables Defence to manage security risks to classified information, Security Protected Assets and infrastructure. Accreditation of facilities provides the confidence Defence Groups and Services, and other Government agencies (domestic and foreign) need in order to share information and Security Protected Assets with each other or Industry partners.

Expected outcomes

3. Certification of facilities is conducted as part of every accreditation and re-accreditation process.
4. Defence conducts certification of facilities against Defence Security Principles Framework (DSPF) and Protective Security Policy Framework (PSPF) security standards, and is consistent with Whole-of-Government direction on protective security.
5. The accreditation authority reviews the outcomes of the certification process, and confirms appropriate mitigation measures are in place. Where applicable, the accreditation authority assesses whether appropriate risk management has been undertaken by control officers to determine if the residual risk to a facility is acceptable to Defence and, if so, provide authority to operate.
6. Facilities are re-accredited at intervals specified within Control 73.1 – *Physical Security Certification and Accreditation*, and when;
 - a. changes occur to the Business Impact Levels associated with the ICT systems or assets handled or stored in the facility;

- b. significant changes to the tenancy and governance arrangements, architecture of the facility or physical security controls used at the facility occur; or
- c. requested by DS&VS or the facility owner.

7. Accreditation authorities temporarily or permanently revoke accreditation on security grounds if they believe the risk of operation to a facility is unacceptable to Defence.

Escalation Thresholds

Risk Rating	Responsibility
Low	APS 6/O-4 – Security Adviser or delegate of relevant equivalent Executive Security Adviser (ESA)
Moderate	EL 1/O-5 – DS&VS Security Manager or delegate of relevant equivalent ESA
Significant	EL 2/O-6 – Director Security Services or delegate of relevant equivalent ESA through EL 1/O-5
High	EL 2/O-6 -Director Security Services or delegate of relevant equivalent ESA
Extreme	Assistant Secretary Security Threat and Assurance (AS STA)

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: The above Escalation Thresholds are for domestic application. 'Defence in depth' and 'force protection' measures applied to an area of operations may replace relevant controls in the DSPF if:

- a. it is operationally prohibitive or impractical to apply DSPF and PSPF prescribed controls (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this Principle); and
- b. the control measures applied provide an equivalent level of protection as the security control being varied.

Document administration

Identification

DSPF Principle	Physical Security Certification and Accreditation
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 73
Version	4
Publication date	22 September 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 73.1
Control Owner	Assistant Secretary Security Threat and Assurance (AS STA)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Entity Facilities; and Entity Physical Security.
Read in conjunction with	N/A
See also DSPF Principle(s)	Personnel Security Clearance Assessing and Protecting Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Access Control
Implementation Notes, Resources and Tools	<u>Australian Government physical security management guidelines—Security zones and risk mitigation control measures</u>

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	17 July 2018	FAS S&VS	Corrected Control Owner designation
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	22 September 2020	FAS S&VS	Control Owner transferred to AS STA on 31 August 2020



Defence Security Principles Framework (DSPF)

Physical Security Certification and Accreditation

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this enterprise wide control.

Escalation Thresholds

Risk Rating	Responsibility
Low	APS 6/O-4 – Security Adviser or delegate of relevant equivalent Executive Security Adviser (ESA)
Moderate	EL 1/O-5 – DS&VS Security Manager or delegate of relevant equivalent ESA
Significant	EL 2/O-6 – Director Security Services or delegate of relevant equivalent ESA through EL 1/O-5
High	EL 2/O-6 - Director Security Services or delegate of relevant equivalent ESA
Extreme	Assistant Secretary Security Threat and Assurance (ASSTA)

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: The above Escalation Thresholds are for domestic application. 'Defence in depth' and 'force protection' measures applied to an area of operations may replace relevant controls in the DSPF if:

- a. it is operationally prohibitive or impractical to apply DSPF and PSPF prescribed controls (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this Principle); and
- b. the control measures applied provide an equivalent level of protection as the security control being varied.

Facilities Needing Accreditation

2. Defence and Defence industry facilities that **must** be accredited are:
 - a. Security Zones that process, handle or store:
 - (1) classified information PROTECTED and above;
 - (2) Security Protected Assets with a [Business Impact Level](#) (BIL) of 3 (high) and above;
 - (3) ICT systems PROTECTED or above that are not protected by Australian Signals Directorate (ASD) endorsed encryption; and
 - (4) aggregated information with a BIL of 3 (high) and above;

Note: Facilities that do not process, handle or store security-protected assets (ie. assets that do not attract a BIL and thus only require standard fire and theft protection), are not categorised as a Security Zone and therefore do not require accreditation.

Note: ICT system accreditation is undertaken separate to physical accreditation and is required for each system that operates in an accredited Security Zone. Refer to DSPF Principle 23 – ICT Certification and Accreditation.

- b. armouries and licenced explosive ordnance facilities;
 - c. facilities where technical surveillance countermeasures are implemented (eg. audio secure rooms); and
 - d. joint and allied facilities subject to relevant legislation, a General Security Agreement (GSA), a Security of Information Agreement or Arrangement (SIA) or a Memorandum of Understanding.

Note: DS&VS can confirm whether or not a GSA, a SIA or a Memorandum of Understanding is in place that would affect joint or allied facilities.

3. Defence and Defence industry facilities that store security-protected assets with BILs of low-medium, or house ICT systems operating at the OFFICIAL (including OFFICIAL: Sensitive information) level (BILs low-medium); are to be risk assessed by the Control Officer (in consultation with the relevant accreditation authority), to determine if the facility is to be subject to a physical accreditation.

Exclusion: A company that is processing OFFICIAL: Sensitive material that is solely related to the company's business dealings with Defence does not require a facility accreditation.

Physical Certification and Accreditation Authorities

4. The following facilities and security zones **must** be certified and accredited by the authorities identified in Table 1 of this Control, unless an alternative is approved by the AS STA:

Table 1: Physical Certification and Accreditation Authorities

Facility	Location	Physical certification authority	Physical accreditation authority
Domestic - Security Zones One through to Four (including deployable facilities, and off-site areas such as home-based areas)	Joint, non-Service unit or DISP members' facilities.	DS&VS(a)	DS&VS(a)
Domestic - Security Zones One through to Four (including deployable facilities, and off-site areas such as home-based areas)	Single-Service Unit	ESA(b)	ESA(b)
Domestic – Commercial Shared Data centre facilities	In Australia on industry premises	DS&VS(a)	DS&VS(a)
Domestic - Security Zone Five Not including SCI	All Defence and Defence industry/DISP members	ASIO T4(c)	DS&VS(a)
	Single-Service unit.	ASIO T4(c)	ESA(b)
Domestic – Compartments (k) within Zone Five	Joint, non-Service unit facility or DISP member's facility	DS&VS(a)	DS&VS(a)
	Single-Service unit	ESA(b)	ESA(b)
Domestic - SCI	All Defence and Defence industry/DISP members	ASIO T4(c)(i) (DS&VS to coordinate with ASIO T4(c) via submission of AE851(i))	ASD(d) to coordinate
Armoury or licensed EO facilities (refer to DSPF Principle 78 –Weapons Security, and	Joint, non-Service unit facility or DISP member's facility	DS&VS(a)	DS&VS(a)
	Single-Service unit. (not including overseas	ESA(b)	ESA(b)

Facility	Location	Physical certification authority	Physical accreditation authority
DSPF Principle 79 – Explosive Ordnance Security)	Areas of Operation)		
	Overseas in Areas of Operation	CJOPS(e)	CJOPS(e)
ADF Platforms	Once in service or during regular maintenance or major refit periods	ESA(b)(h)	ESA(b)(h)
ADF Platform – SCI	Once in service or during regular maintenance or major refit periods	ASD(d) to coordinate	ASD(d) to coordinate
Overseas - All Security Zones Not including SCI	Zones 1 to 5 and compartments in a Zone 5 – internal to an Australian Diplomatic Mission. Not in Areas of Operation	DFAT(f)	DFAT(f)
	Zones 1 to 5 and compartments in a Zone 5 - external to an Australian Diplomatic Mission. Not in Areas of Operation	The DS&VS(a) to coordinate(g) Note: DS&VS consults DFAT and local certification authorities in accordance with a SIA(j)	The DS&VS(a) to coordinate(g) Note: DS&VS consults DFAT and local accreditation authorities in accordance with a SIA(j)
	Zones 1 to 5, and compartments in a Zone 5 In Areas of Operation	CJOPS(e)	CJOPS(e)
Overseas – SCI	SCI - All Defence and Defence industry/DISP members in and external to Australian Diplomatic Missions.	DS&VS(a) to coordinate with ASD(d) and DFAT(a)	ASD(d) to coordinate
	SCI – in Areas of Operation	CJOPS(e) to coordinate with ASD(d)	ASD(d)

Notes:

- (a) Defence Security and Vetting Service.
- (b) Executive Security Authority – For Navy, Army and Air Force.
- (c) Certification activities undertaken by the Australian Security Intelligence Organisation (ASIO) T4 are conducted on a cost-recovery basis. All liaisons between ASIO T4 and Defence in relation to the certification and accreditation of Defence TOP SECRET facilities, including the management of arrangements for TSCM, are managed by the DS&VS.
- (d) Australian Signals Directorate SCIF Accreditation Team.
- (e) Chief of Joint Operations (CJOPS) or authorised Delegate.
- (f) Department of Foreign Affairs and Trade (DFAT).
- (g) On occasions, the DS&VS may delegate certification responsibility to the Chief Information Officer Group (CIOG), where CIOG is attending an overseas location to certify an ICT system.
- (h) Consideration is to be given to service or platform specific policies and applicable Operating Procedures (including emergency destruction) and any physical limitations.
- (i) AE851 – Request for T4 Certification of a Zone 5/SCIF Defence site.
- (j) SIA - Security of Information Agreement or Arrangement
- (k) Compartments are areas that require additional access control, including ICT server rooms and dedicated VTC rooms.

Process**Facility Certification****Prior to Certification**

5. Certification is to be conducted as part of every facility accreditation or reaccreditation. Facility and asset owners are required to apply the minimum security controls detailed in the DSPF (refer to DSPF Principle 72 – *Physical Security*) as determined by the BIL of the assets being protected and consideration of security risks to the asset(s). It is recommended that facility or asset owners contact the certification authority to confirm physical security requirements prior to conducting any infrastructure work. For infrastructure projects, and projects involving the construction of ADF assets and platforms, it is recommended that consultation occur during planning and design stages.

Minimum Physical Security Standards

6. Minimum physical security controls outlined in the DSPF (refer to DSPF Principle 72 – *Physical Security*) are risk-based measures aligned with the PSPF. Application of minimum security controls provides assurance across Defence and other government agencies that a consistent set of controls are applied for the protection of assets.

7. Physical certification authorities will assess the level to which a facility complies with the minimum controls identified in:
 - a. DSPF Principle 72 – *Physical Security* for all Physical Security Zones, including all standards referenced from it;
 - b. Annex C to DSPF Control 78.1 – *Weapons Security* for armoury standards; and

Note: See DSPF Control 79.1 – *Explosive Ordnance Security* for information regarding security standards for licensed explosive ordnance facilities.

- c. DSPF Control 14.1 – *Audio-visual Security* for Audio Secure Room standards, including all standards referenced from it.

If Minimum Security Controls are Met

8. If the minimum security controls are met, the certification authority will:
 - a. certify the facility as having achieved the minimum standard required; and
 - b. document the outcome of the certification in a formal report.

If Minimum Security Controls are Not Met

9. During the certification process, the facility or asset owner, or the certification authority may identify that minimum security controls have not been met or inappropriate security controls applied. In such circumstances the facility or asset owner has the option to either rectify the deficiency by applying the appropriate security control(s) or, undertake a security risk process if departing from the required standard to identify alternate controls in consultation with the certification authority. For guidance on risk management in the DSPF, refer to *DSPF Governance and Executive Guidance*.

If Additional Security Controls are Required

10. Unless specified in a Defence Instruction or International Security Agreement, the need for additional security controls above the minimum standard (refer to DSPF Principle 72 – *Physical Security*) is to be substantiated through a formal security risk management plan.

Certification Documents

11. Where applicable, the certification authority needs to receive the following documentation from facility or asset owners so certification can be provided:
 - a. Confirmation of surveillance arrangements, such as:

- (1) a Type 1A SAS commissioning certificate issued by a Security Construction and Equipment Committee (SCEC) Security Zone Consultant;
 - (2) an installation certificate for a commercial alarm system, which states compliance with Australian Standards AS/NZs2201 standard for Intruder Alarm Systems (not applicable for Zones Four or Five); or
 - (3) guarding and after-hours patrol procedures for the facility, or a combination of SAS and guard patrols.
- b. an electronic access control system certification from suitably qualified system installers or designers (required for Security Zones Three, Four and Five; required only if installed in Security Zones One or Two);
 - c. any treatment plan for controls required above the baseline requirements; and
 - d. any other documentation requested by the certification authority.

Accreditation

12. Accreditation is the process undertaken by an authority providing formal recognition that certification requirements have been met and risks adequately assessed and addressed by facility and/or asset owners. Once satisfied that risks have been appropriately addressed, the accreditation authority will issue an accreditation certificate to the facility owner permitting operation of a facility.

13. Accreditation cannot be awarded where departures from necessary security controls are outstanding or have not been approved; or if the residual risk (as determined through the security risk management process) to Defence's people, information, security-protected assets and infrastructure is considered unacceptable. Any recommendation or decision to prevent or suspend accreditation needs to be justified by the accreditation authority, recorded and communicated to the appropriate facility and asset owner(s).

Accreditation Documents

14. If applicable, the accreditation authority is to receive the following certification reports and documentation before the accreditation process can commence:
- a. a certification report stating the Security Zone rating of the facility;
 - b. confirmation that a trained and qualified security officer is appointed for the facility;
 - c. up-to-date and authorised Security Standing Orders;
 - d. confirmation that a Security Register is in place for the facility;

- e. confirmation that official information is stored in appropriate security containers within the certified Security Zone;
- f. an Acoustic Engineer's Report stating the acoustic rating of the facility;
- g. a Technical Surveillance Counter Measures certification report for the facility; and
- h. a copy of an approved Security Risk Management plan documenting that the security controls for the facility provide adequate protection against identified security risks.

Maintaining Accreditation

15. Accredited facilities are to maintain the standard to which they are accredited. Facility owners are to conduct periodic reviews and self-assessments of the accredited security measures. Annual Protective Security Self Assessments (using form [AC064](#)) provide ongoing assurance to Commanders and Managers that accreditation standards are maintained and identify any remediation where required. For DISP members, your Chief Security Officer (CSO) must complete an Annual Security Report (ASR) to meet DISP eligibility and suitability requirements.

Revoking Accreditation

16. The accreditation authority can temporarily or permanently revoke an accreditation on security grounds if the risk of operation to a facility is found to be unacceptable to Defence. If an accreditation is revoked, the accreditation authority is to document and record the basis for the decision and notify the FAS S&VS before accreditation is revoked.

17. Where accreditation is revoked or not renewed, the accreditation authority will recommend that a facility not operate until the control officer has rectified identified deficiencies or treated risks to an acceptable level. Facility Owners and / or Control Officers retain responsibility for the operation of a facility, including the management of security risks to assets for which they are accountable. In circumstances where an accreditation authority revokes or suspends accreditation, Facility Owners and /or Control Officer's will determine whether a facility will operate, and is required to advise the accreditation authority and relevant stakeholders of their decision.

Reaccreditation

18. Accreditation is not permanent. Reaccreditation of facilities is necessary to provide ongoing assurance that security measures are appropriate for the protection of assets and may be triggered by a number of circumstances including:

- a. significant changes in security policies or standards;

- b. changes to Defence's security risk profile and/or appetite;
 - c. expiry of the accreditation due to the passage of time;
 - d. changes in the BILs associated with the assets handled or stored within a facility;
 - e. significant changes to the architecture of the facility or the physical security controls used; or
 - f. a major security incident affecting the facility; and
 - g. any other conditions stipulated by the accreditation authority.
19. Accredited facilities **must** be reaccredited:
- a. When circumstances change, including:
 - (1) changes to the BILs associated with the ICT system, information or assets handled or stored within;
 - (2) significant changes to the tenancy;
 - (3) changes in governance arrangements; or
 - (4) architecture of the facility or the physical security controls used.
 - b. At regular intervals as per Table 2, below.

Table 2: Reaccreditation intervals

Facility	Reaccreditation interval
Zone Two	Ten Years
Zone Three, Four and Five	Five Years
Armouries/Licensed EO facilities	Five Years

Note: Annual Protective Security Self Assessments (using form AC064) provide ongoing assurance to Commanders, Managers and DISP member executives that accreditation standards are maintained and identify any remediation where required

Roles and Responsibilities

First Assistant Secretary Security and Vetting Service (FAS S&VS)

20. The FAS S&VS is responsible for:

- a. determining the certification standards for the physical security of Defence facilities (including the certification standards for the physical security of ICT systems in accordance with the [Information Security Manual](#) (ISM);
- b. recording the physical accreditation status of all facilities accredited by Defence accreditation authorities in accordance with this DSPF part;
- c. certification and accreditation assessment of facilities;
- d. liaising with the Defence Intelligence Security (DIS) Sensitive Compartmented Information Facility (SCIF) Accreditation Management Team regarding the management and conduct of certification and accreditation of Defence facilities requiring DIS input.

Defence Accreditation Authorities

- 21. The accreditation authority is responsible for:
 - a. accrediting facilities and systems assigned to them in accordance with this DSPF Principle;
 - b. undertaking an independent review of the certifying authority's report and other necessary documentation to determine that the associated residual security risk of a facility is accepted by facility and /or asset owners;

Note: Accreditation authorities are not obliged to accept the recommendation of a certification report, however if they choose not to do so they are responsible for documenting the basis of the decision.

- c. granting or denying accreditation for the operation of a facility;
- d. providing the appropriate risk steward(s) with an accreditation certificate stipulating their responsibilities and accreditation conditions; and
- e. recording the details of accreditations and denials.

Department of Foreign Affairs and Trade (DFAT)

- 22. DFAT is responsible for the physical certification within all Australian missions overseas.

Australian Security Intelligence Organisation (ASIO)

- 23. ASIO is responsible under whole-of-government arrangements for the physical certification of domestic TOP SECRET facilities and outsourced data centres.

Director Defence Intelligence Organisation

24. On behalf of the DDIO, the DIS SCIF Accreditation Management Team is responsible for accrediting facilities that contain some allied systems and which have a requirement to handle, store, process and discuss Sensitive Compartmented Information (SCI).

Facility and System Owners

25. The Facility or System Owner is responsible for:

a. identifying the need for certification or accreditation;

Note: DISP Sponsors will undertake this on behalf of DISP members; refer to DSPF Principle 16 - Defence Industry Security Program.

- b. the timely engagement of the relevant certification or accreditation authorities, including an indication of the assessed BILs of the asset, and providing support to the authority during the conduct of the certification or accreditation process;
- c. where required, providing a security risk management plan to the relevant certification or accreditation authority;
- d. developing the necessary supporting documentation described in this DSPF part that are required to successfully complete certification and accreditation;
- e. identifying funding arrangements, and whether any 'building' works are scheduled before certification is conducted;
- f. ensuring that facilities meet the standards required for certification or accreditation;
- g. where required, identifying the need for variations to minimum physical security standards (refer to DSPF Principle 72 - Physical Security);
- h. maintaining accreditation; and
- i. reporting changes in security risk (including, but not limited to, physical and ICT security, operations and security governance), to the appropriate risk owner, accreditation authority and requesting reaccreditation if required.

Commanders and Managers

26. Commanders and Managers are responsible for ensuring facilities meet and maintain certification and accreditation standards. Conducting Annual Protective Security Self Assessment's, using form AC064, will provide ongoing assurance that

accreditation requirements are maintained and identify any remediation where required.

Certification authorities

27. The certification authority is responsible for:
- a. assessing and certifying facilities against relevant security controls, or variations to those controls, as detailed in the DSPF (refer DSPF Principle 72 - *Physical Security*), and recording the details in a certification report.
 - b. issuing the certification report along with recommendations to the accreditation authority, detailing the extent to which a facility complies with the relevant Security Zone standard for the assets requiring protection.
28. In relation to their certification role, certification authorities are to provide timely advice and assistance to facility owners to help identify:
- a. security zone requirements;
 - b. instances of non-compliance;
 - c. remediation strategies, security-in-depth and alternative controls or variations that may be available to mitigate security risks; and
 - d. requirements for the development of a security risk management plan where necessary.

Key Definitions

29. **Accreditation:** The process by which an authoritative body gives formal recognition that required security standards have been satisfied and, where applicable, associated residual risks have been accepted by a facility and/or asset owner for the operation of a facility. The outcome of the accreditation process is an authority to operate for a particular facility and/or, asset.
30. **Accreditation Authority:** The authority delegated to accredit a facility for use.
31. **Accreditation Certificate:** The formal instrument that:
- a. is signed by the accreditation authority confirming that appropriate security measures are in place for the protection of Defence assets and manage identified security risks; and
 - b. stipulates the conditions under which the facility or asset may operate without requiring a reassessment of the residual risk (by seeking re-accreditation).

32. **Certification:** A formal assurance process resulting in a statement (certification report) that outlines the extent to which a facility conforms to controls for the required Security Zone, and as required by the DSPF. Certification considers any additional controls identified by facility owners as part of a security risk management plan, and ensures appropriate security risk mitigation is applied for the protection of operations, assets and systems handled/stored/processed within the facility.

33. The outcomes of the certification process provide:

- a. assurance to facility owners that appropriate security mitigations have been applied for the assets requiring protection; and
- b. information to the accreditation authority they require to make an informed decision on whether, from a security perspective, the facility should be approved to operate.

34. **Certification Authority:** A subject matter expert who assess a facility against relevant security controls, which may involve review of security risk management plans provided by facility owner(s) where additional controls to baseline requirements of the DSPF are required.

35. **Certification Report:** The instrument produced by the certification authority that documents the extent to which a facility complies with relevant standards, taking into consideration baseline controls and additional controls subject to security risk management plans, where the certification report identifies each standard and assesses the degree to which each element of the standard has been achieved.

36. **Security Zones:** A methodology for the application of physical security measures, principally based on an assets Business Impact Level and, where necessary, a security risk assessment. It is a multi-layered system in which physical security measures combine to provide security-in-depth to those areas on a site that protect assets requiring more than normal fire and theft protection.

37. **Facility:** An area that facilitates government business.

Example: A facility can be a building, storage area floor of a building or a designated space on the floor of a building.

38. **Facility owner:** The person responsible for the operation of a facility.

39. **System:** A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates. A system can range from a single device such as a laptop, to a Defence-wide network.

40. **Security Protected Asset:** A non-financial, reportable or accountable asset that requires greater than standard fire and theft protection due to either:

- a. being allocated a BIL of 2 (Low to Medium) or higher;
 - b. an unacceptable business impact that would result from the unauthorised modification (ie. loss of integrity) of the asset, irrespective of whether that modification can be detected or not;
 - c. an unacceptable business impact that would result from the asset being unavailable (ie. loss of availability) for a given period of time; or
 - d. being categorised as a weapon or explosive ordnance.
41. **Asset owner:** The Group Head or Service Chief with responsibility and accountability for an asset for which responsibility has been assigned to them.
42. **Asset custodian:** The Commander or Manager responsible for the protection of asset(s) on issue to them.

Further Definitions

43. Further definitions for common PSPF terms can be found in the [Glossary](#)
44. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document Administration

Identification

DSPF Control	Physical Security Certification and Accreditation
Control Owner	Assistant Secretary Security Threat and Assurance (ASSTA)
DSPF Number	Control 73.1
Version	7
Publication date	22 September 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Security Certification and Accreditation
Related DSPF Control(s)	Personnel Security Clearance Assessing and Protecting Official Information

	Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security ICT Certification and Accreditation Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Access Control

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	02 July 2018	AS SPS	Launch
2	17 July 2018	AS SPS	Corrected Control Owner designation and modified Table 1 to include ASIO T4 form
3	06 August 2018	AS SPS	Giving CJOPS authority over EO storage and Armouries in areas of Ops
4	8 August 2019	AS SPS	PSPF alignment; Update to Reaccreditation intervals (Table 2)
5	22 May 2020	AS SPS	Update notes to explain acronyms in Table and amendments to para 15 reflect the requirement for DISP members to complete an annual security report
6	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
7	22 September 2020	AS SPS	Control Owner transferred to AS STA on 31 August 2020



Defence Security Principles Framework (DSPF)

Access Control

General principle

1. Defence-controlled areas are only to be accessed by persons whose identities have been established and who have the right and requirement to be there.

Rationale

2. Unauthorised access to Defence-controlled areas can lead to:
 - a. dangers to Defence personnel and persons engaged under contract;
 - b. theft of and damage to Defence assets and infrastructure; and
 - c. unauthorised access to sensitive Defence information, and information and communication technology (ICT) systems.
3. Each of these could compromise national security and personal safety.

Expected outcomes

4. Defence controls access to areas that are not designated as public areas. These include restricted Defence bases, establishments, military or business units, defence industry facilities and the assets and systems contained therein or parts thereof.
5. Personnel accessing Defence assets, information and facilities have been identified to have an accepted reason for seeking that access, and where applicable, the appropriate security clearance.
6. Records are retained about persons who have been granted access to Defence assets, information and facilities.
7. Defence is to issue credentials that convey an individual's clearance levels and under what circumstances they have been granted access.
8. Access to Defence assets, information and facilities is revoked for personnel who no longer meet clearance, need-to-know or suitability requirements.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	Director General (DG) ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Access Control
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 74
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 74.1
Control Owner	DG ESD

Related information

Government Compliance	PSPF Core Requirements: Eligibility and suitability of personnel; and Entity physical resources. Legislation: Privacy Act 1988 (Cth)
Read in conjunction with	N/A
See also DSPF Principle(s)	Assessing and Protecting Official Information Defence Industry Security Program Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Personnel Security Clearance Physical Security Identification, Search and Seizure Regime Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government physical security management protocol ASIO, Security Equipment Guides (SEGs) are available to ASAs from the GovDex Protective Security Community

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Physical Access Control

Control Owner

1. The Director General Estate Service Delivery (DGESD), Estate and Infrastructure Group (E&IG) is the Control Owner of physical access control across Defence sites with physical access control measures in place (electronic or other means).

Escalation Thresholds

2. The DGESD has set the following general threshold for risks managed against this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related *DSPF Principle and Expected Outcome*.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	Director Base Security Operations (DBSO), E&IG
Significant	DGESD, E&IG
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery Division (FAS SD), E&IG
Extreme	DSC – through FAS SD

Physical Access Control Measures at Defence Sites

3. This Control, 74.1 Physical Access Control and its associated Annexes outlines the policy for the physical access components on the Defence Common Access Card (DCAC) that are used to identify personnel and enforce physical access control to the Defence Estate on Defence sites with physical access control measures in place.

4. Controls that outline the policy for the logical information and communications technology (ICT) components on the DCAC are included in the

DSPF Controls; 17.1 *Information Systems (Physical) Security*, 18.1 *Information Systems (Personnel) Security* and 19.1 *Information Systems (Logical) Security*.

5. Contravention of Control 74.1 Physical Access Control and its associated Annexes is deemed to be a security incident as per the DSPF 77.1 *Security Incidents and Investigations* and its associated Control and Annexes.

6. The DSPF 74.1 Physical Access Control roles and responsibilities are defined at the end of this document. The roles and responsibilities are:

- a. Control Owners;
- b. Control Implementers;
- c. Control Officers;
- d. Head of Resident Units (HRUs);
- e. Commanders and Managers;
- f. Defence Industry Security Program (DISP) Members;
- g. Executive Security Advisors;
- h. Security Officers;
- i. Contract Managers;
- j. Sponsors; and
- k. DCAC holders.

7. DCACs are issued to personnel on behalf of the Department of Defence and remains the property of Defence at all times. Defence has obligations to ensure applicable Australian standards are met with the format, image requirements, production and protection of cards to reduce risks associated with fraud.

8. DCACs are a recognised form of secondary identification within the wider community, and Defence is responsible for issuing DCACs in accordance with Australian Government requirements.

9. The following measures are a responsibility of the DCAC holder to ensure their DCAC:

- a. is kept secure;
- b. not misused; and
- c. imagery is not on social media or internet sites.

10. This will assist in protecting personnel from identity theft and fraud risks. Personnel can seek clarification from their Security Officer, or refer to Australian Cyber Security Centre (CSC) [website](#) for more information.

11. It is the responsibility of the DCAC holder to ensure their issued DCAC is secured and not misused. Misuse includes:

- a. reproduction (copy – digital or hardcopy) of the DCAC to gain access to a Defence site;
- b. reproduction for malicious or illegal purposes; or
- c. providing a reproduction to persons without authorisation to view or hold the DCAC.

Exception: *It is acknowledged that some commercial operators may request to verify a person is a member of Defence in order to receive certain benefits. Those persons showing a DCAC for this purpose are advised to ensure operators comply with the Australian Privacy Principles.*

12. Personnel requiring regular access to Defence sites with access control measures in place (electronic or other means) **must** be issued a DCAC as per *Annex A to Access Control – Defence Common Access Card Types*.

13. Personnel with a legitimate reason for access, and whose identities have been established with a valid DCAC, may be authorised to enter Defence sites with physical access control measures in place on an ongoing or short-term basis. The DCAC types are detailed in *Annex A – Defence Common Access Card Types*.

14. The following groups of people can be issued a DCAC:

- a. Defence personnel (Australian Defence Force (ADF) and Australian Public Service (APS));
- b. ADF and APS family members;
- c. sponsored APS employees of other Australian Government departments or agencies;
- d. authorised foreign nationals (non-Australian citizens);
- e. authorised industry personnel (personnel from non-government organisations, businesses, companies or contractors);
- f. authorised members of the community, such as members of military associations, social and sporting clubs accessing Defence sites;

- g. ADF Cadets, Officer of Cadets, Instructor of Cadets, Defence Approved Helpers (DAH) and parents/guardians sponsored in accordance with Reserve and Youth Division's direction; and
 - h. Visitors and Very Important Persons (VIPs).
15. A DCAC remains the property of Defence and **must** be shown on request. Any DCAC not meeting validity requirements as stated in this Control and its associated Annexes will be seized by Defence, or its staff, including by contracted Access Control Officers.
16. A valid DCAC means a DCAC that:
- a. was issued in accordance with Principle 74 and this Control and its associated Annexes;
 - b. has not expired, been suspended or cancelled;
 - c. the holder continues to have a supported reason to hold and use;
 - d. is not a copy, has not been altered or defaced deliberately or through wear; and
 - e. the holder can be positively identified and has been issued to the person who shows or displays it.

Expected Requirements

17. DCACs **must** only be produced at an E&IG managed Defence Pass Office using authorised templates and approved card technology.
18. All electronic access control systems (EACS) at Defence sites are to ensure they comply with this Control and integrate with DCACs.
19. HRUs **must not** create bespoke card types that appear as a copy of an existing DCAC template for internal control systems.
20. Defence has inbuilt layers of security to protect its personnel and assets. One of these layers is the sharing of limited information from DCAC applications with Australian Government partner agencies. This assists Defence in understanding any potential risk a DCAC holder may present.

Transition to new DCAC Types

21. This Control updates Defence's DCAC types, templates and designs that are being introduced across Defence. All personnel **must** transition to the new DCAC type by **30 June 2021**. Only those DCACs detailed in this Control and relevant Annexes will be accepted to facilitate access to Defence sites after this date.

22. The new DCACs will also include multi-factor authentication which is used for logical ICT access to Defence information systems and associated devices such as printers.

23. It is the responsibility of all DCAC holders to ensure they transition to the new DCAC type. Personnel who are in possession of DCACs that are invalid after 30 June 2021 are to refer to *Annex C – Transitional arrangements for certain types of Defence Common Access Cards* for more information, or contact their local Defence Pass Office or Security Officer.

DCAC Types

24. Only those personnel recognised by the sponsor as eligible will obtain and retain access to Defence resources (people, information and assets). Careful consideration should be given to the DCAC type required, including consideration of the DCAC category and the DCAC Colour Series. Refer to paragraph 33 on DCAC sponsorship.

25. There are two primary categories of DCAC:

a. **Security Cleared DCAC** – issued to personnel who:

- (1) have a current Australian Government security clearance, or a security clearance which has been formally recognised by Defence in accordance with DSPF Control 40.1 *Personnel Security Clearance*; and
- (2) have a demonstrated requirement to access security classified Defence information and/or assets.

b. **Uncleared DCAC** – issued to personnel who:

- (1) do not hold a current Australian Government security clearance or a security clearance formally recognised by Defence in accordance with DSPF Control 40.1 *Personnel Security Clearance*; and
- (2) have a demonstrated requirement for unescorted access on a Defence site for Zone 2 and below.

Note: It is recognised that classified information or assets may be located in some areas rated Zone 2. It remains the responsibility of the relevant HRU to ensure that appropriate measures are in place to prevent unescorted access by Uncleared DCAC holders.

26. For more information on DCAC types refer to *Annex A – Defence Common Access Card Types*.

DCAC Colour Series

27. There are five DCAC Colour Series that relate to the holder and that holder's site access privileges and restrictions, escort privileges and card expiry period.
28. The DCAC Colour Series are:
- a. Purple Series – ADF Security Cleared DCAC and ADF Family Uncleared;
 - b. Blue Series – APS Security Cleared DCAC;
 - c. Yellow Series – Defence Industry DCAC Security Cleared and Uncleared;
 - d. Green Series – Foreign Security Cleared and Uncleared, Foreign Security Cleared and Uncleared Temporary Access Card (TAC); and
 - e. Red Series – Common Areas Uncleared.
29. The Colour Series are outlined in the AE294 Defence Common Access Card (DCAC) Application Web Form and this Control's related Annexes.
30. DCAC cards that provide short term access include:
- a. Positive Identification Card – Cleared and Uncleared;
 - b. Visitor Identification Cards (VIC) and Very Important Persons (VIP) Card; and
 - c. Temporary Access Paper Passes (TAPP).

Example: When using a Positive Identification (PI) Card created for specific building access, efforts should be made to use personnel's existing DCAC profile for access to business units and systems which are compliant with perimeter access control systems were possible.

31. DCACs assist in visually identifying access to Security Zones. The security clearance requirements for personnel to gain access to Security Zones on a Defence site are dependent on the classification of any information or asset stored and handled within the Security Zone.
32. For access to Zone 3 all Uncleared DCAC holders **must** be under escort by a Security Cleared DCAC holder and are to remain under direct control by a HRU. Security Zones on Defence sites are detailed in the DSPF Control 72.1 *Physical Security*.

DCAC Sponsorship

33. A DCAC sponsor **must** only sponsor a DCAC holder aged 16 years or older, and have a demonstrated need or supported justification for regular access to Defence sites.

34. Exceptions are as below.

Exceptions: A DCAC may be issued to the following people under the age of 16:

An Australian Defence Force (ADF) Cadet under the age of 16 years a **Red Series Common Areas Uncleared DCAC**;

An ADF family member 14 years or older a **Purple Series ADF Family Uncleared DCAC**; or,

A sponsored Industry person under the age of 16 years, (such as an apprentice) a **Yellow Series Industry Uncleared DCAC**.

35. A sponsor is required for all DCAC applications, and should satisfy themselves of the following:

- a. that the applicant has a demonstrated requirement or justification to access a Defence site;
- b. the DCAC type requested aligns with the intended access requirement; and
- c. where discretion exists, the level of access required is justified, (for example whether access to a single Defence site or national access is justified for Uncleared DCAC holders).

36. Details of the requirements and attributes associated with specific cards are found in *Annex A – Defence Common Access Card Types*.

37. The DCAC sponsor can request a background Police Check before sponsoring an Uncleared DCAC if it is deemed necessary, provided all requirements are met before proceeding with the Police Check. The Police Check **must** be approved by the Director of Base Security Operations E&IG, or their approved delegate, that he/she is satisfied that all of the following requirements are met:

- a. a Security Risk Assessment (SRA) justifying this requirement;
- b. any associated costs should be paid directly from the Defence sponsor's cost centre. A DCAC applicant or Industry partner should not incur any costs directly or indirectly at any time;
- c. is not carried out on any person under the age of 18 years;
- d. the Defence sponsor has appropriate written procedures that:
 - (1) manage information in accordance with the Privacy Act 1988;
 - (2) align with any legislative instruments or international treaties;
 - (3) align with Defence policy, including decision making guidelines (for instance, the [Good Decision Making in Defence: A Guide for Decision-Makers and Those Who Brief Them](#)); and

- (4) includes a framework to address appeals and/or other administrative action if the issue of a DCAC is denied.

Note: Director of Base Security Operations, E&IG as the Control Implementer, can delegate authority to a project, contract or Defence site for multiple police checks to occur when satisfied that all requirements have been met.

38. If the sponsor changes roles or leaves Defence, the sponsor is required to notify the local Pass Office to have their Defence sponsorship records updated.

Sponsorship for ADF, APS and Family

39. To act as the sponsor for an ADF or APS DCAC, the sponsor:
- a. is required to be either an ADF member or a Defence APS employee;
 - b. is to be at a minimum EO5/APS 3 level, unless the individual is in the position of Security Officer in the sponsoring business unit; and
 - c. is to be in the business unit that has some functional or professional responsibility for, or association with, the supervisor of, or function/service being performed/facilitated by the DCAC applicant or their employing organisation.
40. Family members of Defence personnel can hold a DCAC. Defence personnel are to sponsor family members and are responsible and accountable for the ongoing use and return of the DCAC by their family member/s.

Note: Defence personnel are accountable for the DCAC to be returned if there is a change of circumstance, including transition from Defence or changes to family circumstances.

41. ADF personnel seeking DCACs for family members:
- a. should sponsor their own family members for the issue of a **Purple Series ADF Family Uncleared DCAC**, or an authorised Unit delegate may sponsor if the ADF member is absent on deployment or is reasonably unable to do so, e.g. hospitalised; and
 - b. the applicant is required to provide sufficient evidence (i.e. Dependant or Beneficiaries) to confirm the applicant's relationship to the sponsor.
42. It is recognised that extenuating circumstances may exist where ADF personnel may seek Defence site access for extended family members not listed as Dependents or Beneficiaries. The ADF member or the business unit of these ADF personnel may sponsor a **Red Series Common Areas Uncleared DCAC** in these instances.

Note: ADF personnel who deploy may seek external support for their dependants who reside within service residence on base.

43. APS personnel seeking DCACs for family members:
- a. should sponsor their own family members for the issue of a **Red Series Common Areas Uncleared DCAC**; and
 - b. The applicant is required to demonstrate a business need (e.g. drive family member on to a Defence site). The sponsor is to produce sufficient evidence (i.e., emergency contacts from PMKeyS) to confirm the applicant's relationship to the sponsor.
44. Reserve and Youth Division ADF Cadets and their family members should refer to *Annex A – Defence Common Access Card Types* and *Annex C – Transitional arrangements for certain types of Defence Common Access Cards*.

Sponsorship for Industry

45. The responsibility for determining access and DCAC type for Industry personnel resides with the relevant Defence (ADF/APS) Product, Project, Contract Director/Manager or equivalent. This may be delegated to, at a minimum, EO5/APS 3 level.
46. The sponsor is to carefully consider Industry personnel's DCAC physical access requirements. This includes consideration of:
- a. the purpose of the request, and if the DCAC applicant already has a valid DCAC;
 - b. the DCAC category required (Security Cleared or Uncleared);
 - c. where discretion exists, the locations where access for Uncleared Industry personnel is required (base specific, E&IG Zones, State/Territories or national). Security Cleared Industry personnel are granted national access; and
 - d. the selection of a DCAC type and where discretion exists, the expiry period. Where applicable the DCAC expiry period should reflect the period of time that the DCAC holder is expected to have a business requirement to access Defence site/s. In some cases a person may have multiple business relationships with Defence and this should be a consideration.

Note: Sponsorship may be achieved either through sponsorship of individual applications or through a Sponsorship Direction Letter. Guidance on this process can be obtained from DBSO.

Note: The practice of Industry personnel holding multiple Industry DCACs should not occur. Sponsors are authorised to consider all circumstances and request a DCAC that meets all business requirements for an individual.

Example: A contractor is employed on more than one project or is employed by more than one company providing services to Defence. In this situation the contractor should only be issued one card, and their access privileges updated as required. At times this will require the Sponsor details to be updated through local Pass Offices to ensure expressed interest in the holder is known by Defence.

Note: If a Defence Industry person already holds a valid DCAC but requires a different DCAC type due to a change in business role, the existing DCAC **must** be surrendered on issue of the new DCAC.

DCAC Issue and Use

47. All personnel should **only hold a single DCAC** of a colour series unless entitled to as specified in this DSPF Control 74.1 *Physical Access Control* and its associated Annexes. Further information and guidance can be found on the AE294 Defence Common Access Card (DCAC) Application or by contacting the DBSO.

48. The initial issue of a DCAC will only be to personnel upon presentation of approved forms of valid Government issued photographic identification documents (driver's licence, passport or proof of age card) and the signed AE294 Defence Common Access Card (DCAC) Application.

49. A DCAC is a recognised form of secondary identification operating in the community. As such, Defence has an obligation to ensure the Department of Home Affairs' National Identity Proofing Guidelines, or its equivalent, are met. Only identification documents that meet these requirements may be used to establish an identity. For more information contact the DBSO.

50. Verification of persons under the age of 18 years should be established using approved photographic identification. Refer to the National Identity Proofing Guidelines for "verifying the identity of children".

51. A valid DCAC may be presented as a form of identification for DCAC renewals.

Note: A DCAC that has expired for no more than three months shall be deemed valid for the purpose of photographic identification. An expired DCAC is not valid for the purpose of access to a Defence site and will be seized by Defence, or its staff, including contracted Access Control Officers.

52. Security controls **must not** be introduced that impose increased requirements on obtaining a DCAC outside of this Control.

Terms and Conditions

53. The DCAC 'Terms and Conditions' as per the AE294 Defence Common Access Card (DCAC) Application **must** be acknowledged by the DCAC recipient.

Note: Any person under the age of 18 years receiving a DCAC is to be accompanied by a parent,

guardian or other suitable adult. Terms and Conditions are to be counter-signed by an adult.

54. Failure to comply with the 'Terms and Conditions' for a DCAC is reportable as a Security Incident in accordance with DSPF Control 77.1 *Security Incidents and Investigations* and could result in an investigation or further action that may include suspension or cancellation of a DCAC.

55. Holders of a valid DCAC **must**:

- a. clearly display the DCAC for inspection and/or electronic scanning when entering or exiting a Defence site for which its use is required;
- b. show the DCAC when requested by any appropriate authority who, in the course of their duty, requires proof of identity;
- c. wear a DCAC at all times on site, (unless wearing the DCAC presents a safety hazard), in a prominent position on the front or side of the body, and remove it when leaving the Defence site/area/s for which it is required;
- d. only use the DCAC for the purposes and in the areas for which it was sponsored;
- e. make reasonable efforts to protect the DCAC from loss, theft, copying, defacement or unauthorised use;
- f. ensure that the DCAC is secured, not misused and imagery is not on social media or internet sites;
- g. be responsible for the conduct and direction of visitors under direct supervision as an escort **at all times**;
- h. report lost or stolen DCACs to a Defence Pass Office and Security Officer at the earliest opportunity and submit a Defence XP188 Security Incident report;
- i. not lend the DCAC to any other person; and
- j. surrender the DCAC to a Supervisor, Contract Manager, Security Officer, contracted Access Control Officer, Commander or Manager or their approved delegate when there is no longer a demonstrated requirement to hold it.

56. All security incidents are to be reported via Defence XP188 Security Incident report.

57. All valid DCAC holders are expected to challenge any person not wearing a DCAC or suspected of being in a location contrary to their DCAC access limitations. Base Security Management Plans should include local procedures to reinforce a security challenge culture.

Note: When wearing a DCAC presents a potential safety hazard, such as using machinery, there is no requirement for it to be worn. However, a DCAC is to be presented if requested to allow for positive identification to be established.

Access to a Defence Site

58. All persons accessing a Defence site where access control measures exist are required to present their DCAC for inspection to contracted Access Control Officers or equivalent and/or by the use of Electronic Access Control System (EACS).

59. To ensure positive identification at either an access control point or whilst on a Defence site, personnel are to comply with requests to remove items such as glasses, helmet or other items in order for this to occur. Unless safety or other conditions apply, such as religious requirements, a person **must** comply when requested to do so.

Note: Whilst a DCAC is subject to natural wear and tear, the holder of the DCAC should be clearly identified as the person who shows or displays it upon request.

60. Access to a Defence site **must** be in accordance with the valid DCAC type and for reasons that are substantiated if challenged. Valid DCAC holders **must not** access a Defence site at any time without a justifiable requirement. Failure to comply with this requirement will constitute a Security Incident in accordance with *DSPF Control 77.1 Security Incidents and Investigations* and could result in an investigation or further action, which may include suspension or cancellation of a DCAC.

61. Access control arrangements may be determined by a site Security Risk Assessment (SRA) and incorporated into the Base Security Management Plan for the following situations:

- a. public transport access, including taxis and other forms of for-hire transport;
- b. public access to facilities such as museums, church services, golf clubs, etc.;
- c. cash-in-transit or similar activities; and
- d. deliveries on site.

62. Defence sites have specific Base Induction information available for the security, safety and emergency response requirements and restrictions. At heightened SAFEBASE Security Alert levels (Alert and Act), refer to the SAFEBASE security alert system [page](#).

Access for Special Events

63. A special event is a short duration event on a Defence site subject to access control measures where alternate security controls are deemed a requirement.

64. Special events could include:
- a. air shows and other public events at a Defence site, such as ANZAC Day ceremonies or a major Cadet activity;
 - b. disaster assistance, requiring Government agencies or evacuees to access Defence bases;
 - c. activities, such as the opening of a new hangar or display;
 - d. visit by a school group;
 - e. foreign military arrival by ship or air;
 - f. official activities, such as a visit by dignitaries or Very Important Persons (VIPs);
 - g. irregular events, such as the arrival of a diverted civilian aircraft; or
 - h. major construction work (refer to the example of a special event (1) below or contact the DBSO for further clarification).
65. Alternate security controls for a special event are determined by the Base Manager (BM). A Senior ADF Officer (SADFO) may determine physical access requirements when command of a Defence site has been assumed in accordance with the Joint Framework for Base Accountabilities.
66. A SRA should be utilised to determine alternate security controls.

Example 1 of a special event: Annexing a major construction project from a Defence site with the installation of temporary fencing and an alternate entry point. Through this approach contractors do not require access onto a Defence site and therefore there is no requirement for a DCAC to be issued.

Example 2 of a special event: A Defence planning conference is to be held on a Defence site involving a large number of foreign military participants. Obtaining a DCAC or escorting participants is logistically difficult and impracticable. Supported by a SRA, access to the Defence site is controlled by the use of Defence bus transport and personnel movement on the Defence site is restricted to the conference location only.

Access for Emergency Responders

67. Emergency Responders (i.e. Police, Fire, and Ambulance) are not required to be positively identified prior to gaining entry when responding to an incident on a Defence site.

Note: Any Australian Defence Force and/or Civilian emergency responders driving under activated lights and sirens are to be given unimpeded access.

68. Commonwealth, State and Territory government law enforcement, fire and ambulance services accessing a Defence site that is subject to access control measures may, in the normal execution of their routine duties, utilise their Government issued identification as a form of positive identification and be permitted unescorted access within the boundary of Security Zone 2 or below. For access to Security Zone 3 and above the HRU is responsible.

69. Other State, Territory or Commonwealth agencies, such as the Australian Border Force members, may be issued a DCAC.

Note: Liaison with HRUs may be necessary to gain any required access into Security Zone 3 and above area on a Defence site.

Access for Visitors

70. A visitor on a Defence site aged 16 years or older **must** be issued with either a **Visitor Identification Card (VIC)** or a **Very Important Person (VIP) Card** and be escorted at all times by a valid DCAC holder with escort privileges in accordance with that DCAC holder's access privileges and limitations.

71. The continued use of Visitor Identification Cards for persons that regularly access Defence sites should be avoided. If a person is reasonably expected to visit a Defence site more than 28 days over a rolling 12 month period then a DCAC should be issued.

72. A VIC card may be issued to an authorised person who has a supported requirement to access a Defence site and is not in possession of a valid DCAC with access privileges at the applicable Defence site.

73. A VIP card may be issued to a Two Star (or equivalent) and above ranked military officers, spouses/partners and guests of Three-Star ranked (or equivalent) and other persons deemed by the Base Manager (BM) and/or SADFO to fit this category.

74. Examples of a **VIC** or **VIP Card** are provided at *Annex A – Defence Common Access Card Types*.

75. Any failure to provide effective escort to a visitor will be deemed a Security Incident attributed to the relevant DCAC holder.

76. **VIC** and **VIP** cards are to be returned to the issuing officer at the end of the visit on the day of issue.

77. Where there are several visitors requiring access, the Defence host is responsible for providing a sufficient number of escorts appropriate to the size of the visiting party and the environment. Escort means a valid DCAC holder who:

a. has escort privileges;

- b. has accepted responsibility for the conduct of the person(s) being escorted **at all times**; and
 - c. provides direction to all visitors under their supervision.
78. Holders of the following DCAC types **must not** be provided visitor escort privileges:
- a. **Green Series Foreign Uncleared DCACs.**

Exception: Escort permitted for Cadet Members in possession of a Grey Cadet ID Card.

79. HRU or other business units may implement their own visitor management arrangements for Security Zones under their direct control. These arrangements should align with this Control and its associated Annexes.
80. Base Security Management Plans may detail specific requirements for physical access by media representatives. Visitors in this category **must** be issued a **VIC** and be under escort unless part of a designated Special Event.
81. The visit of officials who have a statutory right to enter workplaces (e.g., trade union and Comcare officials) in relation to their official role under relevant legislation (such as the *Fair Work Act 2009* or the *Work Health and Safety Act 2011*) are to be treated as visitors. If these persons do not hold a valid DCAC, they are to be issued a **VIC** and be under escort. The government identification of these persons **must** be recognised. Access should be provided on all occasions unless a heightened threat environment exists under SAFEBASE.

Access for Persons under the Age of 16 years

82. Defence site's Base Security Management Plan may have procedures where persons under the age of 16 years can access, unaccompanied, up to Common Areas only (Security Zone 2 and below) without a DCAC. If not detailed in the Base Security Management Plan, persons under the age of 16 years are to be accompanied by a valid DCAC holder with escort privileges.

Note: In DSPF Control 74.1 Access Control, persons under the age of 16 years are excluded from being required to be issued a DCAC, VIC or Temporary Access Paper Pass (TAPP). Refer to paragraph 34 for exemptions.

83. ADF family members are eligible for a **Purple Series ADF Family Uncleared DCAC** from 14 years of age. It is recommended family members residing in Defence supplied housing on a Defence site arrange for DCACs for persons aged 14 years or older and are to wear the DCAC when and where appropriate. Refer to the site's Base Security Management Plan for further guidance.

Access for Reserve and Youth Division ADF Cadets

84. **From 30 June 2021**, only ADF Cadets issued with a DCAC under this Control and relevant Annexes will be permitted unescorted access to a Defence site subject to access control measures. Refer to *Annex C – Transitional arrangements for certain types of Defence Common Access Cards*.

85. **From 30 June 2021**, the Grey Cadet ID Card produced under the authority of the Directorate of Youth **will not** allow unescorted access onto a Defence site subject to access control measures. The Grey Cadet ID Card will continue to be issued to relevant personnel and will hold the same access privileges as a **VIC**. The holder of this card type **must** be escorted by a valid DCAC holder on a Defence site subject to access control measures.

Note: To allow a transition to occur, Base Security Management Plans may continue to allow unescorted access for Grey Cadet ID Cards up **until 30 June 2021**. From this date, the Grey Cadet ID Cards will not permit unescorted access on to Defence site with access control measures in place. The Grey Cadet ID card will be treated as a Visitor Identification Card and require escort from a valid DCAC holder at all times. Any valid DCAC holder may escort a Grey Cadet ID Card holder.

86. Cadet Support personnel, including Cadet Officers and Instructors, and parent/s or guardian/s of a Cadet member and Cadets seeking access to a Defence site may be issued a **Red Series Common Areas Uncleared DCAC** in accordance with *Annex A – Defence Common Access Card Types*.

Access for Short Term Unescorted Access

87. The production of a **Temporary Access Paper Pass (TAPP) Uncleared Unescorted** allows short-term, unescorted access to a Defence site up to 14 days with a sponsor approved application form and appropriate identification. Issuing a DCAC or escorted **VIC** is considered a more appropriate means to allow access. Refer to *Annex A – Defence Common Access Card Types* for more information about the **TAPP Uncleared Unescorted**.

88. Persons accessing Defence sites on a **TAPP Uncleared Unescorted** are restricted to a maximum of 28 days over a rolling 12 month period in total (i.e. the issue of two 14 day TAPPs to allow time for a DCAC to be issued).

Suspension or Cancellation of a DCAC

89. Defence retains the right to suspend or cancel a DCAC as a result of a security incident or when information becomes available that presents an unacceptable risk to Defence.

90. For suspension or cancellation of DCACs, the decision making authority is, in consultation with relevant stakeholders, as listed below:

- a. Yellow Series Defence Industry DCAC (Security Cleared or Uncleared) – the relevant Project Manager, Contract Manager or their equivalent.
 - b. Green Series Foreign Industry (Security Cleared or Uncleared) – the Project Manager, Contract Manager or their equivalent.
 - c. Green Series DCACs held by non-industry personnel – the relevant sponsor, Commander, Manager, BM or SADFO.
 - d. Purple Series DCACs – the relevant Commander, Manager or SADFO.
 - e. Blue Series DCACs – the relevant Commander or Manager. With respect to external agencies the relevant Commander or Manager **must** be consulted.
 - f. Red Series DCACs – the sponsor, BM or SADFO.
91. Notwithstanding the above, DGED as the Control Owner, or DBSO as the Control Implementer, may exercise the decision to cancel or suspend any valid DCAC as a result of a security incident or when information becomes available through partner agencies that presents an unacceptable risk to Defence.
92. In all instances of a DCAC being suspended or cancelled, the following **must** be carried out:
- a. within 48 hours, a reasonable effort is made to provide the DCAC holder with a letter from a minimum O5/EL1 to cancel or suspend the holder's DCAC and a copy provided to DBSO, E&IG as the Control Implementer;
 - b. provide opportunity for the DCAC holder to appeal the decision within 28 days of receipt of the letter;
 - c. if an appeal is made, the relevant decision maker should be at minimum one level above the original decision maker that cancelled or suspended the DCAC. The respondent is to be provided a letter outlining the judgement to uphold or rescind the original decision and a copy provided to DBSO, E&IG as the Control Implementer; and
 - d. further mechanisms for review should be available through the Administrative Appeals Tribunal or the relevant Ombudsman.
93. Management, security officers and clearance sponsors are to monitor the security attitudes and behaviours of their Security Cleared and Uncleared staff. This includes the prompt reporting to Australian Government Security Vetting Agency (AGSVA) of a noticeable change in attitude or behaviour, security incidents, or any incidents that may be a security concern. Upon receipt of advice regarding a security concern, AGSVA may reassess the suitability of a clearance holder. Refer to Control 40.1 Personnel Security Clearance.

94. If the DCAC holder is under the age of 18 years, then a suitable adult, such as parent, guardian or sponsor, is to be notified.

Note: The E&IG DBSO intranet site contains templates that can be utilised for the suspension and cancellation of DCACs.

95. The [Good Decision Making in Defence: A Guide for Decision-Makers and Those Who Brief Them](#) provides guidance for those in Defence with decision making responsibilities and should be used in all instances for suspension or cancellation of a DCAC.

Stolen DCAC

96. The holder of a DCAC **must** report the theft of a DCAC at the earliest opportunity to a Defence Pass Office and their Security Officer. All security incidents are to be reported via Defence XP188 Security Incident report. The Security Officer is to treat the theft as a security incident and report it in accordance with DSPF Control 77.1 *Security Incidents and Investigations*.

97. When a stolen DCAC is reported, the Defence Pass Office will cancel the DCAC once notified. A replacement DCAC may be issued on receipt of a sponsored AE294 Defence Common Access Card (DCAC) Application.

Lost DCAC

98. Lost DCACs are to be reported to a local Defence Pass Office, which will cancel the card, and an XP188 Security Incident report **must** be submitted. A replacement card may be issued on receipt of a sponsored AE294 Defence Common Access Card (DCAC) Application.

DCAC Renewal

99. Personnel may renew their DCAC within 90 days of the expiry date printed on the card.

Note: A **Purple Series ADF Security Cleared DCAC** holder that is deploying or posting overseas may be issued a new DCAC to ensure that the validity covers the deployment or posting period. As a general rule, the DCAC should be valid for the deployment/posting period plus a further six months. A new DCAC application is required and this will be issued with a five year expiry period (unless otherwise specified).

Any ADF Family DCACs may be renewed under these circumstances also.

Replacement of DCAC

100. Personnel may be issued a replacement DCAC on receipt of a AE294 Defence Common Access Card Application under the following circumstances:

- a. physical appearance of the DCAC, including photo to an extent that positive identification cannot be established; or
- b. movement between ADF Services.

101. Any replacement card for defacement, deterioration or inoperability may be undertaken without an AE294 Defence Common Access Card Application if the DCAC holder's details can be confirmed by the Defence Pass Office. A replacement DCAC **must** reflect the same attributes (expiry date and personal details) as the card being replaced.

102. For a change of name an AE795 Change Your Legal Name form is to be completed electronically and forwarded to the relevant Defence Pass Office for action.

103. For ADF personnel with a change of rank, the DCAC holder can either present evidence of change of rank (PMKeyS print out or Certificate of Promotion) and be issued a replacement DCAC with the same expiry date, or complete an AE294 Defence Common Access Card application to be issued a new DCAC with a five year expiry period.

DCAC Return

104. DCACs remain the property of Defence and **must** be returned to Defence when there is no longer a legitimate reason to access a Defence site. Any failure to surrender a DCAC when required may result in further action, including ineligibility to obtain any future DCACs.

105. Defence personnel transitioning from the APS or ADF are required to surrender their DCAC (including family member DCACs) to their Security Officer, Supervisor, Commander, Manager or contracted Access Control Officers. This should be part of the routine off boarding administration for all Defence personnel.

Exception: As per *Annex A to Access Control – Defence Common Access Card Types*: An ADF member SERCAT 3 to 7 may be issued a **Purple Series ADF Security Cleared DCAC**. The respective Service may issue a **Purple Series ADF Security Cleared DCAC** to persons categorised SERCAT 1 or 2 up to a period of five years. The member **must** continue to hold a national security clearance in accordance with **DSPF Control 40.1 Personnel Security Clearance**.

ADF members transitioning from the Department **may** retain their Purple ADF DCAC if they follow the process at **Management of Purple Series ADF DCAC for Transitioning Members** found at Annex D.

Note: The Commander/Supervisor/Unit Security Officer may decline the request to retain a DCAC at transition if a genuine security threat exists.

106. Industry personnel **must** surrender their DCAC to their Supervisor, Security Officer, contracted Access Control Officer, Contract Manager or equivalent on cessation of their contract or when no longer required to access Defence sites. This

is to be part of the routine off boarding administration at the conclusion of the contract or when the holder no longer has legitimate access requirements.

107. Security Officers, Supervisors, Commanders or Managers **must** destroy the APS, ADF or Industry DCAC that is no longer required and notify a Defence Pass Office of its destruction (which will include documenting the DCAC serial number) or the DCAC can be returned to the nearest Defence Pass Office for destruction within a reasonable timeframe.

***Note:** There will be occasions when the holder of an Industry DCAC ceases employment or contract with Defence but continues to have a demonstrated business need to retain a DCAC because of a further contract or relationship with Defence. In cases such as this, the respective Industry sponsor is to satisfy themselves that retention of the DCAC is legitimate.*

108. All other DCACs **must** be returned to their DCAC sponsor or approved delegate for destruction, after notifying the Defence Pass Office, or by returning the DCAC to the nearest Defence Pass Office for destruction.

109. When a Defence Pass Office receives notification of a destroyed DCAC, the card will be cancelled. When a Pass Office receives a returned DCAC, the receiving Pass Office Operator will cancel and then destroy the DCAC as soon as practicable.

110. The returned DCACs can be physically destroyed using facilities available at the Defence site by cutting or shredding the DCAC.

111. Where a person has ceased to have a legitimate reason to hold a DCAC but has failed to return the card, the relevant sponsor, Commander or Manager **must** inform their Security Officer or relevant Defence Pass Office in order for any Electronic Access Control Systems (EACS) and building permissions to be deactivated and investigated as appropriate.

Standard Operating Procedures and Templates

112. DBSO, E&IG owns and maintains the standard operating procedures on the issue, replacement and return of DCACs. All card templates are controlled by DBSO.

Roles and Responsibilities

Control Owner Responsibilities

Control Owner is responsible for:

- Managing specific security risk controls up to and including Significant in accordance with escalation thresholds;
- Setting access control arrangements at all Defence sites where access control measures exist;
- Determining standards and templates for DCAC and access control systems; and
- May decide to cancel or suspend any valid DCAC as a result of a security incident or unacceptable risk to Defence.

Head of Resident Unit Responsibilities

Head of Resident Units are responsible for:

- Setting security access control requirements for business units or facilities in accordance with the Physical Security Zone methodology; and
- Undertaking duties as specified in the [Joint Framework for Base Accountabilities](#).

Control Implementer Responsibilities

Control Implementer and or their approved delegate is responsible for:

- Managing specific security risk controls up to and including Moderate in accordance with escalation thresholds; and
- May decide to cancel or suspend any valid DCAC as a result of a security incident or unacceptable risk to Defence.

Commanders and Managers Responsibilities

Commanders and Managers are responsible for:

- Ensuring persons under their command are aware of their obligations and any contravention of this policy is addressed in consultation with the Control Owner or Control Implementer and the BM;
- Implementation of access control measures in accordance with the Physical Security Zone methodology;
- Off boarding including following the governance measures to return DCACs when no longer required; and
- Monitoring the security attitudes and behaviours of their Security Cleared and Uncleared staff and reporting any changes to AGSVA.

Control Officer Responsibilities

Control Officers (including BMs and SADFOs are responsible for:

- Elevating access control risks above Low in accordance with Escalation Thresholds;
- Implementing access control measures with the Physical Security Zone methodology at a whole-of-base level; and
- Undertaking duties in managing and operating Defence bases which align to this control as defined in the [Joint Framework for Base Accountabilities](#).

Defence Industry Security Program Responsibilities

DISP members are responsible for:

- Maintaining accreditation of their facilities, including meeting the necessary physical security standards;
- For further information refer to Control 16.1 on Defence Industry Security Program; and
- Off boarding including following the governance measures to return DCACs when no longer required.

Executive Security Advisors Responsibilities

Executive Security Advisors are responsible for:

- Assisting Commanders and Managers of military and/or business units to fulfil their legislative and Defence policy security responsibilities. This may include any specific access requirements; and
- Sponsor DCACs at any rank/APS level, if the Security Advisor is within the relevant military or business unit responsible and has been delegated by Commanders and Managers.

Security Officers Responsibilities

Security Officers are responsible for:

- Supporting Control Owners, Executive Security Advisors, and Commanders and Managers and DCAC holders on security matters.
- Providing advice on the DSPF, general security matters and processes.
- Following the governance measures to return DCACs when no longer required.
- Monitoring the security attitudes and behaviours of their Security Cleared and Uncleared staff and reporting any changes to Commanders, Managers and AGSVA.

Contract Manager Responsibilities

Contract Managers (ADF/APS), Product Directors in E&IG, and their equivalents are responsible for:

- Determining the DCAC category required (security cleared/uncleared);
- The locations where an Uncleared DCAC holder requires access;
- The validity period of a DCAC (e.g. the end of the contract);
- Following the governance measures to return DCACs when no longer required; and
- Management of security risks associated with their respective product/project.

Sponsor Responsibilities

Sponsors are responsible for:

- Ensuring the correct DCAC type is issued to the applicant before they gain access to a Defence base;
- When relevant, that the applicant has an active security clearance;
- Checking the applicant's details are correct and matching their identification documents;
- Ensuring that all sites-specific access requirements are detailed in the application;
- Monitoring their DISP contractor processes to ensure physical security standards are maintained; and
- Off boarding including handing over their sponsorship records should their role change and notifying the local pass office of sponsorship transfer.

DCAC Holder Responsibilities

DCAC holders are responsible for:

- Elevating access control risks in consultation with their Supervisor, Commander or Manager in accordance with escalation Thresholds;
- Complying with the terms and conditions of DCAC use;
- Ensuring their DCAC is secure, not misused and their DCAC imagery is not on social media or internet sites;
- Accessing only those areas and systems they have been authorised to;
- Promptly reporting the loss or theft of their (or a family member's) DCAC;
- Off boarding including returning their (and any family member's) DCAC when transitioning from the APS or ADF, or for Industry at the conclusion of a contract unless other arrangements have been made with a Defence sponsor;
- Challenging any person on a Defence site subject to access control measures who they believe is not conforming with this Control and its associated Annexes;
- Reporting a change of circumstance that impacts on the holder's ability to hold the DCAC; and
- Provide effective escorting to any visitors under their control.

Key Definitions

113. **Access control** means the ability to control access to designated areas, information or other assets requiring protection.

114. **Physical Access control measure** means an established perimeter point of entry, either permanent or temporary, where access is controlled to a Defence site either by a contracted Access Control Officer or equivalent, for example a physical measure such as a gate/boom.

115. **Common Areas** means an area that is inside a Defence-established or base perimeter subject to access control measures and outside of a Physical Security Zone 3 or higher. Further information on the allocation of Security Zones on Defence sites is detailed in the DSPF Control 72.1 *Physical Security*.

116. **Defence Common Access Card** means an access card, which may also be programmed for logical access to ICT or use on an electronic access control system, for those establishments and facilities which the holder has a legitimate need or authorisation to access. Refer to *Annex A – Defence Common Access Card Types* for more information.

117. **Electronic Access Control System (EACS)** means a system that allows physical access to occur through an electronically controlled barrier that usually consists of an electronic DCAC control reader near a barrier that records and facilitates ingress/egress.

118. **Escort** means a valid DCAC holder who:

119. has escort privileges;

120. has accepted responsibility for the conduct of the person(s) being escorted; and

121. provides direction to all visitors under their supervision **at all times**.

122. **Physical access** means the components that are used to identify personnel and enforce physical access control.

123. **Security Zones** are a methodology for physical security mitigation based on a security risk assessment. It is a multi-layered system in which physical security measures combine to provide security-in-depth to those areas on a site that protect assets which require more than normal fire and theft protection.

124. **Unescorted access** means a type of access granted to an individual who has been positively identified, and has a confirmed need or authorisation to enter a Defence site subject to access control measures.

125. **Valid DCAC** means a DCAC:

- a. was issued in accordance with Principle 74 and this Control and its associated Annexes;
- b. has not expired, been suspended or cancelled;
- c. the holder continues to have a supported reason to hold and use;
- d. is not a copy, has not been altered or defaced deliberately or through wear; and
- e. the holder can be positively identified and has been issued to the person who shows or displays it.

126. **Temporary Access Paper Pass (TAPP)** means a paper pass issued by contracted Access Control Officers using the Visitor Management System (VMS) where available.

127. **Visitor** means a person that is not in possession of a valid DCAC and has demonstrated a legitimate requirement to visit a Defence site that has access control measures in place and has been issued a valid **Visitor Identification Card (VIC)** or **Very Important Person (VIP)** Visitor Card. Refer to *Annex A – Defence Common Access Card Types* for more information.

Further Definitions

128. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Glossary

Acronym	Description
ADF	Australian Defence Force
AGSVA	Australian Government Security Vetting Agency
APS	Australian Public Servant
BM	Base Manager
CSC	Cyber Security Centre
DAH	Defence Approved Helper
DBSO	Director Base Security Operations, E&IG
DCAC	Defence Common Access Card
DGESD	Director General Estate Service Delivery
DISP	Defence Industry Security Program
DSC	Defence Security Committee
DSPF	Defence Security Principles Framework
DS&VS	Defence Security & Vetting Service
E&IG	Estate and Infrastructure Group
EACS	Electronic Access Control System
FAS SD	First Assistant Secretary Service Delivery Division
HRU	Head of Resident Unit
ICT	Information Communications Technology
ID	Identification
PACS	Physical Access Control System
PI	Positive Identification
PMKeyS	Personnel Management Key Solution
SADFO	Senior Australian Defence Force Officer
SERCAT	Service Categories
SIA	Security of Information Agreement
SOPs	Standard Operating Procedures
SRA	Security Risk Assessment
TAC	Temporary Access Card
TAPP	Temporary Access Paper Pass
VIC	Visitor Identification Card
VIP	Very Important Person

Annexes and Attachments

Annex A – Defence Common Access Card Types

Annex B – Defence Common Access Card Types – Visual

Annex C – Transitional arrangements for certain types of Defence Common Access Cards

Document Administration

Identification

DSPF Control	Physical Access Control
Control Owner	DGESD
DSPF Number	Control 74.1
Version	5
Publication date	15 March 2022
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Access Control
Related DSPF Control(s)	Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Defence Industry Security Program Personnel Security Clearance Physical Security Security Incidents and Investigations

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DGESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	16 December 2020	DGESD	Annual review of control. Changes made for the delivery of the DCAC Upgrade project consolidation of card types. Reference to DSPF ICT policies introduced.
4	21 December 2020	AS SPS	Format update page 21-22
5	15 March 2022	DGESD	Changes to paragraph 105 exceptions



Defence Security Principles Framework (DSPF)

Annex A to Physical Access Control – Defence Common Access Card Types

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Defence Common Access Card Types
Annex Version	3
Annex Publication date	16 December 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Physical Access Control
DSPF Number	Control 74.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DGESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy, DS&VS Clearance Advice POC details
3	16 December 2020	DGESD	Annual review and renaming of Annex.



Defence Security Principles Framework (DSPF)

Annex B to Physical Access Control – Defence Common Access Card Types - Visual

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Defence Common Access Card Types
Annex Version	3
Annex Publication date	16 December 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Physical Access Control
DSPF Number	Control 74.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DGESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy, DS&VS Clearance Advice POC details
3	16 December 2020	DGESD	Annual review and renaming of Annex.

Version	Date	Author	Description of changes
			Significant changes made to align with the delivery of the DCAC Upgrade project, including consolidation of card types and definitions.

Version	Date	Author	Description of changes
			Significant changes made to align with the delivery of the DCAC Upgrade project, including consolidation of card types and definitions.



Defence Security Principles Framework (DSPF)

Physical Access Control

Annex C – Transitional Arrangements for certain types of Defence Common Access Cards

Defence Common Access Cards

1. From the release of the updated DSPF Control 74.1 Physical Access Control and its associated Annexes, **only** the DCAC types detailed in **Annex A – Defence Common Access Cards** are to be issued to DCAC holders.

Exception: The Grey Cadet ID will continue to be produced by Reserve and Youth Division. Refer to the "Grey Cadet Identification (ID) Card" section for conditions.

2. This Annex details the transitional arrangements and rules for those card types that will **cease to be valid from 30 June 2021**. Refer to figures 1 and 2 of this annex for the DCAC Cleared and Uncleared Transition.
3. It is the responsibility of the DCAC holder to ensure that they have taken the necessary steps to return their invalid DCAC and be issued (and sponsored where required) with a new DCAC; this extends to Australian Defence Force (ADF) personnel that have sponsored family members. For further enquiries, DCAC holders should contact their local Pass Office or the Directorate of Base Security Operations (DBSO).
4. The majority of the DCAC transitions will occur over a four month period, with sequencing of cardholder attendance at a Pass Offices or pre-approved collection point which is to be managed by a project team, to ensure that each Pass Office has sufficient capacity to meet the demand for new DCACs. The majority of transitioning cardholders (those with access to the Defence Protected Environment (DPE)) will be requested to nominate a preferred collection location and time. Sponsors of Cleared cardholders without access to the DPE will be requested to communicate with their sponsored cardholders to assist with meeting transition timeframes.
5. **This Annex ceases to apply after 30 June 2021.**

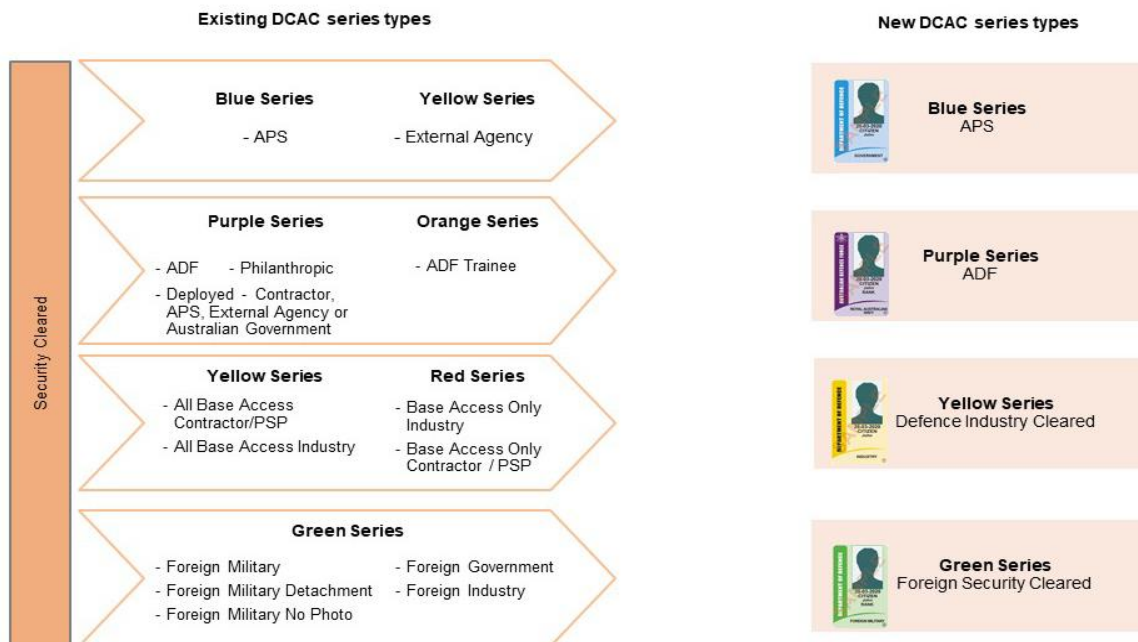


Figure 1: Security Cleared DCAC Transition

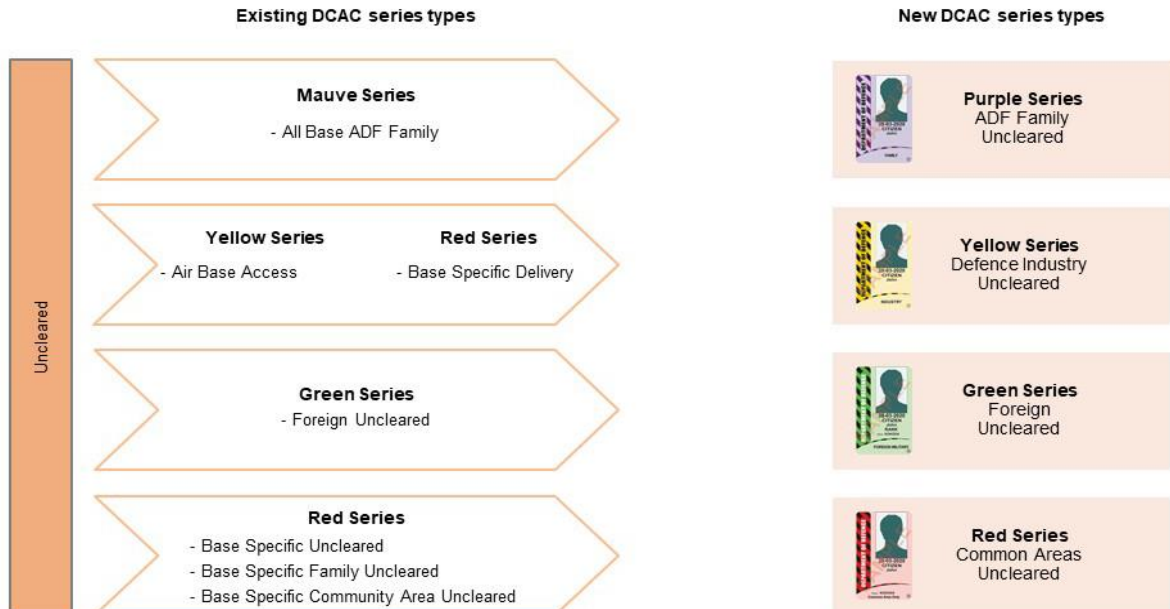


Figure 2: Uncleared DCAC Transition

Purple Series

Purple Series ADF

6. Existing Purple series ADF card holders issued to Navy, Army and Air Force will be required to transition to the new **Purple Series DCAC** by **30 April 2021**.

Transition rule: Holders of this DCAC type will receive a verification email to confirm their DCAC details within the DCAC upgrade portal. If details within the portal are not correct the holder of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The DCAC being replaced is to be current.

Purple ADF Work Health Safety DCAC

7. **Purple ADF Work Health Safety (WHS) DCACs** issued to Navy and Army refers to a **Purple Series ADF Security Cleared DCAC** with information on the back of the DCAC that the holder has completed WHS training, and their signature.

Transition rule: Holders of this DCAC type will receive a verification email to confirm their DCAC details within the DCAC upgrade portal. If details within the portal are not correct the holder of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The DCAC being replaced is to be current.

Purple ADF Philanthropic

8. Existing Purple ADF Philanthropic card holders will be required to transition to the new **Purple Philanthropic DCAC** by **30 April 2021**.

Transition rule: Holders of this DCAC type may attend a Pass Office and request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application form). The DCAC being replaced is to be current. (A valid Sponsor is to be provided at time of request).

Orange ADF Trainee DCAC

9. **Orange ADF Trainee DCACs** issued to Navy, Army and Air Force trainees at the discretion of the relevant Base Manager and Senior Australian Defence Force Officer (SADFO).

10. No further production of this card type will occur. Existing card holders will transition to the **Purple Series ADF Security Cleared DCAC** by **30 April 2021**.

Transition rule: A new DCAC application will be required for the issue of a replacement card at time of renewal.

Mauve Family and Mauve All Base Family DCAC

11. **Mauve All Base Family DCACs** issued to recognised family members aged 16 years and older of ADF permanent and ADF Working Reserve members upon application.
12. No further production of this card type will occur. Existing card holders will transition to the **Purple Series ADF Family Uncleared DCAC** by **30 June 2021**.

Transition rule: Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The DCAC being replaced is to be current and will expire on the same date as the serving member. (Arrangements have been made in the DCAC Portal to assist ADF members to book family appointments concurrently).

Blue Series

Blue Series APS DCAC

13. Existing Blue Series APS card holders issued to, APS Permanent Staff and APS non-ongoing staff will be required to transition to the **Blue Series Australian Public Services (APS) - Government Security Cleared DCAC** by **30 April 2021**.

Transition rule: Holders of this DCAC type will receive a verification email to confirm their DCAC details within the DCAC upgrade portal. If details within the portal are not correct the holder of this DCAC type may request a replacement card without the requirement for a new application (AE294 Common Access Card Application). The DCAC being replaced is to be current.

Blue Series APS External Agency DCAC

14. Existing Blue Series APS External Agency card holders will be required to transition to the new **Blue External Agency - Government Security Cleared DCAC** by **30 April 2021**.

Transition rule: Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). If the new DCAC is not requested through the DCAC portal the expiry date will remain the same as the current DCAC presented to the designated Pass Office Operator. If the replacement DCAC has three months or less remaining a new AE294 is to be submitted. The DCAC being replaced is to be current.

Yellow Series

Yellow Cleared Industry DCAC

15. Yellow Cleared Industry card holders will be required to transition to the new **Yellow Cleared Industry DCAC** by **30 April 2021**.

Transition rule: Holders of this DCAC type may receive a verification email to confirm their DCAC details within the DCAC upgrade portal. If details within the portal are not correct the holder of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card). The expiry date shall reflect five years from the date of issue. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.

Additional transition rule: For holders of this DCAC type who do not have an active ICT account, refer to para 4 of this Annex for further guidance.

Yellow All Base External Agency DCAC

16. **Yellow All Bases External Agency DCACs issued to Australian citizens** with a recognised Australian Government security clearance in the role of contractors, consultants or outsourced service providers from external, Commonwealth agencies (staff of non-corporate Commonwealth entities).

17. No further production of this card type will occur. Existing card holders will transition to either the **Yellow Series Industry Security Cleared DCAC** (for contractors and consultants) or **Blue Series Australian Public Service (APS) – Government Security Cleared DCAC** (for staff of non-corporate Commonwealth entities) by **30 April 2021**.

Transition rule: The expiry date shall reflect five years from the date of issue, unless there is less than three months' validity remaining on the DCAC, if so a new AE294 is to be submitted.

Yellow All Bases Contractor/Professional Service Personnel (PSP)

18. **Yellow All Bases Contractor/Professional Service Personnel (PSP) issued to Australian citizens** with a recognised Australian Government security clearance in the role of contractors/PSPs who require access to all bases.

19. No further production of this card type will occur. Existing card holders will transition to the **Yellow Series Defence Industry Security Cleared DCAC** by **30 April 2021**.

Transition rule: Holders of this DCAC type may receive a verification email to confirm their DCAC details within the DCAC upgrade portal. If details within the portal are not correct the holder of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect five years from the date of issue. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.

Additional transition rule: For holders of this DCAC type who do not have an active ICT account, refer to para 4 of this Annex for further guidance.

Yellow All Base Industry DCAC

20. **Yellow All Bases Industry DCACs** issued to Australian citizens with a recognised Australian Government security clearance that are contractors, consultants and outsourced service providers that require access to all bases.

21. No further production of this card type will occur. Existing card holders will transition to the **Yellow Series Defence Industry Security Cleared DCAC** by **30 April 2021**.

***Transition rule:** Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect five years from the date of issue. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.*

Yellow All Bases Air Base Access DCAC

22. **Yellow All Bases Air Base Access DCAC** issued to authorised Australian citizens, Airservices Australia Flight Inspection Services personnel. Holders are not required to have a recognised security clearance.

23. No further production of this card type will occur. Existing card holders will transition to the **Yellow Series Defence Industry Uncleared DCAC** by **30 June 2021**.

***Transition rule:** Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect three years from the date of issue. A replacement DCAC for this card type will only be issued upon the return of the extant DCAC which has not expired. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.*

Red Series

Red Base Access Only Delivery Uncleared DCAC

24. **Red Base Access Only Delivery Uncleared DCAC** issued to Australian citizens without a recognised Australian Government security clearance that require access to a base/s as a contracted delivery driver.

25. No further production of this card type will occur. Existing card holders will transition to the **Yellow Series Defence Industry Uncleared DCAC** by **30 June 2021**.

***Transition rule:** Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect three years from the date of issue. A replacement DCAC for this card type will only be issued upon the return of the extant DCAC. The DCAC being replaced is to be current, along with a valid Sponsor*

being provided at time of request.

Red Base Specific Community Only Uncleared DCAC

26. **Red Base Specific Community Only Uncleared DCAC issued to** Australian citizens without a recognised Australian Government security clearance that are authorised to access Community Areas only on a specific base.

27. No further production of this card type will occur. Existing card holders will transition to a new DCAC type by **30 June 2021**; refer to *Annex A – Defence Common Access Card Types* to determine the appropriate DCAC type for the individual's needs.

Red Base Specific Uncleared DCAC

28. **Red Base Specific Uncleared DCAC issued to** Australian citizens without a recognised Australian Government security clearance that are authorised to access Community Areas on a base.

29. No further production of this card type will occur. Existing card holders will transition to a new DCAC type by **30 June 2021**; refer to *Annex A – Defence Common Access Card Types* to determine the appropriate DCAC type for the individual's needs.

Transition rule: Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect 12 months from the date of issue. A replacement DCAC for this card type will only be issued upon the return of the holders extant DCAC. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.

Red Base Access Only Family Uncleared DCAC

30. **Red Base Access Only Family Uncleared DCAC issued to** Australian citizens without a recognised Australian Government security clearance who are recognised family members of ADF and APS personnel that require access to the base.

31. No further production of this card type will occur. Existing card holders will transition to either the **Purple Series ADF Family Uncleared DCAC** or the **Red Series Common Areas Uncleared DCAC** depending on whether it is ADF or APS sponsored by **30 June 2021**.

Transition rule: Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect 5 years from the date of issue. A replacement DCAC for this card type will only be issued upon the return of the holders extant DCAC. (**Note:** The expiry date of this new DCAC series is to align with the serving ADF or APS sponsor).

Red Overseas Deployment Family DCAC

32. **Red Overseas Deployment Family DCAC issued to** recognised family members of ADF and APS personnel, and recognised family members of ADF and APS employees posted overseas.

33. No further production of this card type will occur. Existing card holders will transition to the **Purple Series ADF Family Uncleared DCAC** or the **Red Series Common Areas Uncleared DCAC** depending on whether it is ADF or APS sponsored by **30 June 2021**.

Red Base Access Only Industry Cleared DCAC

34. **Red Base Access Only Industry Cleared DCAC issued to** Australian citizens with a recognised Australian Government security clearance that are Industry personnel who require specific base access.

35. No further production of this card type will occur. Existing card holders will transition to the **Yellow Series Defence Industry Security Cleared DCAC** by **30 June 2021**.

***Transition rule:** Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect five years from the date of issue. A replacement DCAC for this card type will only be issued upon the return of the holders extant DCAC. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.*

Red Base Access Only Contractor/PSP Cleared DCAC

36. **Red Base Access Only Contractor/PSP Cleared DCAC issued to** Australian citizens with a recognised security clearance that are contractors/PSPs that require specific base access.

37. No further production of this card type will occur. Existing card holders will transition to the **Yellow Series Defence Industry Security Cleared DCAC** by **30 June 2021**.

***Transition rule:** Holders of this DCAC type may request a replacement card without the requirement for a new application (AE294 Defence Common Access Card Application). The expiry date shall reflect five years from the date of issue. A replacement DCAC for this card type will only be issued upon the return of the holders extant DCAC. The DCAC being replaced is to be current, along with a valid Sponsor being provided at time of request.*

Green Series

Green Foreign Government Cleared DCAC

38. **The Green Foreign Government Cleared DCAC issued to** non-Australian citizens from foreign government agencies who have a Defence recognised security clearance and need ongoing access to a base.

39. Existing card holders will transition to the **Green Series Foreign Security Cleared DCAC** by **30 June 2021**. Refer to *Annex A – Defence Common Access Card Types* for further clarification.

Transition rule: A new DCAC application will be required for the issue of a replacement card.

Green Foreign Cleared DCAC

40. **The Green Foreign Cleared DCAC issued to** non-Australian citizens who have a Defence recognised security clearance. This includes personnel that require regular, unescorted access to a Defence site or foreign force personnel that are temporarily attached (units in Australia on secondment) to the ADF.

41. No further production of this card type will occur. Existing card holders will transition to the **Green Series Foreign Security Cleared DCAC** or the **Green Series Foreign Security Cleared Temporary Access Card (TAC)** by **30 June 2021**. Refer to *Annex A – Defence Common Access Card Types* for further clarification.

Transition rule: A new DCAC application will be required for the issue of a replacement card.

Green Foreign Industry Cleared DCAC

42. **The Green Foreign Industry Cleared DCAC issued to** non-Australian citizens who have a Defence recognised security clearance and are accessing Defence bases as an industry representative.

43. No further production of this card type will occur. Existing card holders will transition to the **Green Series Foreign Security Cleared DCAC** by **30 June 2021**. Refer to *Annex A – Defence Common Access Card Types* for further clarification.

Transition rule: A new DCAC application will be required for the issue of a replacement card.

Green Foreign Military Cleared DCAC

44. The Green Foreign Military Cleared DCAC issued to non-Australian citizens who have a Defence recognised security clearance and are accessing Defence bases as a foreign forces representative.

45. No further production of this card type will occur. Existing card holders will transition to the **Green Series Foreign Security Cleared DCAC** or the **Green Series Foreign Security Cleared Temporary Access Card (TAC)** by **30 June 2021**. Refer to *Annex A – Defence Common Access Card Types* for further clarification.

Transition rule: A new DCAC application will be required for the issue of a replacement card.

Green Foreign Military Detachment Cleared DCAC

46. The Green Foreign Military Detachment Cleared DCAC issued to non-Australian citizens who have a Defence recognised security clearance and are accessing Defence bases as a foreign forces representative.

47. No further production of this card type will occur. Existing card holders will transition to the **Green Series Foreign Security Cleared DCAC** or the **Green Series Foreign Security Cleared Temporary Access Card (TAC)** by **30 June 2021**. Refer to *Annex A – Defence Common Access Card Types* for further clarification.

Transition rule: – A new DCAC application will be required for the issue of a replacement card.

Green Foreign Uncleared DCAC

48. The Green Foreign Uncleared DCAC issued to non-Australian citizens that do not hold a Defence recognised security clearance. This includes members of the public requiring base Common Access only, or foreign force personnel that are temporarily attached to the ADF and do not hold a Defence recognised security clearance.

49. No further production of this card type will occur. Existing card holders will transition to the **Green Series Foreign Uncleared DCAC** or the **Green Series Foreign Uncleared TAC** by **30 June 2021**. Refer to *Annex A – Defence Common Access Card Types* for further clarification.

Transition rule: a new DCAC application will be required for the issue of a replacement card.

Identification Card

Grey Cadet Identification (ID) Card

50. **The Grey Cadet ID** Cards produced with authority under the Head of Reserve and Youth Division and issued to ADF Cadets, Instructors, support staff and family members as needed.

51. The Grey Cadet ID card will continue to be produced but the card will cease to permit escort privileges or unescorted access to those Defence sites with access control measures in place **from 30 June 2021**. The card will act as a form of identification only that allows the holder to be escorted on a Defence site without being signed in/registered as a visitor. For more information, refer to *Annex A – Defence Common Access Cards*.

Note: To allow a transition to occur, Base Security Management Plans may continue to allow unescorted Grey Cadet ID card holders access up until 30 June 2021. From this date, the Grey Cadet ID cards will not permit unescorted access on the Defence estate. Grey Cadet ID cards will be treated as Visitor Identification Cards and require escort from a valid DCAC holder at all times. Any valid DCAC holder may escort a Grey Cadet ID card holder.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex C	Transitional Arrangements for certain types of Defence Common Access Cards
Annex Version	1
Annex Publication date	16 December 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Access Control
DSPF Number	Control 74.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	16 December 2020	DGESD	Launch of transitional arrangements for certain types of Defence Common Access Cards.



MANAGEMENT OF PURPLE SERIES ADF DEFENCE COMMON ACCESS CARDS FOR TRANSITIONING MEMBERS

Step 1: Transitioning ADF Member

- Draft and send an email with your card credentials (**Full Name, PMKeyS, DCAC number, Date of Birth**) to your Commander, Supervisor or Unit Security Officer requesting your card status to be marked 'Returned' with the effect date of your transition or transfer.

Those transferring to the ADF Reserves should retain their DCAC.

Step 2: Commander/Supervisor/Unit Security Officer

- Forwards the departing ADF member's card credentials to Defence Pass Office Restricted Encoding requesting the card be marked as 'Returned'.
- Confirms if the member wishes to retain their DCAC.
- If yes, on the day of transition use a pair of scissors to safely cut the top right hand corner of the DCAC as illustrated in **Diagram 1**.
- For any reason this step cannot be undertaken members are to attend their local Pass Office.
- If the member does not wish to retain their ADF DCAC it **must** be returned to a Defence Security Guard or a local Pass Office for destruction.

Note: The Commander/Supervisor/Unit Security Officer may decline the request to retain a DCAC at transition if a genuine security threat exists.



Diagram 1 – Front and Back of DCAC once cut.

Promptly undertaking the above steps is essential to maintaining Defence security and is a condition of use for all ADF issued DCACs. Further information regarding this change is available through Base Security Operations.



Document administration

Identification

DSPF Annex	Management of Purple Series ADF Defence Common Access Cards for Transitioning Members
Annex Version	1
Annex Publication date	15 March 2022
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Physical Access Control
DSPF Number	Control 74.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	15 March 2022	DGEDS	Launch



Defence Security Principles Framework (DSPF)

Annex E to Physical Access Control – National Police Check

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	National Police Check
Annex Version	1
Annex Publication date	28 September 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Physical Access Control
DSPF Number	Control 74.1

Related Information

Government Compliance	Protective Security Policy Framework (PSPF) Privacy Act 1988 (Cth) Australia's Anti-Discrimination Law Fair Work Act 2009 Australian Standard: 4811:2022: Workforce Screening Australian Standard :31000:2018: Risk Management Guidelines
See also DSPF Principles (s)	11 – Security for Projects 12 – Security for Capability Planning 16 – Defence Industry Security Program 17 – Physical 18 – Personnel 19 – Logical Information Systems Security
Resources and Tools	Australian Human Rights Commission, On the Record, Guidelines for the prevention of discrimination in employment on the basis of criminal record – 2012 Link to Defence Security Zone Guidance ADF Discrimination due to Criminal Record. Good Administrative Decision Making Manual Defence – Security Risk Assessment Template Defence Industry Security Program webpage AGSVA Resources Unconscious Knowledge and Bias Training (CAMPUS) SBS Inclusion – First Nations (0074653) PSPF Policy 12 – Eligibility and suitability of personnel

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	28 September 2023	DGESD	New document



Defence Security Principles Framework (DSPF)

Contracted Security Guards

General principle

1. Contracted security guards contribute to the protection of:
 - a. Defence assets and infrastructure from theft or damage; and
 - b. Official Information, facilities, information and communication technology (ICT) systems from unauthorised access.

Rationale

2. Contracted security guards are an element of an integrated security system to detect, deter, deny, and (in a limited capacity) respond to security threats and incidents at Defence bases and facilities.
3. Guarding requirements are based on the assessed needs for the security of personnel, information and physical assets at the base or facility.

Expected outcomes

4. Defence maintains an efficient, effective and credible contracted guarding service.
5. Contracted security guards engaged by Defence are:
 - a. trustworthy;
 - b. qualified;
 - c. appropriately licensed/accredited; and
 - d. properly briefed/instructed with regard to their duties.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager.
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations.
Significant	Director General Estate Service Delivery (DG ESD).
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery (FAS SD).
Extreme	Defence Security Committee (DSC) – through FAS SD.

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Contracted Security Guards
Principle Owner	First Assistant Secretary Security and Vetting Services (FAS DS&VS)
DSPF Number	75
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 75.1
Control Owner	DG ESD

Related information

Government Compliance	<u>PSPF Core Requirements</u>: Entity physical resources and Entity facilities Legislation: <u>Work Health and Safety Act 2011 (Cth)</u> <u>Privacy Act 1988 (Cth)</u> <u>Security Industry Act 2003 (ACT)</u> <u>Security Industry Act 1997 (NSW)</u> <u>Private Security Act 1995 (NT)</u> <u>Security Providers Act 1993 (Qld)</u> <u>Security and Investigation Industry Act 1995 (SA)</u> <u>Security and Investigations Agents Act 2002 (Tas)</u> <u>Private Security Act 2004 (Vic)</u> <u>Security and Related Activities (Control) Act 1996 (WA)</u> Standards: <u>AS ISO 31000:2018 - Risk management - Guidelines</u> <u>AS/NZS 4421:2011 Guard and Patrol Security Service</u>
Read in conjunction with	Base Services Contract Base Security Plans
See also DSPF Principle(s)	Defence Industry Security Program Identity Security Access Control Identification, Search and Seizure Regime Procurement
Implementation Notes, Resources and Tools	<u>PSPF - Physical Security</u> ASIO, Security Equipment Guides (SEGs) are available to ASAs from the GovDex Protective Security Community Defence Industry Security Program (<u>Industry Security</u>)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch

Version	Date	Author	Description of changes
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Contracted Security Guards

Control Owner

1. Director General Estate Service Delivery (DG ESD) is the owner of this enterprise-wide control.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager.
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations.
Significant	DG ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery (FAS SD).
Extreme	DSC – through FAS SD.

Note: Persons engaged under contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Control

Probity and Security Checking

2. **Licences.** Contracted Security Guards, including employees and subcontractors of contracted guarding service providers, are to maintain current State/Territory licences to carry out their required functions.
3. **Personnel security clearance.** Contracted security guards are to hold a minimum security clearance of Baseline whilst engaged on the Defence Estate. Higher clearances may be required for facility-specific duties.

4. **Defence Industry Security Program (DISP) Membership.** Contracted security providers are to maintain DISP membership (refer DSPF Principle 16 – *Defence Industry Security Program*).

Contract Requirements

5. Contract Managers are to ensure contracted security guards are contractually required to:

- a. be licensed in the relevant State/Territory;
- b. display their security licence on their person whilst on duty;
- c. maintain a minimum security clearance of Baseline; and
- d. understand their responsibilities and obligations under, and not contravene, any Defence directives or Federal/State/Territory/local laws.

6. Contract Managers are to consult with the Defence Security & Vetting Service (DS&VS) regarding guarding contracts, prior to signature.

7. Incorporated security performance measures should focus on outcomes and support a risk management methodology (refer [ISO 31000:2009 Risk Management – Principles and Guidelines](#).)

8. Persons engaged under contract to provide guarding services outside of Base Service guarding contracts are required to comply with the licencing and training requirements in this DSPF Control in addition to anything specified in their contracts.

Competencies

9. Persons engaged as contracted security guards are to possess a minimum Certificate II in Security Operations.

10. Contracted security guards are to maintain the required competencies throughout their employment whilst engaged on the Defence estate.

11. Contracted security guards carrying out specialist functions may be required to obtain and maintain a Certificate III in Security Operations in addition to additional competencies.

12. Contracted security guards are to complete a Defence-endorsed training package (delivered by the contracted security guard service provider, or Defence). This is to cover topics such as:

- a. Defence security policy and relevant Federal, State and Territory laws;
- b. Defence protocols (including rank structure, customer service, etc.);
- c. the Defence security environment;

- d. Defence policing; and
- e. the SAFEBASE alert level security system.

Guarding Duties and Assignment Instructions

13. Contracted security guards are to be given comprehensive, base-specific assignment instructions that include:

- a. the effective security of the base or facility;
- b. dealing with emergency procedures;
- c. lines of communication; and
- d. accountabilities.

14. The Director Base Security Operations (DBSO) is to ensure contracted security guards are familiar with their assignment instructions, and all operational practices and procedures.

15. Assignment instructions are to address the responsibilities of contracted security guards as agents of the Commonwealth in relation to legal powers under the [Crimes Act 1914](#) and [Defence Act 1903](#). These include:

- a. the granting or refusing of entry;
- b. the right of challenge;
- c. common law arrest; and
- d. search in relation to offences.

16. The instructions are to be endorsed by the control owner in consultation with local Base Support Managers (BSMs), and should be reviewed annually. They should also be reviewed when:

- a. There is a change to the SAFEBASE alert level (refer DSPF Principle 83 – *SAFEBASE*); or
- b. infrastructure changes occur.

17. These instructions are to be available for contracted security guards to consult in the course of their duties, but secured in line with DSPF Principle 10 – *Assessing and Protecting Official Information*.

18. The DBSO and the contracted security provider are to be consulted prior to any changes to Base Security Instructions or the operation of physical security equipment being implemented. Any enhancements are to be delivered with adequate notice and training.

Other site specific duties

19. Other duties contracted security service providers and guards may be required to undertake at designated sites include, but are not limited to:
- a. controlling access points;
 - b. issuing, receipting, encoding and recording Defence Common Access Cards (DCAC) and other Defence identity and access cards (refer to DSPF Principle 74 – *Access Control*);
 - c. conducting consensual identification and search, and restraint and detention in defined circumstances (refer to DSPF Principle 76 – *Identification, Search and Seizure Regime*);
 - d. conducting patrols of sites, perimeters and building exteriors (including providing, operating and maintaining electronic patrol recording systems);
 - e. operating and resetting (including arming and disarming) alarm panel systems;
 - f. monitoring and operating alarm control systems, including:
 - (1) following alarm response instructions;
 - (2) conducting alarm verification and acknowledgement;
 - (3) closing alarm incidents; and
 - (4) reporting alarm incidents.
 - g. operating and monitoring surveillance and detection systems;
 - h. operating emergency response systems, including Base Wide Audible Alert Systems;
 - i. responding to security incidents;
 - j. managing security keys including:
 - (1) maintaining a registry for all allocated security keys;
 - (2) ensuring the security of keys and key management systems;
 - (3) issuing and receipting security keys; and
 - (4) reporting lost or suspected compromised keys to Base Support personnel.
 - k. reporting and recording security and patrol incidents and occurrences, including security-related damage;

- l. contributing to the investigation of security incidents; and
- m. providing reports and audits in accordance with contractual regimes.

Patrols and alarm response

20. Contracted guarding services may include mobile and random patrols of bases outside of business hours, even if the site has a 24/7 security guard presence. Requirements for mobile patrols (including their frequency) are to be determined through a Security Risk Assessment (SRA).

21. The frequency of patrols undertaken for regular information container or physical asset inspections, and patrols of facilities out of hours are defined by guidelines:

- a. provided by ASIO in the ASIO -Type 1 SAS – Implementation and Operation Guide (refer to Table 1 – Out of hours patrol and alarm response requirements);
- b. in the [Protective Security Policy Framework \(PSPF\) 16 Entity facilities Security Guards](#); and
- c. requirements defined in any SRAs.

Table 1: Out of Hours Patrol and Alarm Response Requirements

Physical Security Zone	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Out of hours guard patrols (random intervals)	Determined by SRA	Determined by SRA	Minimum every 4 hours	Minimum every 4 hours	Minimum every 2 hours
Out of hours alarm response	As contained in SRA.	As contained in SRA.	Determined by SRA (response should be within the delay period given by the physical security controls)	Determined by SRA (response should be within the delay period given by the physical security controls)	Determined by SRA (response should be within the delay period given by the physical security controls)

22. Out-of-hours contracted security guards, in response to alarms in all Physical Security Zones, are to respond within the delay period afforded by the physical security controls.



Australian Government
Department of Defence

Roles and Responsibilities

Director General Estate Service Delivery (DG ESD)

23. DG ESD is responsible for:
- a. the delivery of contracted guarding services to Defence bases in the Base Accountabilities Model; and
 - b. approving the requirement for specialist guarding functions at a base or facility.

Group Heads and Service Chiefs

24. In the unlikely event that guarding services are required to be engaged outside of the national contract, Group Heads and Service Chiefs are to ensure:
- a. guarding requirements (including those in this DSPF Control) are incorporated into any guarding contracts;
 - b. contract performance is monitored and assessed;
 - c. the service provider is a member of the Defence Industry Security Program (DISP); and
 - d. E&IG is consulted in the development of security guarding contracts and arrangements.

Contract Managers

25. Contract Managers are responsible for ensuring:
- a. guarding requirements are identified (including the requirement for surge as directed by Defence), and are appropriately included in the contract;
 - b. the guarding standards in this DSPF Control and E&IG SOPs are incorporated into security guarding contracts;
 - c. contracts for the provision of guarding services allow for changing requirements and changes to the SAFEBASE alert level;
 - d. contract performance is monitored and assessed;
 - e. the contracted security provider is a member of the DISP;

- f. external service providers are contractually bound to comply with AS/NZS 4421:2011; and
- g. DS&VS is consulted in the development of security guarding contracts.

Base Support Manager

26. The BSM, in consultation with the Senior ADF Officer (SADFO), and as a part of the base SRA, is responsible for consulting with the Contract Manager to determine guarding requirements at their base.
27. The BSM is also responsible for:
- a. ensuring effective communication:
 - (1) the BSM;
 - (2) SADFO; and
 - (3) any other base security personnel that support incident response arrangements, and the management of other contracted guarding functions;
 - b. ensuring there effective management arrangements are in place to coordinate and task guards in response to a security threat, an incident, or a change to the SAFEBASE alert level;
 - c. maintaining oversight of guarding services and ensuring all guarding requirements and standards are met;
 - d. establishing base security instructions; and
 - e. involving contracted security providers in planning activities and site reviews.

Key Definitions

28. **Security Guard:** A person tasked to undertake guarding functions, including:
- a. access control (e.g. reception, pass issue, patrols, traffic control, and search and inspection);
 - b. asset and alarm monitoring;
 - c. responding to security incidents;
 - d. operating alert and communications systems; and
 - e. security administration.
29. **Assignment Instructions:** An operational document detailing the specific duties to be performed under a guarding contract.

Further Definitions

30. Further definitions for common PSPF terms can be found in the [Glossary](#). Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Contracted Security Guards
Control Owner	DG ESD
DSPF Number	Control 75.1
Version	2
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Contracted Security Guards
Related DSPF Control(s)	Defence Industry Security Program Identity Security Access Control Identification, Search and Seizure Regime Procurement

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Identification, Search and Seizure Regime

General principle

1. Defence controls access to Defence facilities, assets and Official Information through an identification, search and seizure regime in full compliance with the relevant legislation.

Rationale

2. Security precautions at Defence bases aim to protect people, prevent theft and damage to Defence assets and infrastructure, and prevent unauthorised access to sensitive Defence information and systems. A key component of these precautions is the implementation of a statutory identification, search and seizure regime.

Expected outcomes

3. Defence operates a statutory regime of graduated identification, search, seizure and related powers, which are exercised by three identified classes of Defence Security Officials, to enhance the security of Defence bases, facilities, assets and personnel within Australia.

4. The level of identification and search capability required at each Defence site is determined on the basis of a security risk assessment, having regard to the nature of the primary assets to be protected and the assessed security risks.

Note: A different search regime may operate on Defence bases where Defence Security Official's (DSO) are not utilised. Searches undertaken outside of the [Defence Act 1903](#) Part VIA may be based on common law or other legislation and are strictly limited in scope. Further information on searches conducted under these circumstances is provided at DSPF Control 76.1, Annex A -Other Non-Statutory Search Regimes.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	Director General (DG) ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary, Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Identification, Search and Seizure Regime
Principle Owner	First Assistant Secretary Security and Vetting Services (FAS DS&VS)
DSPF Number	Principle 76
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 76.1
Control Owner	Director General Estate Service Delivery

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Entity physical resources. Legislation: <u>Defence Act 1903</u> , Part VIA, Security of Defence Premises.
Read in conjunction with	N/A
See also DSPF Principle(s)	Physical Security Certification and Accreditation Security Incidents and Investigations Access Control
Implementation Notes, Resources and Tools	The scope of this principle and underlying security controls is confined to describing the identification search and seizure regime and does not describe the role of Armed Security Wardens or the operation of the Enhanced Self Defence Capability (ESDC) – these remain the responsibility of the Chief of Army (CA).

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Identification, Search and Seizure

Control Owner

1. The Director General Estate Service Delivery (DG ESD) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The DG ESD has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	DG ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary, Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Implementation of Identification, Search and Seizure Regime

3. Implementation of the identification, search and seizure regime and the subsequent appointment of Defence Security Officials (DSO) across Defence premises will vary depending upon the nature of the site, the primary assets to be protected and the threat level. For example:

- a. Consensual search and identification actions might be undertaken by contracted Defence security guards, on entry to and exit from Defence premises, or part thereof, at low to medium SAFEBASE alert levels.
- b. Non-consensual identification, search and seizure actions might be undertaken by security authorised Defence Force members or, by Defence security screening employees if it is not reasonably practical for a security authorised Defence Force member to do so, during higher SAFEBASE alert levels, in response to a specific security incident or at any other time if warranted by specific circumstances.

Note: Further information on the application of the identification search and seizure regime at different SAFEBASE levels is contained in DSPF Principle 83 - SAFEBASE.

4. The Base Support Manager (BSM) and the Senior Australian Defence Force Officer (SADFO) are jointly responsible for providing a recommendation to the DG ESD on the implementation of the identification search and seizure regime at their base. This recommendation should be based on a security risk assessment of the site. The planned operation of the identification search and seizure regime should be addressed in the Base Security Plan.

5. For Offences and Penalties that relate to this DSPF part refer to Annex B to DSPF Control 76.1 - *Offences and Penalties*.

Defence Security Officials

6. The [Defence Act 1903 \(Cth\)](#) (*the Act*) establishes three categories of DSO that are authorised to exercise some or all of the powers conferred by Part VIA of the Act. A DSO may be:

- a. a contracted Defence security guard (Contractor);
- b. a Defence security screening employee (Australian Public Service (APS) Employee); or
- c. a security authorised member of the Defence Force.

Note: In accordance with the [Defence Act 1903](#), a Security Officer cannot exercise any of the identification, search and seizure powers unless they have been authorised to do so by the Minister as a DSO.

7. Table 1 shows the relationship between the various terms used to describe a DSO.

Table 1 – Categories of Defence Security Officials

Contracted Defence Security Guard	Special Defence Security Official (SDSO)	
	Defence Security Screening Employee	Security Authorised Member of the Defence Force: • Identification and Search Warden • Military Working Dog Handler • Armed Security Warden

8. The powers that can be exercised by each category of DSO are summarised at Annex E to DSPF Control 76.1 - *Summary of Defence Security Officials' Powers*.

Contracted Defence Security Guard

9. A contracted Defence security guard is a contractor, subcontractor or their employee, who provides security services at Defence premises under a contract with the Commonwealth, and has been authorised by the Minister, by written instrument, to be a contracted Defence security guard. The Minister will only authorise as contracted Defence security guards, individuals who have met a standard of security training and qualification requirements as determined by the Minister, or his delegate, in a legislative instrument. This training should include scenario based training to provide guidance on the exercise of powers by contracted Defence security guards. For further information on training and qualification requirements refer to DSPF Principle 75 – *Contracted Security Guards*, and Annex D to DSPF Control 76.1 *Defence Security Officials – Training and Qualification Requirements*.

10. Under the [Defence Act 1903](#) (refer to Part VIA, Division 3) and this DSPF part, contracted Defence security guards are only authorised to:

- request or require evidence of a person's identification and authority to pass an access control point or be on Defence premises;
- conduct consensual limited searches of a person (including items in the person's possession);
- conduct consensual searches of vehicles; and
- in specified circumstances, restrain and detain a person for the purposes of placing them in the custody of a Federal, State or Territory Police officer.

Note: All references to contracted Defence security guards in this DSPF part refer to contracted security guards who have been authorised by the Minister as contracted Defence security guards under the Act. Security guards, who work at Defence sites that have not been authorised by the Minister, cannot exercise the powers conferred by Part VIA of the Act.

Defence Security Screening Employees

11. A Defence security screening employee is an APS employee of the Department of Defence who has been authorised by the Minister, by written instrument, to be a Defence security screening employee. The Minister will only authorise as Defence security screening employees, APS employees who have met a standard of security training and qualification requirements as determined by the Minister, or his delegate, in a legislative instrument. This training should include scenario based training to provide guidance on the exercise of powers by Defence security screening employees¹.
12. Defence security screening employees must have volunteered to undertake the additional responsibilities and risks associated with this role, or occupy a position where these additional responsibilities are included in the duty statement.
13. Under the [Defence Act 1903](#) (refer to Part VIA, Division 3) and this DSPF part, Defence security screening employees are authorised to:
- a. request evidence of a person's identification and authority to pass an access control point or be on Defence premises;
 - b. conduct consensual limited searches of a person (including items in the person's possession);
 - c. conduct consensual searches of vehicles; and
 - d. in specified circumstances, restrain and detain a person for the purposes of placing them in the custody of a Federal, State or Territory Police officer.
14. In circumstances where it is not reasonably practicable for a security authorised member of the Defence Force to do so, Defence security screening employees are further authorised under the [Defence Act 1903](#) (refer to Part VIA, Divisions 4 and 5) to:
- a. require evidence of a person's identification and authority to be on Defence premises;

¹ For further information on Training and Qualification requirements refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

- b. conduct non-consensual searches of a person (including items in the person's possession) and non-consensual vehicle searches; and
- c. in specified circumstances:
 - (1) request a person to leave the premises and, if they refuse, remove the person from the premises with reasonable force if required;
 - (2) restrain and detain a person (applying reasonable force) for the purposes of placing them in the custody of a Federal, State or Territory Police officer; and
 - (3) seize items that are a threat to safety or relate to a criminal offence for the purpose of transferring custody to the Australian Federal Police (AFP) or Police Force of a State or Territory.

Security Authorised Member of the Defence Force

15. A security authorised member of the Defence Force is an Australian Defence Force (ADF) member who has been authorised by the Minister, by written instrument, to be a security authorised member of the Defence Force. The Minister will only authorise as security authorised members of the Defence Force, ADF members who have met a standard of security training and qualification requirements as determined by the Minister, or his delegate, in a legislative instrument. This training should include scenario based training to provide guidance on the exercise of powers by security authorised members of the Defence Force.

16. Different training and qualification requirements apply to specialised sub-categories of security authorised Defence Force members, for example Identification and Search Wardens (ISW), Military Working Dog Handlers and Armed Security Wardens².

Note: The exercise of powers by Armed Security Wardens³ is limited to circumstances where an attack on Defence premises is imminent or occurring. For further guidance on Armed Security Wardens refer to DSPF Principle 83 - SAFEBASE.

² For Further information on Training and qualification requirements refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

³ Armed Security Wardens are part of the [Enhanced Self-Defence Capability](#) as managed by the Chief of Army.

17. Under the [Defence Act 1903](#) (refer to Part VIA Divisions 3, 4 and 5) and this DSPF part, security authorised members of the Defence Force, who are trained and qualified as ISW, are authorised to:

- a. request or require evidence of a person's identification and authority to pass an access control point or be on Defence premises;
- b. conduct consensual limited searches of a person (including items in the person's possession) and consensual vehicle searches;
- c. conduct non-consensual searches of a person (including items in the person's possession) and non-consensual vehicle searches; and
- d. in specified circumstances:
 - (1) request a person to leave the premises and, if they refuse, remove the person from the premises using reasonable force;
 - (2) restrain and detain (applying reasonable force when required) a person for the purposes of placing them in the custody of a Federal, State or Territory Police officer to exercise their powers of arrest;
 - (3) seize items that are a threat to safety or relate to a criminal offence for the purpose of transferring custody to the AFP or Police Force of a State or Territory; and
 - (4) take action to make seized items safe or prevent their use.

Authorisation of Defence Security Officials

18. In accordance with the [Defence Act 1903](#), before exercising any powers provided under Part VIA, a DSO **must**:

- a. complete the specified training and hold the requisite qualifications associated with his/her category (or sub-category) of security official as determined by the Minister, or the Minister's delegate, in a legislative instrument⁴;
- b. be authorised to be a contracted Defence security guard, a Defence security screening employee or a security authorised Defence Force member by the Minister; and

⁴ For Further information on Training and qualifications refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

- c. be issued with an identity card by the Secretary or the Secretary's delegate.

19. A DSO may have their authority to exercise powers under the [Defence Act 1903](#) temporarily revoked, for example, if the DSO is being investigated in relation to the possible commission of an offence under the [Defence Act 1903](#). Refer to Annex B to DSPF Control 76.1 - *Offences and Penalties* for further information on offences. In these circumstances, the DSO is required to return their identity card to an authorised delegate until the matter is resolved within 7 days of being notified. Refer to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)* for further information.

Identification of Defence Security Officials

20. In accordance with the [Defence Act 1903](#), Part VIA section 71E, Defence Security Officials (DSO) **must** carry an identity card at all times when performing functions or exercising their powers under Part VIA. In addition, under Section 72B of Part VIA of the Act, a DSO **must** produce this card for inspection by a person before:

- a. requesting or requiring the person to provide evidence of their identification or authority to pass an access control point or be on Defence premises;
- b. requesting a consensual limited search of a person (including items in the person's possession) or a consensual search of a vehicle apparently under the person's control;
- c. requiring a non-consensual search of the person (including items in the person's possession) or a vehicle apparently under the person's control; or
- d. restraining, detaining or removing the person from Defence premises.

Note: *If a SDSO reasonably believes that a person constitutes a threat to safety such that complying with this requirement, prior to conducting a non-consensual search, places the safety of the official and others at risk, they may temporarily delay presenting their identity card. For example, this might occur if the official reasonably believes the person is carrying a concealed weapon. In these circumstances, after the immediate threat to safety has been resolved, the official is required to produce their identity card for inspection by the person and inform the person of the effect of hindering or obstructing the search⁵.*

⁵ Further information on the production and management of identity cards for DSOs refer to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)*.

Identification Powers

21. A DSO is authorised to request evidence of a person's identification or authority to be on Defence premises, when:
- a. a person is entering or exiting Defence premises, or part of Defence premises, through an access control point; or
 - b. a person is on Defence premises (i.e. at areas other than an access control point) and the DSO reasonably believes that the person is not authorised to be there.
22. Further, a SDSO may require a person to present evidence of their identification or authority to be on Defence premises, when:
- a. a person is entering or exiting Defence premises, or part of Defence premises, through an access control point; or
 - b. a person is on Defence premises (i.e. at areas other than an access control point) and the SDSO reasonably believes the person:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises.
23. When requesting or requiring a person to produce identification, all DSOs are required to produce their identity card for inspection and inform the person of the consequences of refusing to comply with the request or requirement.

Consensual Identification Powers

Consensual Identification of a Person at Access Control Points

24. Under the [Defence Act 1903](#) Part VIA section 71H, a DSO may request a person who is about to pass an access control point to provide evidence of their identity and authority to pass the access control point.
25. Further, a DSO may refuse to allow a person to pass an access control point and, if on Defence premises, restrain and detain the person, if:
- a. the person refuses the identification request or fails to provide evidence that satisfies the DSO; or

- b. as a result of complying with the request, the DSO reasonably believes that the person:
 - (1) is not authorised to pass the access control point;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to, the premises.

26. If the circumstances described above occur when a person is seeking to enter a Defence premises, or a part of the premises, a DSO is to refuse the person entry in accordance with Defence's policy on access control. For further information refer to DSPF Principle 74 - *Access Control*.

Consensual Identification of a person on Defence Premises

27. Under the [Defence Act 1903](#) Part VIA section 71K a DSO may request a person, who is on Defence premises (ie at areas other than access control points), and who the DSO reasonably believes is not authorised to be there, to provide evidence of their identity and authority to be on the premises.

Example: It would be reasonable for a DSO to conclude that a person on Defence premises, who is not visibly wearing a Defence access or identity card, is not authorised to be there. As a result, the official would be entitled to stop the person and request that they provide evidence of their identification and authority to be on the premises.

28. Further, a DSO may restrain and detain a person, if:
- a. the person refuses the identification request or fails to provide evidence that satisfies the DSO; or
 - b. as a result of complying with the request, the DSO reasonably believes that the person:
 - (1) is not authorised to be on the premises;
 - (2) threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises.

Refusal to Comply with a Consensual Identification Request

29. A person's refusal or failure to comply with a request from a DSO to provide evidence of their identity and authority to pass an access control point or be on Defence premises does not constitute an offence. However, in these circumstances, the DSO is to deny the person entry to Defence premises and, if the person is already on the premises, may restrain and detain the person for the purposes of placing them into the custody of a Federal, State or Territory Police officer for

trespass or other criminal offences. The DSO is to contact police as soon as practicable after a person has been restrained and detained. The authority to restrain and detain in these circumstances is outlined in this part. For further information on restrain and detain powers refer to "*Restrain and Detain Powers*" in this part.

30. Under the [Defence Act 1903](#) Part VIA section 71T, if a SDSO reasonably believes that a person, who has been restrained and detained in the circumstances outlined above, constitutes a threat to the safety of persons on Defence premises, they may conduct a non-consensual identification and search of the person while awaiting the arrival of police.

Non-consensual Identification Powers

31. Under the [Defence Act 1903](#) Part VIA section 71Y, a SDSO may stop and detain a person or vehicle for the purposes of requiring a person to present evidence of their identification or authority to be on Defence premises.

Non-consensual Identification of a Person at Access Control Points

32. Under the [Defence Act 1903](#) Part VIA section 71R, a SDSO may require a person who is about to pass an access control point to provide evidence of their identity and authority to pass the access control point.

33. Further, the SDSO may refuse to allow a person to pass the access control point, if:

- a. the person refuses the identification requirement or fails to provide evidence that satisfies the DSO; or
- b. as a result of complying with the requirement, the DSO reasonably believes that the person:
 - (1) is not authorised to pass the access control point;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises.

34. If the SDSO refuses to allow a person to pass an access control point and the person is on Defence premises, the SDSO may:

- a. restrain and detain the person, or
- b. request the person to leave the premises and, if he or she refuses, remove the person from the premises.

35. If the circumstances described above occur when a person is seeking entry to Defence premises, or part of the premises, an SDSO is to refuse the person entry in accordance with Defence's policy on access control and identity management⁶.

Non-consensual Identification of a Person on Defence Premises

36. Under the [Defence Act 1903](#) Part VIA section 71T, a SDSO may require a person, who is on Defence premises (i.e. at areas other than access control points), to provide evidence of their identity and authority to be on the premises, if the official reasonably believes that the person:

- a. is not authorised to be on the premises;
- b. constitutes a threat to the safety of people on the premises; or
- c. has or may commit a criminal offence on, or in relation to the premises.

Example: It would be reasonable for a SDSO to conclude that a person on Defence premises who is not visibly wearing a Defence access or identity card is not authorised to be there. As a result, the official would be entitled to stop the person and require that they provide evidence of their identification and authority to be on the premises.

37. Further, a SDSO may restrain and detain a person, or request a person to leave the premises and, if he or she refuses, remove the person from the premises (reasonable force may be applied), if:

- a. the person refuses the identification requirement or fails to provide evidence that satisfies the DSO; or
- b. as a result of complying with the request, the SDSO reasonably believes the person:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises.

Search Powers

38. A DSO is authorised to conduct a consensual limited search of a person (including items in the person's possession) and a consensual search of a vehicle

⁶ For further information on identity management refer to the DSPF Principle 74 - Access Control.

(including things in the vehicle), when a person or vehicle is entering or exiting Defence premises, or part of Defence premises, through an access control point.

39. Further, a SDSO is authorised to conduct a non-consensual search of a person (including items in the person's possession) or a vehicle (including things in the vehicle), when:

- a. a person or vehicle is about to pass an access control point that is located on Defence premises; or
- b. a person or vehicle is on Defence premises (i.e. at areas other than an access control point) and the SDSO reasonably believes the person or vehicle:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises;
 - (3) in the case of a person, has or may commit a criminal offence on, or in relation to the premises; or
 - (4) in the case of a vehicle, relates to a criminal offence that has or may be committed on, or in relation to the premises.

40. At declared explosive ordnance depots, contracted Defence securityguards are further authorised to conduct a consensual limited search of a person and a consensual search of a vehicle, if the person or vehicle is located anywhere on the depot, not just at the access points.⁷ DSO are not authorised to undertake consensual or non-consensual searches of people, items or vehicles on Defence accommodation.

Note: *This restriction on the exercise of consensual and non-consensual search powers applies even if the accommodation is located within Defence premises.*

41. Prior to exercising their powers of search, a DSO is required to produce his or her identity card for inspection and inform the person of the consequences of refusing to comply with a request for a consensual search or a requirement to submit to a non-consensual search.

⁷ For further information on declared explosive ordnance depot special search provisions refer to Annex G to DSPF Control 74.1 - *Special Search Provisions for Declared Explosive Ordnance Depots.*

Note: If an SDSO reasonably believes that a person constitutes a threat to safety such that complying with this requirement, prior to conducting a non-consensual search, places the safety of the official and others at risk, they may temporarily delay presenting their identity card. For example, this might occur if the official reasonably believes the person is carrying a concealed weapon. In these circumstances, after the immediate threat to safety has been resolved, the official is required to produce his or her identity card for inspection by the person and inform the person of the effect of hindering or obstructing the search.

42. Contracted Defence security guards must conduct consensual limited searches of people and consensual searches of vehicles in accordance with the procedures detailed in their assignment instructions.⁸

43. SDSO must conduct all consensual and non-consensual searches of people and vehicles in accordance with the training and qualification requirements applicable to their category of DSO.

Consensual Search Powers

Consensual Searches at Access Points

44. Under the [Defence Act 1903](#) Part VIA section 71H, a DSO may request a person, who is about to pass an access control point, to undergo a consensual limited search of their person, including items in their possession.

45. Under the [Defence Act 1903](#) Part VIA section 71J, a DSO may request a person, who is apparently in control of a vehicle that is about to pass an access control point, to permit a consensual search of the vehicle, including things in the vehicle.

46. Further, a DSO may refuse to allow a person or vehicle to pass an access control point and, if on Defence premises, restrain and detain the person and any other people in the vehicle, if:

- a. the person refuses the consensual search request; or
- b. as a result of complying with the request, the DSO reasonably believes that the person or the vehicle (including a thing in the vehicle):
 - (1) is not authorised to pass the access control point;

⁸ For further information on assignment instructions for guards refer to DSPF Principle 75 - *Contracted Security Guards*.

- (2) constitutes a threat to the safety of people on the premises;
- (3) in the case of a person, has or may commit a criminal offence on, or in relation to the premises; or
- (4) in the case of a vehicle, relates to a criminal offence that has or may be committed on, or in relation to the premises.

47. If the circumstances described within paragraph 46 of this part - “*Consensual Search Powers*” occurs when a person or vehicle is seeking entry to a Defence premise, or a part of the premises, a DSO is to refuse the person entry.

Note: *At declared explosive ordnance depots, contracted Defence security guards are further authorised to conduct a consensual limited search of a person and a consensual search of a vehicle, if the person or vehicle is located anywhere on the depot, not just at the access points⁹.*

Refusal to Comply with a Consensual Search Request

48. A person’s refusal to comply with a consensual search request from a DSO at an access control point does not constitute an offence. However, in these circumstances, the DSO is to deny the person entry to Defence premises and, if the person is already on the premises, may restrain and detain the person for the purposes of placing them in Federal, State or Territory police officer custody. The DSO must contact police as soon as practicable after the person has been restrained and detained. The authority to restrain and detain in these circumstances is outlined in paragraphs 44 to 46 of this part - “*Consensual Search Powers*”.¹⁰

49. Under the [Defence Act 1903](#) Part VIA section 71T, if an SDSO reasonably believes that a person, who has been restrained and detained in the circumstances outlined above, constitutes a threat to the safety of persons on Defence premises, they may conduct a non-consensual search of the person while awaiting the arrival of police.

Non-consensual Search Powers

50. Under the [Defence Act 1903](#) Part VIA section 71Y, a SDSO may stop and detain a person or vehicle for the purposes of conducting a non-consensual search of a person or vehicle.

⁹ For further information on Special Search Provisions for Declared Explosive Ordnance Depots refer to Annex G to DSPF Control 74.1 - *Special Search Provisions for Declared Explosive Ordnance Depots*.

¹⁰ For further information on restrain and detain powers refer to “*Restrain and Detain Powers*” within this DSPF part at paragraphs 110 to 120.

Non-consensual Search of a Person at Access Control Points

51. Under the [Defence Act 1903](#) Part VIA section 71R, a SDSO may require a person, who is about to pass an access control point that is on Defence premises, to submit to a non-consensual search of their person, including items in their possession. This may be required when a person is exiting Defence premises through an access control point, or when entering or exiting an area within the premises through an internal access control point.

Note: *If the access control point is located at the external perimeter of the Defence base or site, a SDSO cannot require a person to undergo a non-consensual search on entry. In these circumstances, a DSO can request the person to undergo a consensual limited search.¹¹*

52. Further, the SDSO may refuse to allow a person to pass the access control point, if:

- a. the person hinders or obstructs the non-consensual search; or
- b. as a result of the search, the SDSO reasonably believes that the person:
 - (1) is not authorised to pass the access control point;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises.

53. If the SDSO refuses to allow a person to pass an access control point, the SDSO may:

- a. restrain and detain the person; or
- b. request the person to leave the premises and, if he or she refuses, remove the person from the premises (reasonable force may be used).

54. If the circumstances described within paragraph 53 of this part - “Access Control Points”, occurs when a person is seeking entry to an area within the Defence premises through an access control point (i.e. other than an access control point located at the external perimeter of a base), an SDSO should refuse the person entry.

¹¹ For further information on consensual limited search refer to “Consensual Search Powers” within this DSPF part at paragraphs 44 to 46.

Non-consensual Search of a Vehicle at Access Control Points

55. Under the [Defence Act 1903](#) Part VIA section 71S, a SDSO may require a person, who is apparently in control of a vehicle that is about to pass an access control point that is located on Defence premises, to permit a non-consensual search of the vehicle, including things in the vehicle. This may be required when the vehicle is exiting Defence premises through an access control point, or when the vehicle is entering or exiting an area within the premises through an access control point.

Note: *If the access control point is located at the external perimeter of the Defence base or site, a SDSO cannot require a person to submit to a non-consensual vehicle search on entry. In these circumstances, a DSO can request the person to permit a consensual vehicle search¹².*

56. The SDSO may refuse to allow a vehicle to pass the access control point, if:

- a. a person hinders or obstructs the non-consensual search; or
- b. as a result of the search, the SDSO reasonably believes that the vehicle (including a thing in the vehicle):
 - (1) is not authorised to pass the access control point;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) relates to a criminal offence that has or may be committed on, or in relation to the premises.

57. If the SDSO refuses to allow a vehicle to pass an access control point, the SDSO may restrain and detain any people in the vehicle.

Non-consensual Search of a Person on Defence Premises

58. Under the [Defence Act 1903](#) Part VIA section 71T, a SDSO may require a person, who is on Defence premises (i.e. at areas other than access control points), to submit to a non-consensual search of their person, including items in their possession, if the official reasonably believes that the person:

- a. is not authorised to be on the premises;
- b. constitutes a threat to the safety of people on the premises; or
- c. has or may commit a criminal offence on, or in relation to the premises.

¹² For further information on non-consensual and consensual search of vehicles refer to “*Consensual Search Powers*” within this DSPF part at paragraphs 44 to 46.

59. Further, a SDSO may restrain and detain a person, or request a person to leave the premises and, if he or she refuses, remove the person from the premises, if:

- a. the person hinders or obstructs the non-consensual search; or
- b. as a result of the search, the SDSO reasonably believes that the person:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises.

Non-consensual Search of a Vehicle on Defence Premises

60. Under the [Defence Act 1903](#) Part VIA section 71U, a SDSO may require a person, who is apparently in control of a vehicle that is located on the premises, to permit a non-consensual search of the vehicle, including things in the vehicle, if the official reasonably believes that the vehicle:

- a. is not authorised to be on the premises;
- b. constitutes a threat to the safety of people on the premises; or
- c. relates to a criminal offence that has or may be committed on, or in relation to the premises.

61. Further, a SDSO may restrain and detain any person in the vehicle, if:

- a. a person hinders or obstructs the non-consensual search; or
- b. as a result of the search, the SDSO reasonably believes that the vehicle:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) relates to a criminal offence that has or may be committed on, or in relation to the premises.

Exemptions to Search Regime

62. It is in Defence's interests to facilitate the lawful activities of other officials when undertaking their statutory functions or responding to incidents on Defence premises. This might include:

- a. civilian law enforcement personnel (including Customs and Border Protection Service Officers);

- b. emergency services personnel; and
 - c. other Commonwealth government officials (e.g. Comcare inspectors).
63. Such officials are provided with a limited exemption from the search powers when performing their statutory duties. That is, prior to requesting the official undergo a consensual limited search of their person or vehicle, the DSO must reasonably believe that the official:
- a. constitutes a threat to the safety of people on the premises; or
 - b. has or may commit a criminal offence on, or in relation to, the premises.
64. If, in the circumstances described within this DSPF part “Exemption To Search Regime” in paragraph 63 occurs and the official refuses to provide their consent, they must be treated the same as any other person who has not provided their consent.
65. A full exemption to the identification search and seizure regime must be provided to a person who has diplomatic status and who is accompanied by a Defence Force member or civilian employee of the Department.
66. The Base Commander, BSM or SADFO may determine whether other exemptions are warranted in specific situations.

Compensation

67. If an item is damaged as a result of a search and no criminal proceedings are instituted in relation to the item, or it is found not to have been involved in the commission of a criminal offence, compensation may be payable to the owner of the item.
68. Refer to [Defence Legal](#) for further information on compensation matters.

Seizure

69. Under the [Defence Act 1903](#) Part VIA section 72, a SDSO may seize an item that is on Defence premises, including a vehicle or an unattended item, or an item that is found as a result of a consensual or non-consensual search, if the official reasonably believes that it may:
- a. constitute a threat to the safety of people on the premises; or
 - b. relate to a criminal offence that has or may be committed on, or in relation to the premises.
70. Where the seizure relates to a possible security threat, a security authorised member of the Defence Force may take any action that is reasonable and necessary

to make the seized item safe or prevent its use, for example, unloading a firearm. In respect of a suspicious item that is left unattended on the premises, this action could include a non-consensual search of the item to establish whether it constitutes a threat to the safety of people on the premises¹³.

71. If a SDSO reasonably believes a seized item has been used or involved in the commission of a criminal offence, the official is required to hand the item over to the police at the earliest practicable time. This requirement, however, does not apply if action is necessary to make the item safe or prevent its use, and this action prevents the item from being provided to the police.

72. In the circumstances outlined above, the seized item cannot be transferred to the custody of a Protective Security Officer of the AFP. Any item believed to be involved in a criminal offence must be carefully handled in accordance with correct evidence management procedures to ensure potential evidential material is not inadvertently contaminated¹⁴.

73. A SDSO should provide a person with a receipt for a seized item, if it is practicable to do so.

74. In the event that it is established that the seized item has not been used or otherwise involved in the commission of an offence, and as such there is no requirement to provide the item to the police, the SDSO should return the item to the person within seven days if it is practicable to do so or, if not, provide it to police.

Note: A seized item that cannot be returned to the person within seven days cannot be handed over to a Protective Service Officer of the AFP.

Additional Considerations

Use of Reasonable and Necessary Force

75. Under the [Defence Act 1903](#) section 72G, when exercising their powers under Part VIA, a DSO:

- a. should only use such force against a person or thing as is reasonable and necessary; and

¹³ Refer to extant emergency management procedures for further guidance in dealing with potentially threatening items.

¹⁴ Handling evidential information or items must be in accordance with training and qualification requirements applicable to their category of DSO.

- b. should not subject a person to greater indignity than is reasonable and necessary.

76. Reasonable force is regarded to be the minimum force reasonably necessary in the circumstances of a particular situation. That is, the use of force must be limited, in its intensity and duration, to that which is required to resolve the situation.

77. In potentially difficult situations, the DSO must attempt to reduce tension and resolve incidents without force or with a minimum use of force. The level of force must be graduated and appropriate to the level of threat faced.

78. If a DSO has used force against a person when exercising their powers under Part VIA of the [Defence Act 1903](#), the official should ensure that the person receives medical attention if required.

79. In all cases where a DSO uses force against a person, he or she is to, as soon as practicable; submit a report setting out the full details of the force used and the circumstances in which the force was applied¹⁵.

80. DSO may touch, as appropriate, a vehicle or item, or anything in a vehicle or item, in order to undertake a search.

Limit on Use of Force or Force Involving Death or Injury

81. The Australian Federal Police (AFP), or State/Territory police as applicable, has primacy during any attack on a Defence base that is imminent or in progress.

82. Under the [Defence Act 1903](#) Part VIA section 72G, a contracted Defence security guard or a Defence security screening employee should not use force against a person, or do anything that is likely to cause death or grievous bodily harm.

Note: Per section 72H, the use of force involving death or grievous bodily harm is strictly limited to Armed Security Wardens in circumstances where an attack on Defence premises, or people on Defence premises is imminent or occurring¹⁶.

Note: In accordance with the [Defence Act 1903](#) Part VIA section 72S, the Defence Act 1903 does not, by implication, limit the exercise of powers or rights of any person under the Defence Act 1903 or any other law. This includes the right to use force in defence of themselves or others.

¹⁵ Further information on reporting requirements refer to “Reporting Requirements” within this DSPF part at paragraphs 129 to 136.

¹⁶ For Further information on Armed Security Wardens refer to DSPF Principle 83 – *SAFE*BASE.

83. A DSO should not use force that is unwarranted or disproportionate to the situation. This includes situations where force has been used and:

- a. no force was required;
- b. more force was applied than was necessary;
- c. the use of force continued after the necessity for it had ceased; or
- d. force was knowingly and wrongfully used.

84. DSO may be criminally prosecuted for unreasonable use of force.

Exercise of Powers in relation to Protests etc.

85. Under the [Defence Act 1903](#) Part VIA section 72L, a DSO should not use their powers to stop or restrict any protest, dissent, assembly or industrial action, unless there is a reasonable likelihood of:

- a. death or serious injury; or
- b. the commission of a criminal offence.

Person to be Informed of Offence

86. Under the [Defence Act 1903](#) Part VIA section 72C if a DSO exercises their powers on the basis of a reasonable belief that the person has or may commit a criminal offence, the DSO is required to inform the person of the substance of the offence.

Note: *The language used may be general, rather than of a precise or technical nature.*

87. This requirement does not apply, however, if the person should, in the circumstances, know the substance of the offence or, through their actions, makes it impracticable for the official to inform the person of the offence.

Number of Defence Security Officials

88. Two DSO should be present during all searches to avoid any evidential dispute. In exceptional circumstances, such as a perceived threat to security or safety, a DSO may undertake a search without another DSO present.

Privacy

89. Where practicable, a person should be provided with the option of undergoing a consensual limited search or a non-consensual search of their person,

including items in their possession, in a private area. Privacy could be provided by a screen or temporary structure.

90. In order to protect the privacy of the person, DSO are not to record or discuss anything of a private or personal nature observed or discovered during a search unless it is directly relevant to the identified reporting requirements or a perceived security or safety risk.

Vehicles

91. If possible, vehicles should be directed to vehicle search bays (if available) for the conduct of a search to ensure that routine vehicular traffic is not unnecessarily impeded.

Gender/Culture

92. Under the [Defence Act 1903](#) Part VIA Section 72D requires that a consensual limited search or non-consensual search of a person should, if practicable, be conducted by a DSO of the same gender as the person being searched. If a person is uncomfortable undergoing a search of their person, including items in their possession, by an official of the opposite gender they may choose to have another person (e.g. a colleague) present during the process. That person must be able to attend the search site in a timely manner.

93. All searches should be conducted in a culturally sensitive manner.

Security Construction and Equipment Committee (SCEC)

94. The contents of briefcases used for carrying classified material, are not exempt from being searched. If it is considered necessary to search a SCEC endorsed briefcase:

- a. the briefcase can be opened and the contents given a cursory inspection to verify the existence of documented authorisation to carry the material (e.g. an [XC019 or XC051 form](#)) and to ensure that the material has been properly protected and does not appear to have been subject to tampering;
- b. the person carrying the briefcase can be asked to move papers and files around, but files must not be opened; and
- c. classified material in a SCEC endorsed briefcase can only be seized by a SDSO.

Use of Equipment to Conduct Searches or Examine Items

95. Under the [Defence Act 1903](#) Part VIA section 72E, a DSO may use electronic and other devices, and obtain expert assistance, for the purposes of

conducting a search of a person, item or vehicle or determining whether an item may be seized.

Example: This may include, but is not limited to, the use of metal detectors, x-ray equipment, arthroscopic camera devices (to examine spaces that are confined or difficult to access such as areas of a vehicle engine bay), explosive residue equipment, chemical sniffers or other search devices.

96. Further, the DSO may use equipment to gain access to data stored on items, for example data on laptops, mobile phones and thumb drives.

97. A search of an item should cease as soon as it has been established that there is a valid basis upon which to seize the item (e.g the discovery of a classified document on a laptop) and it has been determined that there is no immediate safety risk posed by the item/vehicle/person.

98. A DSO may move an item that is on Defence premises to another part of the premises for examination or processing, if the official suspects on reasonable grounds that the item:

- a. constitutes a threat to the safety of people on the premises; or
- b. relates to a criminal offence that has or may be committed on, or in relation to the premises.

99. Prior to utilising equipment to assist a search, a DSO must have completed training and maintain proficiency on that equipment.

Assistance to Defence Security Officials

100. Under the [Defence Act 1903](#) Part VIA section 72N, when exercising their powers, a DSO may be assisted by other people if it is reasonable and necessary to do so, to:

- a. conduct a consensual search of a vehicle at an access control point;
- b. conduct a consensual search of a vehicle on a declared explosive ordnance depot;
- c. conduct a non-consensual search of a vehicle about to pass an access control point that is located on Defence premises;
- d. conduct a non-consensual search of a vehicle located on Defence premises (ie at areas other than access control points);
- e. use equipment to undertake a search of a person, item or vehicle; or
- f. move things on Defence premises.

Example: Assistance may be required to operate a forklift to unload a vessel, vehicle or aircraft so that a thorough search may be properly conducted by a DSO. Expert assistance may also be sought to use technical equipment to process an item.

Note: It would not be reasonable for a DSO to seek assistance to exercise powers that they have the capability, training, authorisation and physical capacity to exercise in their own capacity as a DSO.

101. A person assisting a DSO may exercise the official's powers, but only in accordance with the directions of the DSO. Any person assisting a DSO who acts outside of the direction of a DSO may be individually liable for their actions.

102. Powers that are exercised by a person assisting a DSO are taken to have been exercised by the official. The DSO is liable for any misuse of power by a person assisting them to the extent that the person is following the direction of a DSO. That is, a DSO is not liable for any actions undertaken by a person assisting them if the person acted outside of the direction of the DSO.

Use of Military Working Dogs

103. Under the [Defence Act 1903](#) Part VIA section 72M, a security authorised member of the Defence Force may, if the member considers it is reasonably necessary, use a military working dog to:

- a. assist a DSO to conduct a search or a limited search;
- b. assist a DSO to restrain and detain a person, or remove a person from Defence premises;
- c. assist an ADF member to arrest a person for trespass under section 72P of *the Act*; or
- d. assist a DSO to perform a function or power under Part VIA of *the Act*.

104. Use of military working dogs is strictly limited to security authorised Defence Force members, who have completed the relevant training and qualification requirements as determined by the Minister for military working dog handlers. For further information on the training and qualification requirements refer Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

105. At all times, a military working dog handler should only use such force as is reasonable and necessary and direct their military working dogs in such a manner as to prevent unreasonable injury to people or damage to property

Move Items

106. A DSO may move an item (including a vehicle) that has been left unattended on Defence premises as a result of, or in connection with the exercise of a power under the [Defence Act 1903](#) Part VIA, if the DSO reasonably believes this action is necessary or desirable. For example, when a vehicle has been left unattended, after the driver has been restrained and detained, and the vehicle is impeding the normal operations of the premises or poses a traffic hazard.

107. If there is any suspicion that a vehicle or item poses a significant threat to safety, for example a suspicion that it may contain an improvised explosive device, a DSO must not attempt to move it and must contact the police immediately.

Storage

108. Where practicable, safe and secure storage facilities should be made available outside of Defence premises to allow people to securely store items that they do not want searched prior to entry. A DSO must ensure that people entering Defence premises are aware of the availability of storage facilities.

Signage

109. Notices should be prominently displayed at the entrance to all Defence bases and sites, advising people of the consensual and non-consensual identification and search regime and notifying that offences may apply for failing to comply with non-consensual identification and search requirements.

Notices should be worded as follows:

“You are about to enter Defence premises.

Unauthorised entry to these premises is an offence carrying a significant maximum monetary penalty ([Defence Act 1903](#) Part VIA, section 72P).

You may be asked to:

- provide identification or evidence of your authority to be on these premises;
or
- undergo a search of your person or permit a search of things in your possession (including vehicle).

If you do not consent, you may be refused entry to these premises or, if already on the premises, denied free exit and detained on the premises.

Further, a SDSO may:

- require that you provide identification or evidence of your authority to be on the premises; or
- conduct a non-consensual search of your person and things in your possession (including vehicle).

It is an offence carrying a significant maximum monetary penalty if, while on the premises, you:

- fail to provide evidence of your identity and authority to be on these premises if required to do so by a SDSO (Defence Act 1903 Part VIA section 71V); or
- hinder or obstruct a SDSO from performing a non-consensual search of your person and things in your possession, including a vehicle ([Defence Act 1903](#) Part VIA, section 71W).

[Defence Act 1903, Part VIA, Security of Defence Premises"](#)

Note: There are specific signage requirements applying to declared explosive ordnance depots¹⁷.

Restrain and Detain Powers

110. Under Part VIA of the [Defence Act 1903](#) and this DSPF part, DSOs are authorised to restrain and detain people to support the enforcement of the identification, search and seizure regime. The power to restrain and detain a person is authorised in specific circumstances only and, under the [Defence Act 1903](#) Part VIA section 72J, is solely for the purposes of placing the person in a Federal, State or Territory police officer's custody at the earliest practicable time.

Note: To restrain and detain a person does not necessarily require that they are physically restricted. A verbal direction that a person must remain on Defence premises until the arrival of police constitutes an exercise of the power to restrain and detain.

¹⁷ For further information on declared explosive ordnance depot Refer to Annex G to DSPF Control 76.1 - *Special Search Provisions for Declared Explosive Ordnance Depots*.

111. The specific circumstances in which a DSO may restrain and detain a person are discussed in detail in the earlier sections of this DSPF part on Identification Powers and Search Powers. In summary, under the [Defence Act 1903](#) Part VIA, a DSO may restrain and detain a person if the person is on Defence premises and either:

- a. refuses an identification request or requirement;
- b. fails to provide evidence that satisfies the DSO in response to an identification request or requirement;
- c. refuses a request for a consensual person or vehicle search;
- d. hinders or obstructs a non-consensual person or vehicle search;
- e. is an occupant in a vehicle and the person apparently in control of the vehicle refuses a consensual vehicle search;
- f. is an occupant in a vehicle and a person hinders and obstructs a non-consensual search of the vehicle;
- g. complies with a consensual or non-consensual identification or search action and, as a result, the DSO reasonably believes the person:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) has or may commit a criminal offence on, or in relation to the premises; or
- h. is an occupant in a vehicle and, as a result of a vehicle search, the DSO reasonably believes the vehicle or anything in it:
 - (1) is not authorised to be on the premises;
 - (2) constitutes a threat to the safety of people on the premises; or
 - (3) relates to a criminal offence that has or may be committed on, or in relation to the premises.

Note: A DSO is not permitted to restrain and detain a person who has yet to enter a Defence base or site through the access control point that is located at the external perimeter of that base or site. If the circumstances detailed at sub-paragraphs b to h occur when a person is seeking to enter a Defence base or site through an access control point that is located at the external perimeter, the DSO is only authorised to refuse the person entry to the base or site. If a person who has been refused entry to Defence premises continues to loiter near the premises or causes some other disturbance, the police should be contacted to deal with the situation.

112. A DSO should immediately contact the police in every instance where they have restrained and detained a person.

113. Under the [Defence Act 1903](#) Part VIA section 71T, if a SDSO reasonably believes that a person who has been restrained and detained constitutes a threat to safety of persons on Defence premises, they may conduct a non- consensual search of the person while awaiting the arrival of police.

114. In exercising the power to restrain and detain, a DSO, at all times and in all circumstances, is required to:

- a. only use force against a person or item that is reasonable and necessary;
- b. not subject a person to greater indignity than is reasonable and necessary; and
- c. only restrain and detain for the purposes of placing the person in police custody at the earliest practicable time.

115. The power to restrain and detain a person is discretionary. A DSO must determine whether it is appropriate to restrain and detain a person in the circumstances described in this DSPF part “Restrain and Detain” in paragraph 117 having regard to:

- a. the safety of the person, the DSO and other people on the premises;
- b. the proximity of police assistance;
- c. the seriousness of the circumstances giving rise to the exercise of the d. restrain and detain power;
- d. the age and vulnerability of the person – for example trespassing teenagers would be handled differently to suspected terrorists;
- e. whether the person is violent or their demeanor gives rise to the apprehension of violence;
- f. the availability of suitable facilities to hold a person safely until the arrival of police; and

- g. the SAFEBASE security alert level as this could be an indication of the potential seriousness of the circumstances.

116. Alternative response options must be assessed and implemented so as to minimise the use of force. When determining the most appropriate restrain/detain response, a DSO must also give consideration to:

- a. the proximity of police assistance;
- b. the age and vulnerability of the person;
- c. the level of physical aggression presented by the person being restrained – for example, a person who is compliant to a request to wait in a particular location until the arrival of police would be handled differently to a person who is physically aggressive and confrontational towards the DSO;
- d. whether the person is violent or their demeanor gives rise to the apprehension of violence;
- e. whether the person has attempted, or is likely to attempt to flee;
- f. whether the person is required to be escorted or detained with others;
- g. the necessity to prevent the person from injuring themselves, or any other person;
- h. the necessity to restrain the person to prevent the loss, concealment or destruction of evidence; and
- i. whether the person has a weapon.

117. If the person has a weapon, the DSO must exercise caution for their own safety and the police must be contacted. Contracted Defence security guards and Defence security screening employees must not attempt to use force to restrain and detain an armed suspect. Security authorised Defence Force members, who have been trained to deal with armed suspects, may deal with the situation in accordance with their training.

Note: Depending on the situation, the presence of a weapon could indicate that an attack on Defence premises is likely to result in death or serious injury is imminent. In these circumstances, security authorised Defence Force members may be able to exercise their powers in responding to an attack¹⁸.

¹⁸ For further information on Armed Security Wardens refer to DSPF Principle 83 – SAFEBASE.

118. Only security authorised Defence Force members may use equipment (such as handcuffs) to restrain and detain a person if it is considered reasonable and necessary to do so. Security authorised Defence Force members must have been trained in the use of this equipment prior to its use.

119. A security authorised Defence Force member must not use handcuffs to restrain a minor unless they believe on reasonable grounds that the use of handcuffs is essential for the welfare or security of the minor or other people.

120. Security authorised Defence Force members may use military working dogs to assist the DSO to restrain or detain a person. For further information on the use of military working dogs under the identification, search and seizure regime, refer to paragraphs 103 to 105 within this DSPF part - *"Use of Military Working Dogs"*.

Detention

121. A person, who is being detained while awaiting the arrival of police should, where practicable, be held in an area away from other people. Depending on the availability of suitable facilities, this could be in a potentially lockable room or private area located near the access control point. Where practicable, a person being temporarily detained should be kept under observation to avoid occurrences such as destruction of evidence or self-harm.

122. The dignity, safety and proper treatment of the person awaiting transfer to police custody is to be maintained at all times.

123. A DSO **must** provide a detained person an explanation for their apprehension.

124. A DSO is not to deny necessary medical treatment to a person who has been detained. If the injuries are of a serious nature, an ambulance must be called.

125. If a DSO subsequently determines that there is no longer a basis for detaining a person, the DSO should release the person.

126. It is recommended that the use of facilities to support detention should be determined on the basis of the available facilities at the site and the particular circumstances of the situation.

Procedural Guidance

127. Contracted Defence security guards should comply with the restrain and detain response procedures detailed in their assignment instructions.

128. SDSO must comply with the restrain and detain response procedures in accordance with training and qualification requirements applicable to their category of DSO.

Reporting Requirements

Search Report

129. Contracted Defence security guards should maintain log books to record details of all consensual searches undertaken when no dangerous or prohibited items are found. At a minimum, this log book should include the following information:

- a. the person's name;
- b. the person's pass/ID number;
- c. location of the search;
- d. date and time of the search; and
- e. the type of search (person/carried item/vehicle).

130. In situations where a dangerous or prohibited item is found, a DSO should prepare a report on the incident. This report must be signed by the DSO and include the following information:

- a. the person's name;
- b. the person's pass/ID number;
- c. status of the person (Defence civilian/ADF member/contractor/visitor);
- d. location of the search;
- e. date and time of the search;
- f. whether the search was consensual or non-consensual;
- g. whether the person hindered or obstructed the search;
- h. the type of search (person/vehicle/item);
- i. if a vehicle has been searched, the vehicle registration, make and model; and
- j. a description of the item(s) found.

131. The report must be signed by both DSOs present during the search and the person who has been searched. If the person refuses to sign, this should also be noted.

132. The discovery of a dangerous or prohibited item during a search also constitutes a security incident. Additional reporting requirements for security incidents will apply¹⁹.

Restrain/Detain Report

133. When a DSO has restrained and detained a person, the official must also record the time the detention of the person commenced.

134. It is recommended that the restrain/detain report include information on any obvious injuries or medical concerns regarding the person being restrained and detained by the DSO and any treatment provided.

135. If a person has been detained and then released (i.e. if a DSO subsequently determines that there is no longer a basis for detaining a person), a report must still be prepared that provides information on the original reason for detention and the reason for release.

Use of Force Report

136. In all cases where a DSO uses force, he or she is to, as soon as is practicable, submit a report through the BSM/SADFO to the Head Defence Support Operations (HDSO) and the Chief Security Officer setting out the full details of the force used and the circumstances in which force was applied. This includes any situation where the DSO used force:

- a. to conduct a non-consensual search of a person;
- b. to break open an item in order to conduct a non-consensual search;
- c. to restrain and detain a person;
- d. to stop and detain a person; or
- e. a military working dog was released against a person.

Note: Separate reporting requirements exist for Armed Security Wardens who use force when exercising their powers.

¹⁹ For further information on reporting requirements refer to DSPF Principle 77 - *Security Incidents and Investigations*.

Roles and Responsibilities

Secretary

137. The Secretary is to approve the form of identity cards for the DSO in writing.

138. The Secretary is to issue an identity card to each DSO. The Secretary may delegate the authority to issue DSO identity cards in accordance with s 71E of the Defence Act.

139. A DSO is to return their identity card to the Secretary within seven days of ceasing to be a DSO. The Secretary may delegate the authority to receive DSO identity cards in accordance with *the Act*.²⁰

Group Heads and Service Chiefs

140. Group Heads and Service Chiefs are responsible for guarding contracts that do not fall within Garrison Support activities managed by Defence Support and Reform Group²¹.

First Assistant Secretary Service Delivery (FAS SD)

141. FAS SD is responsible to Deputy Secretary Estate and Infrastructure for the delivery of contracted guarding services to Defence bases covered in the Base Accountabilities Model²².

Director General Estate Service Delivery (DG ESD)

142. DG ESD is responsible for determining, on the basis of advice from the SADFO and BSM, how the identification, search and seizure regime should be implemented at each Defence base.

Base Support Manager (BSM) and Senior ADF Officer (SADFO)

143. The BSM and the SADFO, in consultation with Heads of Resident Units and as part of the base security plan development process, are to recommend to the DG ESD how the identification, search and seizure regime should be implemented at their base.

²⁰ For further information on security official identity cards refer to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)*.

²¹ For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

²² For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

Base Support Managers

144. The BSM is responsible for coordination of whole-of-base security at SAFEbase ALPHA, BRAVO and CHARLIE and for managing a response to a security incident at the Defence premise that requires routine coordination of the DSO or other base personnel and resources. The BSM is also accountable to the HDSO and the SADFO for the delivery of guarding services to meet the base security requirements²³.

Senior ADF Officer

145. The SADFO supports the BSM in the planning of the identification, search and seizure regime and its implementation at SAFEbase ALPHA, BRAVO and CHARLIE. In addition, each SADFO has particular responsibilities associated with the assumption of command at SAFEbase DELTA and ECHO, and for commanding the response to a security incident that requires a capability beyond that routinely available and that involves ADF members²⁴.

Commanders and Managers

146. If guarding services are not an element of base support services, the relevant Commander or Manager is responsible for recommending to the BSM and SADFO, based on a security risk assessment, the guarding requirements for their base²⁵.

Contract Managers

147. Contract managers are responsible for ensuring that contracts for guarding services meet the identified guarding requirements and for the development of assignment instructions for contracted guards²⁶.

Outsourced Service Providers of Security Services

148. Outsourced service providers of security services are responsible for the implementation of assignment instructions for guarding services.

²³ For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

²⁴ For further information on SAFEbase level and command refer to DSPF Principle 83 – *SAFEbase*.

²⁵ For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

²⁶ For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

Key Definitions

149. **Assignment Instructions.** An operational document detailing the specific duties to be performed under a contract for guarding and patrolling services ([Australian Standard \(AS\) 4421](#)).

150. **Consensual search.** A consensual search of a person has the same meaning as a limited search of a person as defined by the [Defence Act 1903](#) section 71A. Refer to the definition of a limited search below. A consensual search of a vehicle refers to a search of a vehicle, or anything in the vehicle, that is undertaken with the consent of the person apparently in control of the vehicle. A thing includes substances or things in magnetic or electronic form.

151. **Contracted Defence security guard.** A category of Defence Security Official. Refer paragraph 156 for further information.

152. **Declared explosive ordnance depot.** A specified area of land or any other place, building or structure identified and authorised by the Minister as a 'declared explosive ordnance depot'. Declared explosive ordnance depots are further defined in the [Defence Act 1903](#) Part VIA in section 71L.

153. **Defence Access control point.** Defined by the [Defence Act 1903](#) Part VIA in section 71A as a point of entry to, or exit from Defence premises or a part of Defence premises, where entry or exit is controlled or limited by any means. In addition to being located at the perimeter, Defence access control points may be also situated at specified locations within the premises. A Defence access control point may also be established at the base of a gangway to a vessel, the stairs leading up to an aircraft or a ramp providing access to a vehicle. Further explanation of Defence access control points is provided at Annex C to DSPF Control 76.1 – *Defence Access Control Points*. In this DSPF part, Defence access control points are referred to as access control points.

154. **Defence accommodation.** Defined in the [Defence Act 1903](#) Part VIA section 71A as any building, structure, or place within Australia that is used for, or in connection with, the accommodation of a group of members of any part of the Defence Force. It includes accommodation blocks and complexes accommodating members of the Defence Force and their families, but does not include single, stand-alone residences, which are located off base and are either privately owned or rented by Defence Force members. Defence accommodation includes areas connected with accommodation buildings such as private car parks, gardens and recreational facilities which form part of the accommodation buildings.

155. **Defence premises.** Defined in section the [Defence Act 1903](#) Part VIA 71A as any area of land or other place, a building or other structure, a vehicle, vessel or aircraft, or a prohibited area within the meaning of the [Defence \(Special Undertakings\) Act 1952](#) that is located in Australia and is owned or occupied by the Commonwealth for use by the Defence Force or the Department. It includes any fixed

or moveable ramp, stairs or other means of access to or from a vehicle, vessel or aircraft.

Note: Land or buildings that have a Defence purpose, that are not currently in use by the Defence Force or the Department, do not meet the legal definition of Defence premises for the purposes of the identification, search and seizure regime. For example, a former Defence base or a portion of an operational Defence base that has been set aside for a use that is unrelated to the Defence Force or the Department, is not regarded as Defence premises and therefore the identification, search and seizure regime does not apply to these locations.

Note: A Defence base, as defined and referred to in other parts of the DSPF, falls within the definition of a Defence premise.

156. **Defence Security Official (DSO).** Defined in the [Defence Act 1903](#) Part VIA section 71A as a contracted Defence security guard, a security authorised member of the Defence Force or a Defence security screening employee. DSOs are authorised by the Minister to exercise identification, search, seizure and related powers under Part VIA of the Act.

157. **Defence security screening employee.** A category of DSO. For further information refer to paragraphs 11 to 14 within this DSPF part - “Defence Security Screening Employees”, and Table 1 – “Categories of Defence Security Officials” within DSPF Control 76.1 Identification, Search and Seizure Regime.

158. **Detain.** To deny a person free exit from Defence premises until the arrival of police. Section 71Y of the Act also provides that a SDSO may stop and detain a person, or vehicle, vessel or aircraft to:

- a. require a person to provide evidence of particular matters; or
- b. search the person, vehicle, vessel or aircraft.

159. **Identification and Search Warden (ISW).** A specialised sub-category of security authorised members of the Defence Force (for further information refer to the Key Definitions section within the DSPF Principle, and Table 1 – “Categories of Defence Security Officials” within DSPF Control 76.1 further information) who are authorised by the Minister to affect the identification, search and seizure regime contained in Part VIA of the [Defence Act 1903](#).

160. **Limited search.** A limited search of a person is defined in the [Defence Act 1903](#) Part VIA section 71A. It is a search of a person that is performed by a DSO with the person’s consent and includes:

- a. a search of items in the possession of a person that may include requesting the person to remove his or her overcoat, coat or jacket and any gloves, shoes and hat and an examination of any of those items that the person consents to remove; or

- b. a search of a person conducted by quickly running the hands over the person's outer garments and an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person.

A limited search does not include requesting the person remove all of their garments.

Any reference to a consensual search of a person in this DSPF part means a limited search of a person undertaken with the person's consent.

161. **Minor.** A person who has not attained the age of 18 years.

162. **Non-consensual search.** A non-consensual search of a person has the same meaning as a search as defined by section 51 of the Act. It is performed by the SDSO without the requirement for consent from the person. Refer below for the definition of a search. A non-consensual search of a vehicle refers to a search of a vehicle, or anything in the vehicle, that is performed by the SDSO without the requirement for consent from the person apparently in control of the vehicle. A thing includes substances or things in magnetic or electronic form.

163. **Person.** In this DSPF part, a reference to a person includes a Defence APS employee, a Defence Force member, a Defence contractor or a visitor.

164. **Police.** In this DSPF part, a reference to police includes State and Territory Police Officers, AFP Officers and Protective Service Officers of the AFP.

165. **Restrain.** Any word or action that is used for the purpose or intent of restricting the free movement of another person.

166. **Search.** A search of a person has the same meaning as in section 51 of the [Defence Act 1903](#). A search of a person is a search that is undertaken by a SDSO without the requirement for consent from the person and includes:

- a. a search of a person or items in the possession of a person that may include requiring the person to remove his or her overcoat, coat, jacket, gloves, shoes and hat and an examination of those items; or
- b. a search of a person conducted by quickly running the hands over the person's outer garments and an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person.

A search of a person differs from a limited search of a person in that the 'pat down' of the person can be conducted after requiring the removal of the person's overcoat, coat, jacket, gloves, shoes and hat.

A search of a person does not include requiring the person to remove all of their garments or an examination of the person's body cavities.

A search of a vehicle, as defined in the [Defence Act 1903](#) Part VIA section 71A, includes a search of a thing in the vehicle.

167. **Security authorised Defence Force member.** A category of DSO. For further information refer to paragraphs 15 to 17 of this DSPF part and Table 1 – “*Categories of Defence Security Officials*” within DSPF Control 76.1 Identification Search and Seizure Regime.

168. **Special Defence Security Official (SDSO).** A security authorised member of the Defence Force or a Defence security screening employee as defined by the [Defence Act 1903](#) Part VIA sections 71C and 71D. SDSO are authorised under the [Defence Act 1903](#) Part VIA to undertake non-consensual identification, search, seizure and related actions.

169. **Vehicle.** In this DSPF part, a reference to a vehicle includes a vessel and an aircraft.

Further Definitions

170. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Annexes and Attachments

Annex A – *Other Non-Statutory Search Regimes*

Annex B – *Offences and Penalties*

Annex C – *Defence Access Control Points*

Annex D – *Defence Security Officials – Training and Qualification Requirements*

Annex E – *Summary of Defence Security Officials’ Powers*

Annex F – *Defence Security Official Identity Cards (DSOIC)*

Annex G – *Special Search Provisions for Declared Explosive Ordnance Depots*

Document Administration

Identification

DSPF control	Identification, Search and Seizure Regime
Control Owner	DG ESD
DSPF number	76
Version	3
Publication date	4 March 2022
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry

Related Information

General Principle and Expected Outcomes	Identification, Search and Seizure Regime
Government compliance	<u>PSPF Core Requirements:</u> Agency physical security policy and planning; protection of employees Legislation: <u>Defence Act 1903</u>, Part VIA, Security of Defence Premises.
Read in conjunction with	
See also DSPF	Physical Security Certification and Accreditation Security Incidents and Investigations Access Control
Implementation Notes, Resources and Tools	The scope of this principle and underlying security controls is confined to describing the identification search and seizure regime and does not describe the role of Armed Security Wardens or the operation of the Enhanced Self Defence Capability.

Version Control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with

Version	Date	Author	Description of changes
			PSPF; update of language to reflect Defence Admin Policy
3	4 March 2022	DG ESD	Update Para 43, Footnote 14, Para 128



Defence Security Principles Framework (DSPF)

Annex A to Identification, Search and Seizure Regime – Other Non-Statutory Search Regimes

Other Non-Statutory Search Regimes

1. At Defence sites that are assessed as having a low security risk and where there are minimal assets requiring protection, it may be determined that implementation of the statutory search regime contained within the [Defence Act 1903](#) (the Act), Part VIA, Security of Defence Premises is not warranted. At these sites, security searches that are based on common law can be conducted by appropriately trained contracted security guards in accordance with the policy contained in this Annex and approved base security plans and instructions.
2. At Defence sites that are not operating the statutory search regime contained in the Act, security inspections are strictly limited to:
 - a. consensual inspections of carried items, or items in a person's possession on entry to and exit from the site; and
 - b. consensual inspections of vehicles, including things in the vehicle, on entry to and exit from the site.
3. A search of a person that involves a 'pat down' over the person's outer garments and non-consensual searches are not to be conducted under any circumstances.
4. All inspections are to be conducted in accordance with approved base security plans and instructions. Refer to DSPF Principle 83 - *SAFEBASE* for further information. Additionally, all contracted security guards who conduct inspections are to meet the security, licensing and competency requirements detailed in DSPF Principle 75 - *Contracted Security Guards*.

Non-statutory Consensual Inspection of Carried Items or Vehicle on Entry to or Exit from a Defence Base

5. Contracted security guards may request a person, who is about to enter or exit a Defence site, to permit a consensual inspection of their carried items or items in their possession.

6. Similarly, contracted security guards may request a person apparently in control of a vehicle that is about to enter or exit a Defence site to permit a consensual inspection of the vehicle, including things in the vehicle.

Inspection Process

7. During a non-statutory consensual inspection, a person is to display all items and their identification as requested by contracted security guards. This may involve removing items from vehicles.

8. The contents of briefcases used for carrying classified material are not exempt from a non-statutory consensual inspection. If consent is given to undertake an inspection then:

- a. the briefcase may be opened and the contents given a cursory inspection to verify the existence of documented authorisation to carry the material and to ensure that the material has been properly protected and does not appear to have been subject to tampering; and
- b. the person carrying the briefcase can be asked to move papers and files around, but files are not to be opened.

9. Where practicable, storage facilities should be made available outside the Defence base to allow personnel to securely store items prior to entry.

10. Two contracted security guards should be present at all non-statutory consensual inspections to avoid any evidential dispute. The guards are to be appropriately trained in the conduct of inspections. In order to protect the privacy of the person, guards must not record or discuss anything of a private or personal nature observed during the conduct of a non-statutory consensual inspection.

11. Same gender non-statutory consensual inspections may not always be possible. Females or males who are uncomfortable with having their vehicles or carried items inspected by a guard of the opposite gender may choose to have another person (a colleague for example) present during the inspection. That person must be able to attend the site in a timely manner.

12. Contracted guards must conduct non-statutory consensual inspections in accordance with their training and qualifications.

13. If a dangerous or prohibited item is located during a non-statutory consensual inspection and the person in possession of it has no reasonable explanation or authority for having the item then the person is not to enter the base with the item.

14. Form [AD432 – Security Inspection Report](#) is to be completed if a dangerous or prohibited item is found, or if a person complains about the manner in which the

non-statutory consensual inspection was undertaken. As a completed Form AD432 may be used as evidence, it is to be signed by the person as a true and accurate record of events, or provide an explanation as to why the individual failed to sign the report.

15. Completed reports are to be forwarded in a timely manner through the chain of command to the Commander or Manager. If the report is a complaint about the manner in which the non-statutory consensual inspection was undertaken, the Commander or Manager is to undertake a review of the conduct of the inspection.

Refusal to Consent to a Non-statutory Inspection

16. **Visitors.** A visitor may be denied access to a Defence base if they refuse to consent to a non-statutory inspection of their carried items or vehicle on entry. A visitor must not be denied exit from a Defence base if they refuse to consent to a non-statutory inspection on exit.

17. **Defence Personnel.** Defence personnel must not be denied entry to, or exit from a Defence base if they refuse to consent to a non-statutory inspection of their vehicle or carried items. In the event that a Defence Force member or civilian employee of the Department of Defence refuses to consent to a non-statutory inspection of their carried items or vehicle, their immediate supervisor must be informed. Repeated refusals may lead to disciplinary action under the [Public Service Act 1999](#) (for not complying with a lawful and reasonable direction) or the [Defence Force Discipline Act 1982](#) (for refusing to comply with the security requirements of the DSPF).

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Other Non-Statutory Search Regimes
Annex Version	3
Annex Publication date	4 March 2022
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	4 March 2022	DG ESD	Amendments to para 12



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Identification, Search and Seizure Regime – Offences and Penalties

Offences and Penalties

1. The [Defence Act 1903](#) (the Act) Part VIA establishes offences and penalties associated with the execution of the identification, search and seizure regime.

Unauthorised Entry on Defence Premises or Defence Accommodation

2. Under Part VIA section 72P of the Act, a person commits an offence if they enter, or are on Defence premises or in Defence accommodation when they are not authorised to do so.
3. A member of the Defence Force, Australian Federal Police, State and Territory police, or a protective service officer may, without a warrant, arrest the person if the member reasonably believes that the person is not authorised to be on the Defence premises or in the Defence accommodation. In the event that a person is arrested by a Defence Force member, the person is to be placed in police custody as soon as practicable after the arrest.

Note: A person arrested by a Defence Force member in the situation outlined above cannot be transferred to the custody of a Protective Service Officer of the Australian Federal Police.

Note: This offence is also a protective service offence for the purposes of the [Australian Federal Police Act 1979](#).

4. Only members of the Defence Force who have been appropriately trained and equipped may arrest a person in the circumstances outlined above.
5. A member of the Defence Force may use handcuffs, if it is considered reasonable and necessary, to restrain a person following their arrest on Defence premises or in Defence accommodation. Only members of the Defence Force who have been properly trained and equipped may arrest a person in the circumstances outlined above.

Note: *Authorised Commonwealth Officers have comparable powers to apprehend and detain a person who has trespassed on prohibited Commonwealth land or discharged a firearm on or over Commonwealth land. The exercise of these powers is separate from the powers of a Defence Security Official (DSO) as specified in Part VIA of the Act.*

Refusal to Provide Evidence of Identity in Response to a Non-Consensual Identification Action

6. Under the Act Part VIA section 71V a person, who is on Defence premises, commits an offence if a Special Defence Security Official (SDSO) requires the person to provide evidence of their identity or authority to be on the premises, and the person:

- a. refuses;
- b. fails to provide the evidence; or
- c. gives a name or address that is false in a material particular.

7. A monetary penalty applies to this offence.

8. The offence, however, will not apply if the SDSO did not comply with the requirement to produce their identity card and inform the person of the effect of refusing to comply with the requirement, prior to exercising this power.

Note: *This offence is also a protective service offence for the purposes of the [Australian Federal Police Act 1979](#).*

Offences Relating to Consensual Search Powers

9. Under the Act Part VIA section 71Q, a DSO commits an offence if they conduct a limited search of person without the person's consent. A monetary penalty applies to this offence.

10. Further, a DSO commits an offence if they conduct a search of a vehicle, purportedly under the consensual regime, and the person apparently in control of the vehicle did not consent to the search. A monetary penalty applies to this offence.

11. These offences would apply in circumstances where the person believed they had to comply with the consensual search request. That is, a DSO must not do anything that causes a person to believe they must submit to a consensual search. A person must freely and voluntarily provide clear consent to the DSO immediately prior to the conduct of any consensual search.

12. A DSO **must** immediately cease a consensual limited search of a person or a consensual search of a vehicle if the person subsequently withdraws their consent. A DSO commits an offence if they continue to undertake a purportedly consensual search after consent has been withdrawn.

Hindering or Obstructing a Non-Consensual Search by a Special Defence Security Official

13. Under the Act Part VIA section 71W, a person commits an offence if they hinder or obstruct a non-consensual search by a SDSO. The offence only applies if prior to conducting the non-consensual search, the official produced their identity card for inspection and informed the person of the consequences of refusing to comply with, or hindering the non-consensual search. A monetary penalty applies to the offence.

Note: If an SDSO reasonably believes that a person constitutes a threat to safety such that complying with the requirement, prior to conducting a non-consensual search, places the safety of the official and others at risk, they may temporarily delay presenting their identity card. For example, this might occur if the official reasonably believes the person is carrying a concealed weapon. In these circumstances, after the immediate threat to safety has been resolved, the official is required to produce his or her identity card for inspection by the person and inform the person of the effect of hindering or obstructing the search.

Note: This offence is also a protective service offence for the purposes of the [Australian Federal Police Act 1979](#).

Return of Defence Security Official Identity Cards

14. Under the Act Part VIA section 71E, a person commits an offence if they do not return their identity card to the Secretary (or delegate) within 7 days of ceasing to be a DSO. A monetary penalty applies to this offence. For further information, refer to Card Return in Annex F to DSPF Control 76.1 – *Defence Security Official Identity Cards (DSOIC)*.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Offences and Penalties
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex C to Identification, Search and Seizure Regime – Defence Access Control Points

Defence Access Control Points

1. A Defence access control point is an identified location on a Defence premises where Defence Security Officials (DSOs) are authorised to exercise their identification, search and related powers.
2. A Defence access control point is defined by the [Defence Act 1903](#) Part VIA section 71A as a point of entry to, or exit from Defence premises or a part of Defence premises, where entry or exit is controlled or limited by any means. In addition to being located at the perimeter, Defence access control points may be also situated at specified locations within the premises. A Defence access control point may also be established at the base of a gangway to a vessel, the stairs leading up to an aircraft or a ramp providing access to a vehicle. In this annex, Defence access control points are referred to as access control points.
3. A sign or boundary marker on its own does not constitute an access control point. An access control point must include one or more measures to limit access. These measures may include, but are not limited to:
 - a. the presence of a DSO;
 - b. the requirement to present access cards or other identification for inspection;
 - c. electronic security barriers fitted with access card readers;
 - d. electronic handheld access card readers; or
 - e. retinal scanners, hand scanners and comparable devices or other biometric identity management solutions.
4. These measures may be used in conjunction with, but are not limited to, any of the following physical security controls:
 - a. gates, including boom gates;
 - b. security bollards;

- c. locked or electronically controlled doors; or
 - d. entry points to vehicles, vessels or aircrafts including gangways and stairs.
5. An access control point could be set up at the entrance to an outsourced service provider's facility if it is located on Commonwealth land or within a building occupied by the Commonwealth.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Defence Access Control Points
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	[Launch <i>Description of changes</i>]
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex D to Identification, Search and Seizure Regime – Training and Qualification Requirements

Defence Security Officials – Training and Qualification Requirements

1. Training and qualification requirements are outlined in two Legislative Instruments:
 - a. [Defence \(Contracted Defence Security Guards – Training and Qualification Requirements\) Determination 2013](#), dated 1 September 2013; and
 - b. Defence (Security Authorised Members -Training and Qualification Requirements) Determination 2013, dated 25 September 2013.
2. This Annex outlines these requirements against different roles.

Contracted Security Guards

3. Refer to DSPF Principle 75 – *Contracted Security Guards* for more detailed information.

Qualifications

4. The person must hold:
 - a. a current certificate II in Security Operations or a higher qualification in Security Operations; or
 - b. in the case of guards carrying out specialist functions, a Certificate III in Security Operations and/or additional competencies.
5. The person must hold a current licence to work as a security guard in the State or Territory where the person works, or would work, as a contracted defence security guard.

Training

6. Contracted security guards are to complete a Defence-endorsed training package (delivered by the contracted security guard service provider, or Defence). This is to cover topics such as:
 - a. Defence security policy and relevant Federal, State and Territory laws;
 - b. Defence protocols (including rank structure, customer service, etc.);
 - c. the Defence security environment;
 - d. Defence policing; and
 - e. the SAFEBASE alert level security system.
7. For each year after the person complete training to refresh or update the skills and knowledge the person needs to perform the duties of a contracted defence security guard.
8. The person **must** hold a current qualification or competency in first aid.
9. The person **must** hold, at minimum, a current Baseline security clearance issued or recognised in accordance with the Department's security policy. A higher clearance may be required for specialist tasks.
10. The person **must** have completed the course Defence Security Official – Roles and Responsibilities – Course Campus ID 00007028.

Defence Security Screening Employee

11. Defence security officials (DSOs) who are Defence Australian Public Service security screening employees are required to have fulfilled the training, qualification, probity and licensing prerequisites as determined by the Minister, or his delegate, in a legislative instrument.
12. A valid first aid qualification is a mandatory requirement for security screening employees, to administer qualified basic first aid as required.
13. Security screening employees must hold a minimum Defence security clearance.
14. Security screening employees **must** have completed the course Defence Security Official – Roles and Responsibilities – Course Campus ID 00007028.

Security Authorised Defence Force Members

Identification and Search Warden

15. DSOs who are Security Authorised Defence Force Members must have fulfilled the training, qualification, probity and licensing prerequisites as determined by the Minister, or his delegate, in a legislative instrument ([Defence \(Security Authorised Members-Identification and Search Wardens: Training and Qualification Requirements\) Determination 2014](#), dated 27 November 2014).

Qualifications

16. The training and qualification requirements for a person to be a Security Authorised Member of the Defence Force—Identification and Search Warden are:

17. The person **must** have successfully completed:
- a. the Service Police Officer Basic Course;
 - b. the Service Police Basic Course; or
 - c. training that is of a kind approved, in writing, by the Minister, or a delegate of the Minister, and that is designed to give the person competence in the following:
 - (1) managing security risk situations;
 - (2) searching people, vehicles and other things;
 - (3) controlling access to and exit from premises;
 - (4) conducting search and seizure operations; and
 - (5) operational safety skills and tactics.

Training

18. The person **must** have successfully completed training that is:
- a. of a kind approved, in writing, by the Minister or a delegate of the Minister; and
 - b. designed to give the person familiarity with the following:
 - (1) The Act and other relevant Commonwealth, State and Territory laws;
 - (2) the security policies and protocols of the Department;
 - (3) other matters relevant to the security of the Department;
 - (4) the policing arrangements used by the Defence Force; and

(5) the security alert system used by the Department.

19. Every 12 months after the person has successfully completed both the course or training outlined in paragraphs 15 and 17 of this Annex, the person must successfully complete training that is:

- a. of a kind approved, in writing, by the Minister or a delegate of the Minister; and
- b. designed to refresh or update the skills and knowledge the person needs to perform the duties of a Security Authorised Member of the Defence Force – Identification and Search Warden.

20. The person **must** hold a current security clearance issued or recognised in accordance with the Department's security policy.

Military Working Dog Handler

Military Dog Handler

21. DSOs who are Security Authorised Defence Force Members are required to have fulfilled the training, qualification, probity and licensing prerequisites as determined by the Minister, or his delegate, in a legislative instrument ([Defence \(Security Authorised Members – Military Working Dog Handlers: Training and Qualification Requirements\) Determination 2015](#), dated 2 November 2015).

22. Military dog handlers are required to undertake the training below, where relevant:

23. Successfully complete:

- a. the Air Force Security Military Working Dog Handler 1 course; or
- b. the Air Force Security Military Working Dog Handler Reteam course; and
- c. while working with his or her assigned dog as a Military Working Dog team, have been assessed by the Manager of the Military Working Dog section in the Air Force as proficient at the operational level of capability.

24. If the person is assigned an Explosive Detector Dog, the person **must** have successfully completed;

- a. the Australian Customs Service Explosive Detector Dog course;
- b. the United States Air Force Specialised Search Dog course; or
- c. the Royal Australian Air Force Explosive Detector Dog course.

25. Every 12 months Military Dog Handlers are to undertake the following:
- the Air Force Security Military Dog Handler 1 course; or
 - the Reteam course is to be completed and assessed as being proficient at the operational level of capability.
26. Every 12 months if a Military Dog Handler is also an Explosive Detector Dog Handler they must undertake and successfully complete one of the following:
- the Australian Customs Service Explosive Detector Dog course;
 - the United States Air Force Specialised Search Dog course; or
 - the Royal Australian Air Force Explosive Detector Dog course.
27. The person must successfully complete all training that is:
- of a kind approved, in writing, by the Minister or delegate of the Minister, and
 - designed to refresh or update the skills and knowledge the person needs to perform the duties of a Security Authorised Member of the Defence Force – Military Working Dog Handler.
28. A requirement to undertake the training and to be a Security Authorised Member of the Defence force, a valid security clearance is to be held in accordance with the Departments security policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Training and Qualification Requirements
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Defence Security Principles Framework (DSPF)

Annex E to Identification, Search and Seizure Regime – Summary of Defence Security Officials' Powers

Summary of Defence Security Official's Powers

Table 1: Summary of Defence Security Officials' Powers

Power	<u>Defence Act 1903</u> Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Consensual identification and limited search of person about to pass an access control point including, in defined circumstances, authority to: • refuse to allow the person to pass the access control point; and • if on Defence premises, restrain and detain.	71H	Y	Y	Y
Consensual search of vehicle, vessel or aircraft at an access control point including, in defined circumstances, authority to: • refuse to allow the vehicle to pass the access control point; and • if on Defence premises, restrain and detain any people in the vehicle.	71J	Y	Y	Y
Consensual identification of person on Defence premises if there is a reasonable belief the person is not authorised to be on the premises including, in defined circumstances, authority to: • restrain and detain.	71K	Y	Y	Y

Power	<u>Defence Act 1903</u> Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Consensual limited search of person on a declared explosive ordnance depot including, in defined circumstances, authority to: restrain and detain.	71M	Y	N/A	N/A
Consensual search of vehicle, vessel or aircraft while on a declared explosive ordnance depot including, in defined circumstances, authority to: restrain and detain any people in the vehicle.	71N	Y	N/A	N/A
Non-consensual search of vehicle, vessel or aircraft at an access control point including, in defined circumstances, authority to: - refuse to allow a vehicle to pass an access control point; and - if on Defence premises, restrain and detain any people in the vehicle.	71S	N	N	Y
Non-consensual identification and search of person on Defence premises if there is reasonable belief that person is not authorised to be on the premises, poses a threat to safety or may be involved in a criminal offence, including in defined circumstances, authority to: - request the person to leave and, if he/she refuses, remove the person from the premises; or - in specific circumstances (safety of self and others) restrain and detain for purposes of placing them in custody of the police; - If the ADF Special Defence Security Official (SDSO) is not available or it is not practical for them to undertake the search, the above duties can be undertaken.	71T	N	N	Y
	71T	Y	Y	Y
	71T	N	Y	Y

Power	<u>Defence Act 1903</u> Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Non-consensual search of vehicle, vessel or aircraft while on a Defence premises if there is reasonable belief that it is not authorised to be on the premises, constitutes a threat to safety or may be involved in a criminal offence, including authority to: - restrain and detain any people in the vehicle; - If the ADF SDSO is not available or it is not practical for them to undertake the search, the above duties can be undertaken. - If the ADF Special Defence Security Official (SDSO) is not available or it is not practical for them to undertake the search, the above duties can be undertaken.	71U	N	N	Y
	71U	N	N	Y
	71U	N	Y	Y
Stop and detain person, vehicle, vessel or aircraft, for the purposes of undertaking non-consensual identification or search actions If the ADF SDSO is not available or its not practical for them to undertake the search, the above duties can be undertaken	71Y	N	N	Y
Seize an item found on a Defence base or as a result of a search, if there is reasonable belief that it constitutes a threat to safety, or relates to a criminal offence, including authority to: - take such action that is reasonable and necessary to make the item safe or prevent it being used. - request the item to remain in place until the police arrive.	72	N	N	Y
	72	Y	Y	Y

Power	<u>Defence Act 1903</u> Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Restrain and detain for the purpose of placing the person, at the earliest practicable time, into police custody.				
Undertake common law (Citizens) arrest	72J	Y	Y	Y
Use reasonable force to restrain and detain	72J	N	N	Y
Use equipment to examine items , including electronic equipment as part of the search process, or if the item constitutes a threat to safety or relates to a criminal offence. This includes using equipment to access data stored on an item. Staff who are qualified to utilise the equipment can only operate the equipment this may be on behalf of the DSO and SDSO	72E	Y	Y	Y
Power to move certain unattended things to another place if it is necessary or desirable to do so	72F	Y	Y	Y
Use of dogs is limited to security authorised members of the Defence Force to assist in exercising their powers of search, restrain/detain and remove when it is considered reasonable and necessary	72M	N	N	Y

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Summary of Defence Security Officials' Powers
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Defence Security Principles Framework (DSPF)

Annex F to Identification, Search and Seizure Regime – Defence Security Official Identity Card Delegations

Defence Security Official Identity Cards (DSOIC)

1. Under the [Defence Act 1903](#) (the Act) Part VIA, section 71E, all Defence Security Officials (DSO) **must** carry their identity cards at all times when performing the functions or exercising powers under Part VIA of the Act. In addition, under the Act Part VIA, section 72B a DSO must produce this card for inspection by a person before:
 - a. requesting or requiring the person to provide evidence of their identification or authority to pass an access control point or be on Defence premises;
 - b. requesting a consensual limited search of a person (including items in the person's possession) or a consensual search of a vehicle apparently under the person's control;
 - c. requiring a non-consensual search of the person (including items in the person's possession) or a vehicle apparently under the person's control; or
 - d. restraining, detaining or removing a person from Defence premises.

Card Issue

2. Under the Act Part VIA, section 71E (1), the Secretary must issue an identity card to each DSO. The Secretary may delegate the authority to issue DSO identity cards in accordance with the Act Part VIA, section 71G. In the event that this power is delegated, the Secretary must delegate the authority to issue DSOIC to specific Australian Public Service (APS) employees in Executive Level 2 positions or higher, or military officers holding the rank of Colonel (or equivalent) or higher. Delegates who have been authorised to issue DSOIC are listed in Appendix 1 to Annex F to DSPF Control 76.1 – *Defence Security Official Identity Card Delegations*.
3. Delegates are to be satisfied that the proposed DSO:
 - a. has met the relevant minimum training and qualification requirements as identified by the Minister in a legislative instrument; and

- b. has met any other pre-conditions established in the ministerial authorisation for the relevant category or sub-category of DSO.
- 4. Every person issued with a DSOIC is to sign a form acknowledging that they:
 - a. may only use the card for the purpose of fulfilling their duties as a DSO; and
 - b. **must** return their identity card to a nominated point of contact within seven days of ceasing to be a DSO.

Card Return

5. Under the Act Part VIA, section 71E, a DSO **must** return their identity card to the Secretary within seven days of ceasing to be a DSO. A DSO commits an offence if they do not return their DSOIC within this timeframe. This offence does not apply if the card was lost or destroyed.

6. The Secretary may delegate the authority to receive DSOIC in accordance with the Act Part VIA, section 71G of. In the event that this power is delegated, the Secretary **must** delegate the authority to receive returned identity cards to specific APS employees at the APS 5 level or higher, and military officers of the rank of Captain (or equivalent) or higher. Delegates who have been authorised to receive DSOIC are listed in Appendix 1 to Annex F to DSPF Control 76.1 – *Defence Security Official Identity Card Delegations*.

7. Delegates who have received cards are to return the DSOIC to a pass office by SAFEHAND or destroyed on-site using an approved method and the pass office notified accordingly.

Format

8. Under the Act Part VIA, section 71E, the Secretary is to approve the format of the DSOIC in writing. The DSOIC should include a recent photographic image of the official. In accordance with the Secretary's direction, the DSOIC should also include:

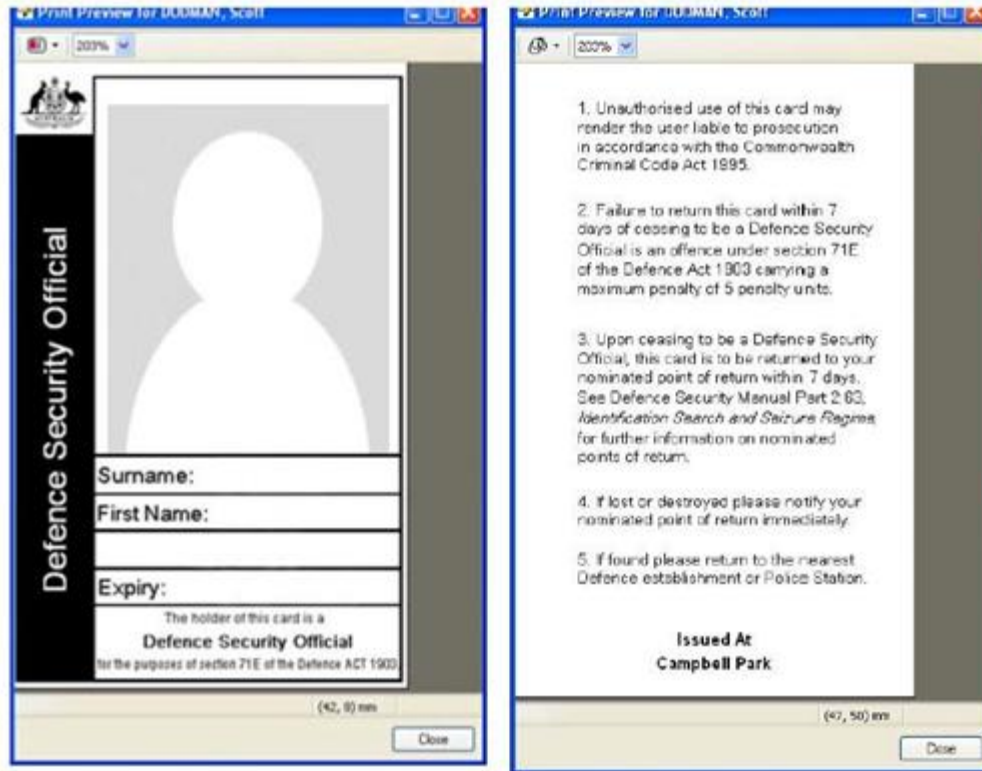
- a. the official's first name and surname;
- b. an expiry period of five (5) years for DSOIC from the date of issue for the particular category or sub-category of Special Defence Security Official (SDSO); and
- c. for security authorised Defence Force members, their rank.

9. Legal disclaimers appear on the reverse of the card to remind the bearer of the offence for not returning a DSOIC within 7 days and provide further instruction on how to return it.

10. Two forms of DSOIC have been developed to distinguish between officials who are authorised under the Act to exercise consensual powers only, and officials who are authorised to exercise both consensual and non-consensual powers.
- a. Officials who are authorised to exercise consensual powers only will be identified through the use of an identity card that has 'Defence Security Official' printed in white font on a black background; and
 - b. Officials who are authorised to exercise both consensual and non-consensual powers will be identified through the use of a card that has 'Special Defence Security Official' printed in red font on a black background.
11. The distinction between DSOs and SDSOs supports proposed signage at primary access points that informs Defence employees and visitors of the exercise of consensual and non-consensual powers on the Defence premises. There is no requirement for a separate DSOIC to identify each discrete category or sub-category of Defence security official.
12. Training regimes require DSOs undertake refresher training within a specified timeframe in order to remain an official. In recognition of this safeguard, an expiration date is displayed on the front of the card that is linked to the date when the official is required to undertake refresher training. For further information on training requirements for DSOs refer to Annex D to DSPF Control 76.1 – *Defence Security Officials – Training and Qualification Requirements*.
13. As the Act also includes an offence relating to the failure to return a DSOIC within seven days of ceasing to be a DSO, legal disclaimers appear on the reverse of the card to remind the bearer of this offence and to provide instruction on how to return the card.
14. The DSOIC are reproduced below.

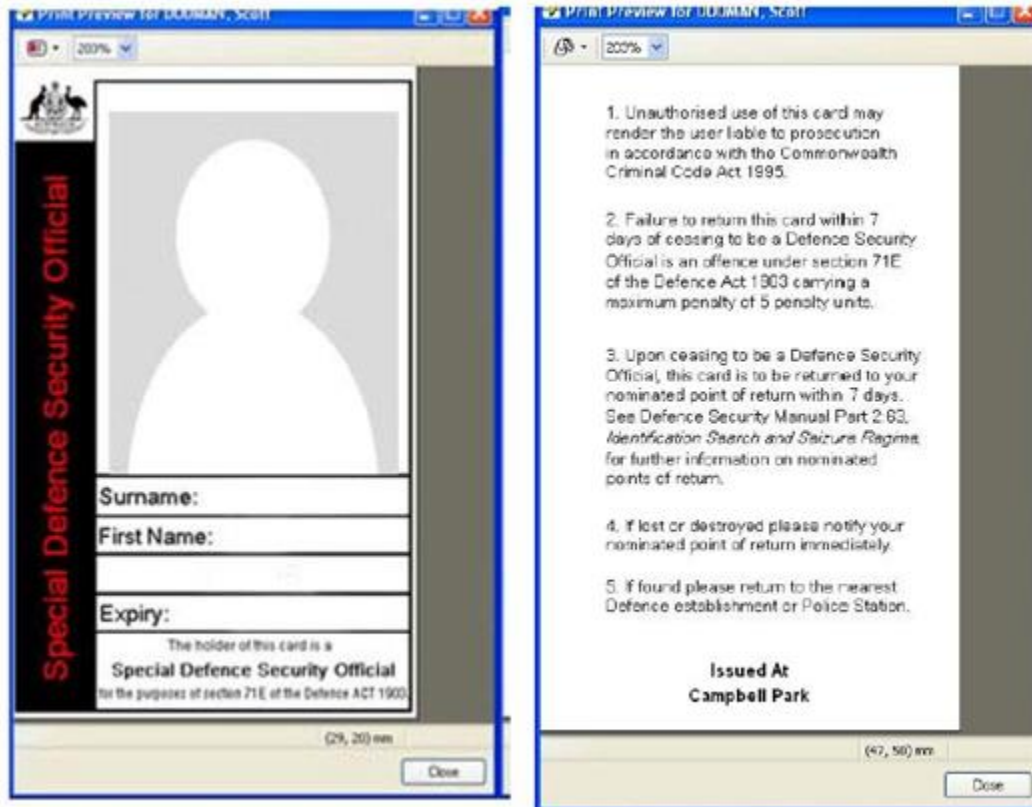
Defence Security Official Identity Card (DSOIC)

Figure 1: Defence Security Official Identity Card



Special Defence Security Official Identity Card (SDSO)

Figure 2: Special Defence Security Official Identity Card



Appendixes and Attachments

Appendix 1 – Defence Security Official Identity Card Delegations

Document administration

Identification

DSPF Annex	Defence Security Official Identity Cards
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Appendix 1 to Annex F of Identification, Search and Seizure Regime – Defence Security Official Identity Card Delegations

Instrument of Delegation

A copy of the Secretarial instrument of delegation in relation to the issue and receipt of Defence Security Official Identity Cards is provided below.

Defence Security Official Identity Cards Delegation 2012

Defence Act 1903

I, DUNCAN EDWARD LEWIS, Secretary of the Department of Defence, make the following delegation under subsections 71G (1) and (2) of the *Defence Act 1903*.

Dated 6 JULY 2012

SIGNED

Secretary

1 Name of delegation

This delegation is the *Defence Security Official Identity Cards Delegation 2012*.

2 Commencement

This delegation commences when it is made.

3 Definitions

In this delegation:

Base Support Manager means a Defence civilian employee or ADF member at the APS Level 5 or equivalent (or military equivalent) or above who is responsible for base support management and services and who has been appointed a Base Support Manager.

Chief Staff Officer Establishments (Navy) means an officer of the Navy who holds the rank of Captain or a higher rank and has been appointed Chief Staff Officer Establishments (Navy).

Deputy Air Commander Australia means an officer of the Air Force who holds the rank of Group Captain or a higher rank and has been appointed Deputy Air Commander Australia.

Director General Capability Planning Air Force means an officer of the Air Force who holds the rank of Group Captain or a higher rank and has been appointed Director General Capability Planning Air Force.

Group Security Adviser means a Defence civilian employee at the Executive Level 2 or above who is the senior security officer in a Group and has been appointed as a Group Security Adviser.

Provost Marshal Australian Defence Force means:

- (a) an officer of the Army who holds the rank of Colonel or a higher rank; or
- (b) an officer of the Navy who holds the rank of Captain or a higher rank; or
- (c) an officer of the Air Force who holds the rank of Group Captain or a higher rank; and
- (d) has been appointed Provost Marshall Australian Defence Force.

Regional Director means a Defence civilian employee at the Executive Level 2 or above who has been appointed as a Regional Director within the Defence Support Group.

Security Officer means a Defence civilian employee or ADF member at the APS 5 Level or equivalent (or military equivalent) or above who coordinates or administers the security functions within a business or military unit and has been appointed a Security Officer.

Senior Australian Defence Force Officer (SADFO) means:

- (a) an officer of the Army who holds the rank of Colonel or a higher rank; or
- (b) an officer of the Navy who holds the rank of Captain or a higher rank; or
- (c) an officer of the Air Force who holds the rank of Group Captain or a higher rank; and
- (d) has been appointed the SADFO of a base or bases.

Service Security Adviser means:

- (a) an officer of the Army who holds the rank of Colonel or a higher rank; or
- (b) an officer of the Navy who holds the rank of Captain or a higher rank; or
- (c) an officer of the Air Force who holds the rank of Group Captain or a higher rank; and
- (d) has been appointed a Service Security Adviser.

4 Delegation

I delegate to each person occupying, or performing the duties of, an office or position mentioned in an item in Schedule 1 my powers or functions under the *Defence Act 1903* mentioned in the item.

Schedule 1 Delegation

(section 3)

Item	Provision	Description	Position
1	subsection 71E (1)	To issue an identity card to a defence security official who is a contracted defence security guard	Regional Director, Defence Support Group
2	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Identification and Search Warden; and (c) a member of the Service Police	Provost Marshal Australian Defence Force
3	subsection 71E (1)	To issue an identity card to a defence security official who: (a) is a security authorised member of the Defence Force; and (b) is an Identification and Search Warden; and (c) is a member of the Air Force Security Forces	Deputy Air Commander Australia
4	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) is an Identification and Search Warden; and (c) is not a member of the Service Police or a member of the Air Force Security Forces	Senior ADF Officer (SADFO) Group Security Adviser Service Security Adviser
5	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Armed Security Warden; and (c) performing duties at a base at which enhanced self-defence capability is in operation	Senior ADF Officer (SADFO) of a base at which the enhanced self-defence capability is in operation

Item	Provision	Description	Position
6	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Armed Security Warden; and (c) performing duties at Fleet Base East	Chief Staff Officer Establishments (Navy)
7	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) a Military Working Dog Handler	Provost Marshal Australian Defence Force Director General Capability Planning Air Force
8	subsection 71E (1)	To issue an identity card to a defence security screening employee	Group Security Adviser Service Security Adviser
9	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is a contracted defence security guard	Security Officer Base Support Manager
10	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Identification and Search Warden	Security Officer Base Support Manager
11	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Armed Security Warden	Security Officer Base Support Manager
12	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is: (a) a security authorised member of the Defence Force; and (b) a Military Working Dog Handler	Security Officer Base Support Manager
13	paragraph 71E (3) (c)	To receive an identity card that has been returned by a defence security screening employee	Security Officer Base Support Manager

Attachments

This DSPF Appendix has no Attachments.

Document administration

Identification

DSPF Annex	Defence Security Official Identity Card Delegations
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex G to Identification, Search and Seizure Regime – Special Search Provisions for Declared Explosive Ordnance Depots

Special Search Provisions for Declared Explosive Ordnance Depots

1. Given the inherent risk to public safety posed by the unlawful removal of weapons, ammunition and explosive ordnance from Defence premises, special search provisions have been enacted in the [Defence Act 1903](#) (the Act), Part VIA, Division 3, Subdivision B – Special provisions for declared explosive ordnance depots.

Note: Not all explosive ordnance depots are covered by the provisions in the Act, Division 3, Subdivision B.

2. A declared explosive ordnance depot is an area of land, place, building or structure, which is a Defence premise that is used wholly or in part for the storage of explosive ordnance, and where Australian Defence Force members are not normally present. To become a declared explosive ordnance depot, the site must be specified by the Minister in a legislative instrument under the Act, section 71L. In this legislative instrument, the site **must** be referred to either by its:

- a. geographical location; or
- b. unique code or number.

3. Signs stating that it is a condition of entry to the site that people consent to undergo searches, as provided by the Act Subdivision B, must be prominently displayed at the entrance to, and at regular intervals around the perimeter of the declared explosive ordnance depot.

4. Contracted Defence security guards on declared explosive ordnance depots have the same consensual identification and search powers as contracted Defence security guards at the other Defence premises.²⁸ Similarly, as at other Defence premises, contracted Defence security guards at declared explosive ordnance depots are not empowered to conduct non-consensual searches.

5. The special provisions for declared explosive ordnance depots empower a contracted Defence security guard to request a consensual limited search of a person or a consensual search of a vehicle anywhere on the depot, not just at an access control point.

6. Under *the Act*, section 71 M a contracted Defence security guard may request a person, who is on a declared explosive ordnance depot, to undergo a consensual limited search of their person, including items in their possession.

7. Under *the Act*, section 71N a contracted Defence security guard may request a person, who is apparently in control of a vehicle on a declared explosive ordnance depot, to permit a consensual search of the vehicle, including things in the vehicle.

8. A contracted Defence security guard may restrain and detain a person, or any other people in the vehicle (for the purpose of handing them over to a state or territory police officer at the earliest practicable time), if:

- a. the person refuses the consensual request; or
- b. as a result of complying with the request, the contracted Defence security guard reasonably believes that the person or vehicle, including a thing in the vehicle:
 - (1) is not authorised to be on the declared explosive ordnance depot;
 - (2) constitutes a threat to the safety of people on the declared explosive ordnance depot;
 - (3) in the case of a person, has or may commit a criminal offence on, or in relation to the declared explosive ordnance depot; or
 - (4) in the case of a vehicle, relates to a criminal offence that has or may be committed on, or in relation to the depot.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

²⁸ Refer to DSPF Control 76.1 – *Identification, Search and Seizure Regime* paragraphs 20 to 23 and 45 to 53 for further information

Document administration

Identification

DSPF Annex	Special Search Provisions For Declared Explosive Ordnance Depots
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	Control 76.1

Related information

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	DG ESD	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Defence Security Principles Framework (DSPF)

Security Incident Management and Investigation

General Principle

1. Defence will ensure that all security incidents are reported, investigated and dealt with in accordance with the relevant policies and legislation.

Rationale

2. Defence's ability to monitor the effectiveness of its security arrangements is supported by the accurate, timely, and consistent reporting of all security incidents across the enterprise.
3. A strong security incident reporting culture assists with the early identification of issues and trends to minimise the potential impact of security incidents and mitigate future occurrences.
4. The reporting of all security incidents to Security Incident Coordination Centre (SICC) provides Defence with enterprise oversight of security incidents and trends, providing additional incident management support and advice as required, conducting investigations when needed and identifying vulnerabilities across Defence.

Expected Outcomes

5. Defence has a strong security incident management culture where:
 - a. All personnel understand and meet their responsibilities for security incident management and reporting;
 - b. Security incidents are identified promptly and managed in accordance with the actual or potential damage of the incident to Defence;
 - c. Notification of security incidents is escalated within Services/Groups/Companies in accordance with their requirements;
 - d. All security incidents are reported to the Defence Security Incident Coordination Centre (SICC) via the Security Report;
 - e. Security incidents are assessed both individually and in aggregate, enabling the support, investigation, and, where appropriate, referral of security incidents to external security agencies;
 - f. Risk management principles underpin proportionate and consistent management of security incidents; and

- g. A pattern of learning from and strengthening security arrangements in response to security incidents is evident across defence.

Escalation Thresholds

Risk Rating	Responsibility
Low	Director Security Incident Coordination Centre
Moderate	Director Security Incident Coordination Centre or Assistant Secretary Security Threats and Assurance (ASSTA).
Significant	ASSTA
High	ASSTA
Extreme	First Assistant Secretary Security and Vetting Service (FAS S&VS) or nominated representative

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Security Incident Management and Investigation
Principle Owner	FAS S&VS
DSPF Number	Principle 77
Version	3
Publication date	03 May 2021
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 77.1
Control Owner	ASSTA

Related Information

Government Compliance	Protective Security Policy Framework – PSPF 5 Reporting on security Standards: Australian Government Investigations Standards 2011
See also DSPF Principle(s)	Principle 24 – Information Systems Principle 45 – Contact Reporting

Implementation Notes, Resources Tools	Defence Records Management Policy Manual Good Decision Making in Defence - A Guide for Decision Makers and Those Who Brief Them Incident Reporting and Management Incident Reporting and Management Manual (IRMMAN)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	02 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	03 May 2021	FAS S&VS	Updates to align with PSPF. Name change.



Defence Security Principles Framework (DSPF)

Security Incident Management and Investigation

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this Enterprise-wide control.

Escalation Thresholds

2. ASSTA has set the following general thresholds for variation from compliance with this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility
Low	Director Security Incident Coordination Centre
Moderate	Director Security Incident Coordination Centre or ASSTA.
Significant	ASSTA
High	ASSTA
Extreme	First Assistant Secretary Security and Vetting Service (FAS S&VS) or nominated representative

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Security Incident Management Is Everyone's Responsibility

3. Protecting the integrity of Defence's people, information and assets is vital to ensuring the organisation functions effectively and all personnel, regardless of service type, rank, or location, are responsible for upholding security within Defence.

Definition of a Security Incident

4. A Security Incident is a suspicious approach, event or action (whether deliberate, reckless, negligent or accidental) that:
 - a. fails to meet the expected outcomes of the DSPF
 - b. compromises Defence's protective security arrangements;
 - c. results in or has the potential to result in loss, damage, harm or disclosure to Defence's information, assets, and/or personnel.
5. There are a range of events that are security incidents; below are some examples:
 - a. Unauthorised access to Defence facilities;
 - b. Loss or theft of weapons, associated equipment (weapon parts, combat body armour, night fighting equipment and night vision equipment), and explosive ordnance including all ammunition, propellants, pyrotechnics, and explosives;
 - c. Unauthorised access to and/or use of Defence information and communications equipment or systems;
 - d. Inappropriate handling or storage of classified information, weapons, associated equipment, and explosive ordnance;
 - e. Loss, theft of, or unauthorised access to/or disclosure of official Defence information;
 - f. Security contacts where Defence Personnel are approached by, or communicate with, representatives of foreign interests, extremist or subversive groups, criminals, or commercially, politically or issue motivated groups whose purpose appears to be to obtain official information;
 - g. Any investigation or other action by civil police, either in Australia or overseas, that involves Defence people or Defence property;
 - h. Events of actual or suspected espionage and/or sabotage; and
 - i. Security incidents involving material classified PROTECTED and above.
6. There are other types of incidents that must be reported but which are not security incidents. Information on how to report and manage these incidents can be

found in the Incident Reporting Hub at
<http://drnet/AssociateSecretary/AFCD/Incident-Reporting/Pages/Home.aspx>.

Defence Industry Application of Control

7. This Control refers to the roles of Commander/Manager and Security Officer in the management and reporting of security incidents.

8. For Defence Industry Security Program (DISP) members, the terms Commander/Manager and Security Officer in this Control both refer to a DISP Member's Security Officer as defined in DSPF Control 16.1 – Defence Industry Security Program.

9. For persons engaged under a contract that are not DISP members, these terms mean:

- a. Commander/Manager: The Defence Commander/Manager responsible for the supervision or management of the work being performed by the contracted party; and
- b. Security Officer: The Defence Security Officer for the area within Defence engaging the contracted party.

Security Incident Reporting

10. Defence Personnel who identify a security incident has or may have occurred **must** inform their Commander/Manager and Security Officer as soon as possible (refer to paragraph 4 for the definition of a Security Incident).

11. Commanders/Managers are responsible for the management of security incidents that arise within or are identified by their Unit/Group/Company, including reporting the incident to the Defence Security Incident Coordination Centre (SICC).

12. Commanders/Managers **must** ensure that the immediate risk of harm to Defence Personnel, information, and assets is minimised as a priority before reporting.

13. Once the risk of immediate harm has been effectively managed, a Security Report **must** be submitted to SICC via the Security Report within 24 hours of the incident occurrence or discovery.
14. Commanders/Managers should ensure notification and/or management of all security incidents are escalated in accordance with Unit/Group/Company requirements as soon as possible.
15. For security incidents involving persons engaged under a contract (whether DISP members or not), the relevant Defence Contract Manager **must** also be notified of the incident.
16. The Security Report is available via the Defence Protected Network (DPN) homepage, on the Defence Online Services Domain (DOSD) portal for DISP members, from your local Security Officer, and Defence Contract Manager.
17. Certain security incident types may require additional reporting beyond the preparation and submission of the Security Report. Additional reporting requirements are detailed in **Annex A** of this Control.

Reporting incidents involving classified information

18. A Security Report must be prepared and submitted on the appropriately rated ICT Network. PROTECTED information can only be provided via the DPN and in accordance with DSPF Control 10.1 – *Assessing and Protecting Official Information*
19. Security Reports lodged with SICC by unsecure means **must not** contain any sensitive or classified information.
20. If reporting a security incident requires the inclusion of SECRET information, report the incident to SICC via the Security Report on the DPN, excluding any SECRET information but noting the SECRET information will be provided separately. Once lodged, provide the SECRET information relevant to the security incident via the DSN to Security.Incident.Centre@jcse.defence.gov.au quoting the Security Report reference number.
21. TOP SECRET information can only be provided to SICC by special arrangement. In these circumstances, report the incident to SICC via the Security Report on the DPN, excluding any classified information but noting the TOP SECRET information will be provided separately.

Prompt reporting matters

22. The prompt reporting of security incidents ensures:
- a. Accurate and timely records are made of the security incident;
 - b. An effective and timely response to the security incident is implemented;
 - c. Timely advice and specialist support can be provided to Commanders/Managers to enable effective security incident management; and
 - d. Strategic oversight of security risk and incident management by Defence leadership is possible.

Things to include when reporting an incident

23. To provide the most benefit from security incident reporting, personnel should consider the following factors to ensure a complete and accurate report can be made:
- a. Time and location of security incident;
 - b. How the incident was detected and by whom;
 - c. Type of assets or resources affected or exposed to risk;
 - d. Description of the circumstances of the security incident;
 - e. Nature or intent of the security incident where possible, e.g. deliberate, or accidental;
 - f. Assessment of the actual or potential degree of harm or business impact arising from the security incident;
 - g. Whether it is an isolated incident or a reoccurring issue;
 - h. Summary of immediate action taken and management strategies to reduce or mitigate the actual or potential harm of business impact arising from the security incident; and
 - i. What actions need to be taken to avoid a recurrence of the security incident in the future.
24. The Security Incident Impact Level (SIIL) is the actual or potential impact of a security incident on Defence's ability to conduct business operations. SIILs can be LOW, MEDIUM, HIGH, or EXTREME; guidance to assist with assessing the Security Incident Impact Level is at **Annex B**.

Assistance when reporting an incident

25. For assistance in assessing the nature and impact of a security incident, personnel should first consult their Commander/Manager and Security Officer. Additional assistance can be found on the Associate Secretary's advice on [Defence Business Impact Analysis](#).

26. If further guidance is required, contact:

- a. **Telephone:** 1800 Defence (1800 333 362)
- b. **DPN:** Security.IncidentCentre@defence.gov.au
- c. **DSN:** Security.IncidentCentre@jcse.defence.gov.au

Security Incident Management

27. Commanders/Managers are responsible for the management of security incidents that arise within their Unit/Group/Company from identification through to closure (unless referred to an Investigative Authority).

28. SICC provides security incident management advice to incident managers when required to enable the effective management of security incidents and ensure that Defence reduces, where possible, the impact on capability while also meeting its reporting obligations to the Commonwealth. In some circumstances, security incidents may result in investigation by the Security Investigations Unit (SIU) or another Defence Investigative Authority (DIA).

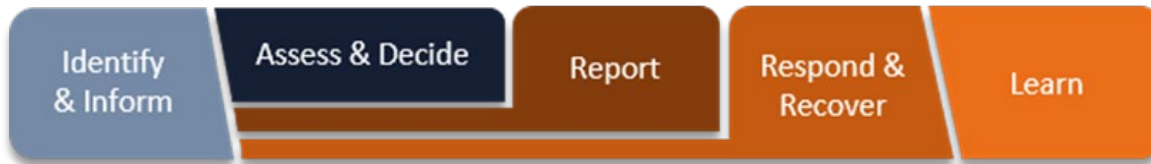
29. When SICC refers a security incident to another entity for advice or support, that entity assumes responsibility for supporting the security incident to closure, or until such time as it is referred back to SICC.

Security Incident Management Process

30. Security incident management is the process of identifying, managing, reporting, and learning from irregular or adverse activities or events, threats, and behaviours.

31. Effective management of security incidents is fundamental to enabling a safe and secure operating environment and relies on a positive security culture with a strong understanding of protective security policies and practices.

32. Defence Personnel and persons engaged under a contract should follow the following process to manage security incidents effectively and comprehensively:



Identify and Inform

33. Defence Personnel and persons engaged under a contract who identify that a security incident has or may have occurred **must** inform their chain of command (Commander/Manager) and/or Security Officer as soon as possible (refer Paragraph 4 for the definition of a Security Incident).

34. Where a security incident involves actual or suspected criminal activity including theft or serious damage, the AFP, local police or Joint Military Police Unit (JMPU) should be contacted immediately, while also notifying the Commander/Manager and/or Security Officer.

35. For emergencies or potentially life-threatening situations contact the AFP, local police, or JMPU) immediately.

Assess and Decide

36. Once aware that a security incident has or may have occurred within their area of responsibility, Commanders/Managers with support from Security Officers should take all reasonable actions within their remit to:

- a. ascertain the nature of the incident;
- b. assess the actual or potential impact of the incident on Defence assets or business operations, and
- c. decide what action is required to recover from and prevent future recurrence of the security incident.

37. In assessing the security incident and determining an appropriate response, Commanders/Managers should consider the actual or potential Security Incident Impact Level (SIIL) to Defence of the incident occurring. Guidance for the assessment of the Security Incident Impact Level is at **Annex B**.

Report

38. Security incidents **must** be reported centrally to SICC using the standard Security Report.
39. Reporting security incidents should occur once the immediate risk of harm is minimised, but as noted earlier, **must** occur within 24 hours of the incident occurring or being identified.
40. Commanders/Managers should ensure security incidents are escalated in accordance with Unit/Group/Company requirements as soon as possible.
41. If subsequent, relevant information comes to light in the process of responding to and recovering from a security incident, Commanders/Managers are to advise SICC by sending an email to Security.IncidentCentre@defence.gov.au containing the original security incident report reference number.
42. Security incidents involving classified information are to be reported to SICC as detailed in [Reporting incidents involving classified information](#).

Respond and Recover

43. Commanders/Managers should respond to and recover from security incidents in an effective and timely manner to minimise the potential impact of an incident and to help prevent a recurrence of the security incident.
44. In the course of responding to a security incident, a Commander/Manager may need to conduct a Fact Find to gain more information to identify vulnerabilities and determine the appropriate treatment action to contain the situation.
45. Commanders/Managers should not conduct a Fact Find into security incidents with an assessed SIIL of HIGH or EXTREME until directed by SICC, the SIU or a DIA.
46. Commanders/Managers should be aware that a Fact Find is not an investigation and care should be taken to conduct Fact Finds without compromising potential future investigations. For guidance, refer to ['Good Decision Making in Defence'](#) guide.

47. Commanders/Managers are responsible for the management of security incidents reported to them until:

- a. All reasonable responses to limit the impact of a security incident have been implemented,
- b. All reasonable actions to prevent future recurrence have been completed, or
- c. Responsibility for investigating the incident has been referred to an appropriate internal or external investigative authority.

48. Notwithstanding the rights and interests of an individual potentially adversely affected by a security investigation, all Defence personnel and persons engaged under a contract **must** afford all reasonable assistance to, and comply with reasonable directions given by, personnel from an internal or external investigative authority to prevent any impediment or interference with the investigation or inquiry process. All Defence personnel and personnel engaged under a contract **must not** direct or obstruct an external agency or DIA in the execution of their duties or disclose any part of an investigation without the prior approval of the investigator.

Learn

49. Defence Personnel should learn from security incidents to continuously improve security risk management practices, reduce the likelihood of recurrences, and minimise the consequences of future incidents.

50. Commanders/Managers should take all reasonable actions within their remit to ensure that the conditions which enabled a security incident to occur are appropriately controlled to mitigate the risk of recurrence.

51. The SICC analyses trends in security incident management data to inform strategic decision making and support continuous improvement of security measures.

Record Keeping

52. Commanders/Managers, with support from Security Officers, **must** maintain records within the Unit/Group/Company regarding all security incidents that occur within their remit. These records include a copy of the lodged Security Report and any subsequent documents generated through the Security Incident Management process, including outcomes of any Fact Finds.

53. The Security Officer is responsible for the custody and maintenance of security incident records.

54. SICC maintains a record of all Security Reports in a centralised case management database, the Defence Policing Security Management System (DPSMS).

55. In managing security incident record keeping, Security Officers are to apply the standards in the [Defence Records Management Policy Manual \(RECMAN\)](#).

Security Investigations

56. A security investigation is the process of seeking information relevant to an alleged, apparent, or potential breach of Defence security policy or failure of security controls. The primary purpose of a security investigation is to:

- a. gather sufficient evidence to conclude whether security risk controls have failed or are failing to mitigate security risks and provide recommendations on how controls can be modified to improve their effectiveness and/or
- b. gather admissible evidence for any subsequent action, whether under criminal, civil penalty, disciplinary, or administrative sanctions relating to the breach of security policy.

57. The SICC assesses which security incidents are escalated to investigation by a DIA after consulting the relevant DIA Commander/Manager. The SIU is a designated DIA which has been established to conduct investigations of complex or serious actual or suspected breaches of security policy and failures of security controls.

58. Investigations undertaken by the SIU are conducted in accordance with the requirements of the PSPF and the Australian Government Investigations Standards (AGIS) where appropriate.

Security Investigation Outcomes

59. Security investigations aim to establish the root cause of security matters and provide recommendations to prevent a reoccurrence and the future risk of harm to Defence.

60. Should an investigation confirm an actual breach of security policy, the investigation will provide evidence to whichever party is to conduct the resultant sanctioning response.

61. Where an investigation identifies failure of a security control/s, the investigation will provide recommendations to remediate the issue to the relevant Control Owner/s.

Security Incident Management Roles

Commander/Managers

62. Commanders/Managers are responsible for the management and reporting of security incidents that occur within their Unit/Group/Company.

Contract Manager

63. Contract Managers are responsible for monitoring compliance of Contractors, Consultants, Outsourced Service Providers, and other persons engaged under a contract with the terms of their contractual arrangements, including contractual security obligations.

64. Contract Managers should consider reported security incidents when monitoring compliance with contractual security obligations.

Security Officer

65. Each Unit and Group **must** designate a Security Officer who has completed the Defence Security Officer training course. The Security Officer will be able to recognise security risks and support Defence Personnel, including Commanders/Managers, to manage and report security incidents. This will also include maintaining records of security incidents that occur within their Unit and Group and how they were managed.

66. DISP members should refer to DSPF Control 16.1 – Defence Industry Security Program for security role requirements.

Security Incident Coordination Centre

67. SICC within DS&VS maintains a centralised record of all received Security Reports and provides advice and support as required to Defence Personnel in the management of security incidents.

Security Investigations Unit

68. The SIU is a designated DIA which has been established to conduct investigations of actual or suspected breaches of security policy, and actual or potential failures of security controls.

Security Incident Information Management

69. The release of Official Information in response to a freedom of information request is to be completed in accordance with the *Freedom of Information Act 1982* (the FOI Act). For advice, contact the Freedom of Information Directorate.

70. SICC refers or reports security incidents to external Agencies in accordance with the requirements of the PSPF.

Annexes and Attachments

Annex A - Additional Reporting Requirements

Annex B – Security Incident Impact Level (SIIL) Assessment Guide

Document administration

Identification

DSPF Control	Security Incident Management and Investigation
Control Owner	Assistant Secretary Security Threat and Assurance
DSPF Number	Control 77.1
Version	4
Publication date	4 February 2022
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Security Incident Management and Investigation
Related DSPF Control(s)	10.1 – Assessing and Protecting Official Information

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	02 July 2018	ASSTA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	03 May 2021	ASSTA	Major updates including introduction of SIILs and new Security Report. Control name change.
4	4 February 2022	ASSTA	Changes to mandatory provisions in paragraph 48 and 57



Defence Security Principles Framework (DSPF)

Annex A to Security Incident Management and Investigation – Additional Reporting Requirements

1. In addition to the security incident reporting requirements described in Control 77.1, the subjects of some incidents may result in the need for additional reporting.

Asset Loss

2. In the case of a loss of asset in any manner (deliberate or accidental), the loss may have to be reported as a financial incident in addition to a security incident. For further information, refer to the [Financial Management Manual 5 \(FINMAN 5\)](#).
3. Loss of controlled items, including Defence and dual-use goods, technology acquired under licence and technology subject to export controls, may have additional reporting requirements. The Defence Export Control Branch and the [Defence Logistics Manual \(DEFLOGMAN\)](#) should be consulted in these cases.

Radioactive Sources

4. Where a security incident involves a sealed radioactive source, the Australian Government Code of Practice for the Security of Radioactive Sources takes precedence over the DSPF and specific incident notification requirements apply for immediate notification to appropriate authorities. For further information see DSPF [Principle 80 Security of Radioactive Sources](#).

Weapons

5. On discovering the loss or suspected loss, theft or attempted theft, recovery, discovery, or suspicious incidents involving Defence weapons, cadet firearms, and associated equipment related to weapons, the person in charge is required to:
 - a. immediately report the matter to the appropriate authority in their Group or Service;
 - b. notify the [Joint Military Police Unit \(JMPU\)](#) and local civilian police;

- c. notify the Stock Item Owner within 24 hours; and
 - d. immediately report the incident through the submission of a Security Report to the Security Incident Coordination Centre (SICC).
6. For further information see DSPF [Principle 78 Weapons Security](#).

Explosive Ordnance

7. If an attempted theft or suspicious event is in progress the police are to be called immediately.
8. If a loss or suspected loss, theft or attempted theft, recovery, discovery, or suspicious incidents involving explosive ordnance is discovered the person in charge is required to immediately:
- a. report the matter through the Chain of Command and Unit Security Officer in their Group or Service;
 - b. notify the JMPU;
 - c. complete a [Security Report](#) selecting 'Non ICT Equipment eg weapons, vehicles, ordnance' as the asset involved, and 'EO/munitions' as the type of equipment, submit the resulting incident report to the SICC.
9. For further information see [DSPF Principle 79 Explosive Ordnance Security](#).

Free From Explosive violations

10. Free From Explosive (FFE) violations are to be reported through a [Security Report](#) selecting 'Non ICT Equipment e.g. weapons, vehicles, ordnance' as the asset involved, and 'EO/munitions' as the type of equipment, submit the resulting incident report to the SICC.

Communications security and cryptography

11. Communications security and cryptography breaches, including the loss or recovery of any cryptographic controlled item where there is no suspicion of espionage, are to be reported to the Defence Cryptographic Controlling Authority in accordance with the reporting procedures contained in [Australian Communications Security Instruction \(ACSI\) Reporting and Evaluating COMSEC Incidents](#) and Defence Communications Security Accounting and Management Manual (DEFCAMMAN).

12. The [Defence Logistics Manual \(DEFLOGMAN\)](#) should also be consulted in these cases.

Reporting the loss of Official Information

13. The Protective Marking of lost information will determine the actual or potential business impact level of the security incident to Defence.

14. When an incident occurs involving sensitive or classified information and the reporting entity/unit is not the information originator, then the originator, if identified and located, is to be notified and asked to provide a damage assessment. If the originator cannot be identified or located, it is recommended that a subject matter expert is identified and consulted to assist with the damage assessment.

15. The reporting entity/unit for the loss is to provide the following information to an SES Band 1/ADF O7 level officer within the reporting entity/unit's line management or chain of command before write-off action can be authorised by that SES Band 1/ADF O7 level officer:

- a. the information to be written off;
- b. the sensitivity or classification level of the information;
- c. the damage assessment (whether on the Security Report or subsequently provided); and
- d. a copy of any associated documentation:
 - (1) a Minute requesting write-off approval from the relevant SES Band 1 / ADF O7, to be signed by the Commander/Manager;
 - (2) any Fact Finding or administrative inquiry report;
 - (3) any investigation report provided by a Defence Investigative Authority.

16. Following approval to write off of Official Information, and if the lost information was registered in a Classified Document register (CDR):

- a. the lost information entries are to be identified in the CDR;
- b. the serial number in the CDR is to be ruled out and all relevant information annotated in the 'remarks' column;

- c. any records relating to the lost information is to be correctly amended and, where lost information is replaced, the new entry needs to be cross-referenced to the original entry;
- d. an independent officer is to record their signature to each serial that is declared missing in the CDR;
- e. any other record(s) listing the lost information is to be amended accordingly; and
- f. a copy of the approved minute requesting write-off together with any Annexes and Enclosures is to be sent via email to the SICC.

Cabinet Material

17. Commanders/Managers are to report actual or suspected security incidents involving Cabinet material to the Cabinet Secretariat in the Department of the Prime Minister and Cabinet. The Cabinet Handbook and DSPF Control 10.1 – Assessing and Protecting Official Information provide information about the security and handling of Cabinet documents.

Anonymous Reporting and Public Interest Disclosure

18. Defence encourages Defence personnel and persons engaged under a contract who have serious security concerns and believe themselves to be at risk of recrimination if they report a security incident to use the reporting provisions of the Defence Public Interest Disclosure scheme.

Personal Information and Notifiable Data Breaches

19. Incidents involving the disclosure of personal information need to consider management and reporting requirements of the Notifiable Data Breach scheme (established under Part IIIC of the *Privacy ACT 1988* (Cth)).

20. Under the Notifiable Data Breach scheme, Defence is required to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. Such breaches are referred to as 'eligible data breaches'. Notifications must include recommendations regarding the steps individuals should take in response to the breach.

21. Further information in relation to the Notifiable Data Breach scheme, including management and response to data breaches, is available on the Office of the Australian Information Commissioner website.

22. Data breaches, including suspected eligible data breaches, are to be managed by the area collecting the personal information and responsible for its protection and security.

23. Suspected eligible data breaches are to be notified to Defence Privacy who will advise commanders and managers regarding reporting to the Office of the Australian Information Commissioner.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Additional Reporting Requirements
Annex Version	3
Annex Publication date	03 May 2021
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Security Incident Management and Investigation
DSPF Number	Control 77.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	02 July 2018	ASSTA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin policy.
3	03 May 2021	ASSTA	Update to align with updated Control 77.1 and change name from 'Special Reporting Requirements' to 'Additional Reporting Requirements'.

Defence Security Principles Framework (DSPF)

Annex B to Security Incident Management and Investigation – Security Incident Impact Level (SIIL)			
Security Incident Impact Levels - Principles			
Low	Medium	High	Extreme
Limited damage to the Defence interest, military or business unit, individuals and/or unlikely to cause reputational damage.	Damage to the Defence interest, military or business unit, or individuals, limited localised reputational damage.	Serious damage to the Defence interest, military or business unit, individuals, possible damage to national interest, national media attention and possible short-term reputational damage	Exceptionally grave damage to Defence interest, military or business unit, multiple individuals, actual damage to national interest, sustained national media attention and reputational damage
Physical Assets			
Facility, Base, Building - Minor damage or vandalism to Defence facility, base or building - Loss of ID/access pass - Failure to report lost ID/access pass	- Damage or vandalism to Defence facility, base or building requiring remediation - Non-compliance with defence physical security policy relating to facility/base or building access - Threat to defence facility, base or building	- Serious damage to defence facility, base or building impacting the operations or compromising the level of security - Multiple incidents relating to non-compliance with defence physical security policy - Suspected reconnaissance of defence facility, base or building - Credible threat to defence facility, base or building	Significant damage to defence facility, base or building causing a cessation of operations and unacceptable level of risk to defence assets including personnel
Armoury, Weapons, ammunition, explosive ordnance - Loss or unaccounted part of weapon - Loss or unaccounted minor quantities of small arms ammunition, up to 50 calibre, training aids and inert items of explosive ordnance <i>Note: minor quantities are considered as a volume error of less than 2%; or the total value is less than \$250</i> - An occurrence of unaccompanied access to armoury or explosive ordnance store house (ESH) by Defence or contractor personnel	- Recovery of weapon, weapon part - Loss or unaccounted ammunition greater than 50 calibre or explosive ordnance including training aids or inert items that by their nature may cause alarm. - Failure to secure armoury by Defence or contractor personnel	- Loss or unaccounted complete weapon(s) - Loss or unaccounted explosive ordnance that can be used as a standalone ‘weapon system’ in their own right or are readily usable as part of an IED. This includes items such as grenades, demolition stores and detonators - Recovery of unreported weapon, ammunition or explosive ordnance including training aids or inert items of explosive ordnance. - Attempted theft of weapon, ammunition or explosive ordnance including training aids or inert items of explosive ordnance. - Loss of keys, cards or other access devices associated with weapon, ammunition or explosive ordnance security or storage - Inappropriate storage, use or transport of weapon, ammunition or explosive ordnance	- Loss or theft of multiple weapons - Loss or theft of significant quantities of ammunition or explosive ordnance - Compromise of, or unauthorised access to, an explosive ordnance storage facility or of explosive ordnance during a transport activity - Theft of keys, cards or other access devices associated with weapon, ammunition or explosive ordnance security or storage
Security Enhanced Radioactive Sources Unauthorised disclosure that Defence holds Security Enhanced Sources	Unauthorised disclosure of the location of Defence’s Security Enhanced Sources	- Disclosure of the composition of Security Enhanced Sources in Defence Radioactive waste - Theft, loss or damage to a security enhanced source whilst being transported under an approved transport plan (i.e. on a public road). - Subsequent reporting of a security enhanced source incident in the media.	- Unauthorised (actual or attempted) access to a security enhanced source whilst in storage or transit (ie on Defence property or in Defence vehicle). - Theft, loss or damage to a security enhanced source whilst in storage (ie on Defence property). - Verified use of a Defence security enhanced source by terrorists in a ‘dirty bomb’.
Defence Vehicles Minor damage or vandalism to Defence “white fleet” vehicle	Vandalism causing minor damage to Defence operational vehicle or theft of “white fleet” vehicle	Attempted theft, suspected or actual theft of Defence operational vehicle.	Theft of Defence armed operational vehicle

<u>Security Incident Impact Levels - Principles</u>			
Low	Medium	High	Extreme
Limited damage to the Defence interest, military or business unit, individuals and/or unlikely to cause reputational damage.	Damage to the Defence interest, military or business unit, or individuals, limited localised reputational damage.	Serious damage to the Defence interest, military or business unit, individuals, possible damage to national interest, national media attention and possible short-term reputational damage	Exceptionally grave damage to Defence interest, military or business unit, multiple individuals, actual damage to national interest, sustained national media attention and reputational damage
<u>Official or Classified Information</u>			
- Loss or unauthorised disclosure of OFFICIAL information relating to internal policies or Defence personnel - Inappropriate storage, transport or disposal of OFFICIAL information	- Loss of large amounts of OFFICIAL information - Loss or unauthorised disclosure of small amounts of classified information classified at the PROTECTED level - Inappropriate storage, transport, or disposal of PROTECTED information	- Loss or unauthorised disclosure of large amounts of information classified PROTECTED - Loss or unauthorised disclosure of SECRET information - Inappropriate storage, transport, or disposal of SECRET information	- Loss or unauthorised disclosure of large amounts of information classified SECRET - Loss or unauthorised disclosure of TOP SECRET information - Inappropriate storage, transport or disposal of TOP SECRET information - Loss or theft of cryptographic equipment or COMSEC material
<i>Compromise of foreign classified information</i>	Suspected loss, loss or unauthorised disclosure of small amounts of OFFICIAL foreign information not publicly available	- Suspected loss, loss or unauthorised disclosure of small amounts of foreign classified information - Suspected loss, loss or unauthorised disclosure of large amounts of OFFICIAL foreign information not publicly available	Suspected loss, loss or unauthorised disclosure of large amounts of foreign classified information
<i>Foreign release of official information</i> Unauthorised disclosure of small amounts of OFFICIAL information to a foreign national	Unauthorised disclosure of large amounts of OFFICIAL information to a foreign national	Unauthorised disclosure of small amounts of information classified PROTECTED to a foreign national	- Unauthorised disclosure of information classified SECRET or TOP SECRET to a foreign national - Unauthorised disclosure of large amounts of any classified information to a foreign national
<u>Defence or Defence Industry Personnel</u>			
<i>Foreign interference, Espionage and Contact Reporting</i> Defence personnel (non-targeted) contacted electronically (email, social media, online forum) by suspected foreign intelligence service seeking information	Defence personnel targeted electronically (email, social media, online forum) by suspected foreign intelligence service seeking information	Defence personnel targeted by suspected foreign intelligence service in person	Defence personnel compromised by foreign intelligence service in person
<i>Security Incidents Impacting Defence Personnel</i> Limited harm to Defence or Defence Industry Personnel – could cause harm to individuals including injuries that are not serious or life threatening	- Threat to harm Defence Personnel - Endangering individuals - the compromise of information could lead to serious harm or potentially life-threatening injury to an individual - Defence Personnel targeted electronically (email, social media, online forum) by suspected foreign intelligence service seeking information	- Incident involving physical or psychological harm to defence personnel - Endangering small groups of individuals - the compromise of information could lead to serious harm or potentially life-threatening injuries to a small group of individuals - Defence personnel targeted by foreign intelligence service in person	- Incident involving physical or psychological harm to multiple defence personnel - Compromise of information that is expected to lead to loss of life of an individual or small group with the potential for widespread loss of life
<i>Security Incidents caused by Defence personnel</i> Unexpected/erratic/out of character behaviour by Defence Personnel	- Defence Personnel with security clearance displays behaviours of concern or dramatic change in behaviour - Defence Personnel identified with POI, issue motivated group	Defence or industry personnel intentionally disclose official or PROTECTED information to unauthorised individual	- Defence or industry personnel intentionally disclose SECRET or TOP SECRET information to unauthorised individual - Defence personnel intentionally disclose any official information to foreign entity or intelligence service

Security Incident Impact Levels - Principles			
Low	Medium	High	Extreme
Limited damage to the Defence interest, military or business unit, individuals and/or unlikely to cause reputational damage.	Damage to the Defence interest, military or business unit, or individuals, limited localised reputational damage.	Serious damage to the Defence interest, military or business unit, individuals, possible damage to national interest, national media attention and possible short-term reputational damage	Exceptionally grave damage to Defence interest, military or business unit, multiple individuals, actual damage to national interest, sustained national media attention and reputational damage
ICT Systems, Infrastructure or Hardware			
- Loss of ICT equipment or UNCLASSIFIED hardware - Misuse of ICT system - Incorrect storage, transportation or disposal of ICT equipment or hardware	- Theft of ICT equipment or hardware - Suspicious ICT event such as spam or phishing	- Unauthorised access to system or defence terminal - Sharing or misuse of ICT credentials (password sharing) - Unauthorised or suspected access to ICT server or server room by unauthorised individual - Loss of ICT hardware containing sensitive or classified information	- Loss of significant levels of data or data spill - Loss of, or confirmed compromise of critical ICT infrastructure such as data warehouse - Loss or theft of cryptographic equipment or COMSEC material

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Security Incident Impact Levels (SIIL) Assessment Guide
Annex Version	1
Annex Publication date	03 May 2021
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Security Incident Management and Investigation
DSPF Number	Control 77.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	03 May 2021	ASSTA	Launch



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Weapons Security

General principle

1. All Defence weapons and Cadet Firearms are to be secured or controlled to prevent loss, theft or misuse. Defence weapons are to be stored in accordance with Defence security policy.

Rationale

2. Defence holds weapons that are illegal for possession by the general population. This makes Defence weapons attractive to criminal elements, including extremist organisations and malicious trusted insiders. As a result, there is an increased risk that criminal elements may target Defence armouries, repair facilities, personnel, and associated transportation activities as potential sources of these items.

3. There is also a significant potential risk to weapons security from Defence personnel and persons engaged under a contract. Theft by Defence personnel or persons engaged under a contract can be opportunistic and can occur where supervision and checking procedures have not properly taken account of this threat.

Expected outcomes

4. Defence weapons are adequately stored to prevent loss, theft and misuse.

5. Only appropriately cleared and trained personnel have access to Defence weapons.

6. Defence has controls or procedures in place to detect the loss, theft and attempted theft of weapons within specific timeframes.

Escalation Thresholds

Risk Rating	Responsibility
Low	O4 or APS 6 or equivalent in the relevant Group/Service
Moderate	O5 or EL 1 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.

Document administration

Identification

DSPF Principle	Weapons Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 78
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 78.1
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Document administration

Identification

DSPF Control	Security Incident Management and Investigation
Control Owner	Assistant Secretary Security Threat and Assurance
DSPF Number	Control 77.1
Version	3
Publication date	03 May 2021
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Security Incident Management and Investigation
Related DSPF Control(s)	10.1 – Assessing and Protecting Official Information

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	02 July 2018	ASSTA	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	03 May 2021	ASSTA	Major updates including introduction of SIILs and new Security Report. Control name change.

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security planning; Security governance for international sharing; and Entity physical resources. Legislation: <u>Workplace Health and Safety Act 2011</u> (Cth)
Read in conjunction with	- Interim Capability Life Cycle Manual - Estimates Memorandum 2015/51 – Defence Specific Costing Requirements for Projects in the Defence Integrated Investment Programme.
See also DSPF Principle(s)	- Security Incidents and Investigations - Physical Transfer of Official Information, Security Protected and Classified Assets - Physical Security - Escorting Security Protected or Classified Assets - SAFEBASE
Implementation Notes, Resources and Tools	- Australian Government physical security management protocol: <u>https://www.protectivesecurity.gov.au/physicalsecurity/Pages/Protocol.aspx</u> - Security Equipment Guides (SEGs) via the Security Toolkit. - ASIO Tech Notes via the Security Toolkit. <u>Security Equipment Evaluated Product List</u> (SEEPL). This list contains products endorsed by the Security Construction and Equipment Committee (SCEC). Contact 1800DEFENCE, your Executive Security Advisor (ESA), or your DS&VS regional office for further information.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	7 August 2019	FAS S&VS	PSPF Aligned
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Security Incident Management and Investigation

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this Enterprise-wide control.

Escalation Thresholds

2. ASSTA has set the following general thresholds for variation from compliance with this Defence Security Principles Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility
Low	Director Security Incident Coordination Centre
Moderate	Director Security Incident Coordination Centre or ASSTA.
Significant	ASSTA
High	ASSTA
Extreme	First Assistant Secretary Security and Vetting Service (FAS S&VS) or nominated representative

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Security Incident Management Is Everyone's Responsibility

3. Protecting the integrity of Defence's people, information and assets is vital to ensuring the organisation functions effectively and all personnel, regardless of service type, rank, or location, are responsible for upholding security within Defence.

Definition of a Security Incident

4. A Security Incident is a suspicious approach, event or action (whether deliberate, reckless, negligent or accidental) that:
 - a. fails to meet the expected outcomes of the DSPF
 - b. compromises Defence's protective security arrangements;
 - c. results in or has the potential to result in loss, damage, harm or disclosure to Defence's information, assets, and/or personnel.
5. There are a range of events that are security incidents; below are some examples:
 - a. Unauthorised access to Defence facilities;
 - b. Loss or theft of weapons, associated equipment (weapon parts, combat body armour, night fighting equipment and night vision equipment), and explosive ordnance including all ammunition, propellants, pyrotechnics, and explosives;
 - c. Unauthorised access to and/or use of Defence information and communications equipment or systems;
 - d. Inappropriate handling or storage of classified information, weapons, associated equipment, and explosive ordnance;
 - e. Loss, theft of, or unauthorised access to/or disclosure of official Defence information;
 - f. Security contacts where Defence Personnel are approached by, or communicate with, representatives of foreign interests, extremist or subversive groups, criminals, or commercially, politically or issue motivated groups whose purpose appears to be to obtain official information;
 - g. Any investigation or other action by civil police, either in Australia or overseas, that involves Defence people or Defence property;
 - h. Events of actual or suspected espionage and/or sabotage; and
 - i. Security incidents involving material classified PROTECTED and above.
6. There are other types of incidents that must be reported but which are not security incidents. Information on how to report and manage these incidents can be

found in the Incident Reporting Hub at
<http://drnet/AssociateSecretary/AFCD/Incident-Reporting/Pages/Home.aspx>.

Defence Industry Application of Control

7. This Control refers to the roles of Commander/Manager and Security Officer in the management and reporting of security incidents.
8. For Defence Industry Security Program (DISP) members, the terms Commander/Manager and Security Officer in this Control both refer to a DISP Member's Security Officer as defined in DSPF Control 16.1 – Defence Industry Security Program.
9. For persons engaged under a contract that are not DISP members, these terms mean:
 - a. Commander/Manager: The Defence Commander/Manager responsible for the supervision or management of the work being performed by the contracted party; and
 - b. Security Officer: The Defence Security Officer for the area within Defence engaging the contracted party.

Security Incident Reporting

10. Defence Personnel who identify a security incident has or may have occurred **must** inform their Commander/Manager and Security Officer as soon as possible (refer to paragraph 4 for the definition of a Security Incident).
11. Commanders/Managers are responsible for the management of security incidents that arise within or are identified by their Unit/Group/Company, including reporting the incident to the Defence Security Incident Coordination Centre (SICC).
12. Commanders/Managers **must** ensure that the immediate risk of harm to Defence Personnel, information, and assets is minimised as a priority before reporting.

13. Once the risk of immediate harm has been effectively managed, a Security Report **must** be submitted to SICC via the Security Report within 24 hours of the incident occurrence or discovery.
14. Commanders/Managers should ensure notification and/or management of all security incidents are escalated in accordance with Unit/Group/Company requirements as soon as possible.
15. For security incidents involving persons engaged under a contract (whether DISP members or not), the relevant Defence Contract Manager **must** also be notified of the incident.
16. The Security Report is available via the Defence Protected Network (DPN) homepage, on the Defence Online Services Domain (DOSD) portal for DISP members, from your local Security Officer, and Defence Contract Manager.
17. Certain security incident types may require additional reporting beyond the preparation and submission of the Security Report. Additional reporting requirements are detailed in **Annex A** of this Control.

Reporting incidents involving classified information

18. A Security Report must be prepared and submitted on the appropriately rated ICT Network. PROTECTED information can only be provided via the DPN and in accordance with DSPF Control 10.1 – *Assessing and Protecting Official Information*
19. Security Reports lodged with SICC by unsecure means **must not** contain any sensitive or classified information.
20. If reporting a security incident requires the inclusion of SECRET information, report the incident to SICC via the Security Report on the DPN, excluding any SECRET information but noting the SECRET information will be provided separately. Once lodged, provide the SECRET information relevant to the security incident via the DSN to Security.Incident.Centre@jcse.defence.gov.au quoting the Security Report reference number.
21. TOP SECRET information can only be provided to SICC by special arrangement. In these circumstances, report the incident to SICC via the Security Report on the DPN, excluding any classified information but noting the TOP SECRET information will be provided separately.

Prompt reporting matters

22. The prompt reporting of security incidents ensures:
- a. Accurate and timely records are made of the security incident;
 - b. An effective and timely response to the security incident is implemented;
 - c. Timely advice and specialist support can be provided to Commanders/Managers to enable effective security incident management; and
 - d. Strategic oversight of security risk and incident management by Defence leadership is possible.

Things to include when reporting an incident

23. To provide the most benefit from security incident reporting, personnel should consider the following factors to ensure a complete and accurate report can be made:

- a. Time and location of security incident;
- b. How the incident was detected and by whom;
- c. Type of assets or resources affected or exposed to risk;
- d. Description of the circumstances of the security incident;
- e. Nature or intent of the security incident where possible, e.g. deliberate, or accidental;
- f. Assessment of the actual or potential degree of harm or business impact arising from the security incident;
- g. Whether it is an isolated incident or a reoccurring issue;
- h. Summary of immediate action taken and management strategies to reduce or mitigate the actual or potential harm of business impact arising from the security incident; and
- i. What actions need to be taken to avoid a recurrence of the security incident in the future.

24. The Security Incident Impact Level (SIIL) is the actual or potential impact of a security incident on Defence's ability to conduct business operations. SIILs can be LOW, MEDIUM, HIGH, or EXTREME; guidance to assist with assessing the Security Incident Impact Level is at **Annex B**.

Assistance when reporting an incident

25. For assistance in assessing the nature and impact of a security incident, personnel should first consult their Commander/Manager and Security Officer. Additional assistance can be found on the Associate Secretary's advice on [Defence Business Impact Analysis](#).

26. If further guidance is required, contact:

- a. **Telephone:** 1800 Defence (1800 333 362)
- b. **DPN:** Security.IncidentCentre@defence.gov.au
- c. **DSN:** Security.IncidentCentre@jcse.defence.gov.au

Security Incident Management

27. Commanders/Managers are responsible for the management of security incidents that arise within their Unit/Group/Company from identification through to closure (unless referred to an Investigative Authority).

28. SICC provides security incident management advice to incident managers when required to enable the effective management of security incidents and ensure that Defence reduces, where possible, the impact on capability while also meeting its reporting obligations to the Commonwealth. In some circumstances, security incidents may result in investigation by the Security Investigations Unit (SIU) or another Defence Investigative Authority (DIA).

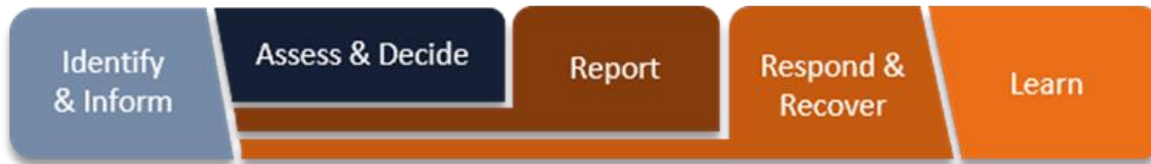
29. When SICC refers a security incident to another entity for advice or support, that entity assumes responsibility for supporting the security incident to closure, or until such time as it is referred back to SICC.

Security Incident Management Process

30. Security incident management is the process of identifying, managing, reporting, and learning from irregular or adverse activities or events, threats, and behaviours.

31. Effective management of security incidents is fundamental to enabling a safe and secure operating environment and relies on a positive security culture with a strong understanding of protective security policies and practices.

32. Defence Personnel and persons engaged under a contract should follow the following process to manage security incidents effectively and comprehensively:



Identify and Inform

33. Defence Personnel and persons engaged under a contract who identify that a security incident has or may have occurred **must** inform their chain of command (Commander/Manager) and/or Security Officer as soon as possible (refer Paragraph 4 for the definition of a Security Incident).

34. Where a security incident involves actual or suspected criminal activity including theft or serious damage, the AFP, local police or Joint Military Police Unit (JMPU) should be contacted immediately, while also notifying the Commander/Manager and/or Security Officer.

35. For emergencies or potentially life-threatening situations contact the AFP, local police, or JMPU) immediately.

Assess and Decide

36. Once aware that a security incident has or may have occurred within their area of responsibility, Commanders/Managers with support from Security Officers should take all reasonable actions within their remit to:

- a. ascertain the nature of the incident;
- b. assess the actual or potential impact of the incident on Defence assets or business operations, and
- c. decide what action is required to recover from and prevent future recurrence of the security incident.

37. In assessing the security incident and determining an appropriate response, Commanders/Managers should consider the actual or potential Security Incident Impact Level (SIIL) to Defence of the incident occurring. Guidance for the assessment of the Security Incident Impact Level is at **Annex B**.

Report

38. Security incidents **must** be reported centrally to SICC using the standard Security Report.
39. Reporting security incidents should occur once the immediate risk of harm is minimised, but as noted earlier, **must** occur within 24 hours of the incident occurring or being identified.
40. Commanders/Managers should ensure security incidents are escalated in accordance with Unit/Group/Company requirements as soon as possible.
41. If subsequent, relevant information comes to light in the process of responding to and recovering from a security incident, Commanders/Managers are to advise SICC by sending an email to Security.IncidentCentre@defence.gov.au containing the original security incident report reference number.
42. Security incidents involving classified information are to be reported to SICC as detailed in [Reporting incidents involving classified information](#).

Respond and Recover

43. Commanders/Managers should respond to and recover from security incidents in an effective and timely manner to minimise the potential impact of an incident and to help prevent a recurrence of the security incident.
44. In the course of responding to a security incident, a Commander/Manager may need to conduct a Fact Find to gain more information to identify vulnerabilities and determine the appropriate treatment action to contain the situation.
45. Commanders/Managers should not conduct a Fact Find into security incidents with an assessed SIIL of HIGH or EXTREME until directed by SICC, the SIU or a DIA.
46. Commanders/Managers should be aware that a Fact Find is not an investigation and care should be taken to conduct Fact Finds without compromising potential future investigations. For guidance, refer to ['Good Decision Making in Defence'](#) guide.

47. Commanders/Managers are responsible for the management of security incidents reported to them until:

- a. All reasonable responses to limit the impact of a security incident have been implemented,
- b. All reasonable actions to prevent future recurrence have been completed, or
- c. Responsibility for investigating the incident has been referred to an appropriate internal or external investigative authority.

48. Commanders/Managers **must** afford all reasonable assistance to personnel from an internal or external investigative authority to prevent any unreasonable impediment or interference with the investigation or inquiry process. Commanders/Managers **must not** direct or obstruct an External Agency or DIA in the execution of their duties.

Learn

49. Defence Personnel should learn from security incidents to continuously improve security risk management practices, reduce the likelihood of recurrences, and minimise the consequences of future incidents.

50. Commanders/Managers should take all reasonable actions within their remit to ensure that the conditions which enabled a security incident to occur are appropriately controlled to mitigate the risk of recurrence.

51. The SICC analyses trends in security incident management data to inform strategic decision making and support continuous improvement of security measures.

Record Keeping

52. Commanders/Managers, with support from Security Officers, **must** maintain records within the Unit/Group/Company regarding all security incidents that occur within their remit. These records include a copy of the lodged Security Report and any subsequent documents generated through the Security Incident Management process, including outcomes of any Fact Finds.

53. The Security Officer is responsible for the custody and maintenance of security incident records.

54. SICC maintains a record of all Security Reports in a centralised case management database, the Defence Policing Security Management System (DPSMS).

55. In managing security incident record keeping, Security Officers are to apply the standards in the [Defence Records Management Policy Manual \(RECMAN\)](#).

Security Investigations

56. A security investigation is the process of seeking information relevant to an alleged, apparent, or potential breach of Defence security policy or failure of security controls. The primary purpose of a security investigation is to:

- a. gather sufficient evidence to conclude whether security risk controls have failed or are failing to mitigate security risks and provide recommendations on how controls can be modified to improve their effectiveness and/or
- b. gather admissible evidence for any subsequent action, whether under criminal, civil penalty, disciplinary, or administrative sanctions relating to the breach of security policy.

57. Security investigations are undertaken by the SIU. The SIU is a designated DIA which has been established to conduct investigations of actual or suspected breaches of security policy, and actual or potential failures of security controls.

58. Investigations undertaken by the SIU are conducted in accordance with the requirements of the PSPF and the Australian Government Investigations Standards (AGIS) where appropriate.

Security Investigation Outcomes

59. Security investigations aim to establish the root cause of security matters and provide recommendations to prevent a reoccurrence and the future risk of harm to Defence.

60. Should an investigation confirm an actual breach of security policy, the investigation will provide evidence to whichever party is to conduct the resultant sanctioning response.

61. Where an investigation identifies failure of a security control/s, the investigation will provide recommendations to remediate the issue to the relevant Control Owner/s.

Security Incident Management Roles

Commander/Managers

62. Commanders/Managers are responsible for the management and reporting of security incidents that occur within their Unit/Group/Company.

Contract Manager

63. Contract Managers are responsible for monitoring compliance of Contractors, Consultants, Outsourced Service Providers, and other persons engaged under a contract with the terms of their contractual arrangements, including contractual security obligations.

64. Contract Managers should consider reported security incidents when monitoring compliance with contractual security obligations.

Security Officer

65. Each Unit and Group **must** designate a Security Officer who has completed the Defence Security Officer training course. The Security Officer will be able to recognise security risks and support Defence Personnel, including Commanders/Managers, to manage and report security incidents. This will also include maintaining records of security incidents that occur within their Unit and Group and how they were managed.

66. DISP members should refer to DSPF Control 16.1 – Defence Industry Security Program for security role requirements.

Security Incident Coordination Centre

67. SICC within DS&VS maintains a centralised record of all received Security Reports and provides advice and support as required to Defence Personnel in the management of security incidents.

Security Investigations Unit

68. The SIU is a designated DIA which has been established to conduct investigations of actual or suspected breaches of security policy, and actual or potential failures of security controls.

Security Incident Information Management

69. The release of Official Information in response to a freedom of information request is to be completed in accordance with the *Freedom of Information Act 1982* (the FOI Act). For advice, contact the Freedom of Information Directorate.

70. SICC refers or reports security incidents to external Agencies in accordance with the requirements of the PSPF.

Annexes and Attachments

Annex A - Additional Reporting Requirements

Annex B – Security Incident Impact Level (SIIL) Assessment Guide



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Weapons Security

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

Annex A – *Storage Requirements for Weapons*

Annex B – *Storage and Management of Privately Owned Weapons and Ammunition*

Annex C – *Armouries*

Annex D – *Transporting Defence Weapons*

Annex E – *Security Requirements for Display and Demonstration of Weapons*

Document administration

Identification

DSPF Control	Weapons Security
Control Owner	First Assistant Secretary, Security and Vetting Service
DSPF Number	Control 78.1
Version	3
Publication date	31 July 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Principle 78
Related DSPF Control(s)	Physical Transfer of Information and Assets Physical Security Security Incidents and Investigations Escorting Security Protected of Classified Assets SAFEBASE

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	7 August 2019	AS SPS	PSPF Aligned
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex A – Storage Requirements for Weapons

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

Appendix 1- Ceasing Periodic Checks During an Extended Reduced Activity Period

Document administration

Identification

DSPF Annex	Storage Requirements for Weapons
Annex Version	4
Annex Publication date	15 March 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	August 2019	AS SPS	PSPF Aligned

Version	Date	Author	Description of changes
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	15 March 2023	FAS DS	Update to para 8 and 9 to revise storage requirements for innocuous, replica and edged Defence weapons



Defence Security Principles Framework (DSPF)

Appendix 1 to Annex A – Ceasing Periodic Checks During an Extended Reduced Activity Period

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Appendix has no Attachments.

Document administration

Identification

DSPF Appendix	Ceasing Periodic Checks During an Extended Reduced Activity Period
Appendix Version	3
Appendix Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	7 August 2019	AS SPS	PSPF Aligned
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B – Storage and Management of Privately Owned Weapons and Ammunition

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Storage and Management of Privately Owned Weapons and Ammunition
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	7 August 2019	AS SPS	PSPF Aligned
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex C – Armouries

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Armouries
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	7 August 2019	AS SPS	PSPF Aligned
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex D – Transporting Defence Weapons

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Armouries
Annex Version	4
Annex Publication date	16 March 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	August 2019	AS SPS	PSPF Alignment
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF

Version	Date	Author	Description of changes
4	16 March 2023	FAS DS	Update to Table 1 Step 2 to include guidance to secure guidance to secure containers with lock mechanisms that do not fit the larger, SCEC-endorsed padlocks.



Defence Security Principles Framework (DSPF)

Annex E – Security Requirements for Display and Demonstration of Weapons

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

Appendix 1 – Mounting Procedures for Small and Trophy Weapons

Document administration

Identification

DSPF Annex	Security Requirements for Display and Demonstration of Weapons
Annex Version	3
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	7 August 2019	FAS S&VS	PSPF Alignment
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Defence Security Principles Framework (DSPF)

Appendix 1 to Annex E – Mounting Procedures for Small and Trophy Weapons

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Appendix has no Attachments.

Document administration

Identification

DSPF Appendix	Mounting Procedures for Small and Trophy Weapons
Appendix Version	2
Appendix Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF



Defence Security Principles Framework (DSPF)

Guided Weapons and Explosive Ordnance Security

General principle

1. All Guided Weapons and Explosive Ordnance (GWEO) (physical assets and associated information) must be secured against compromise to its confidentiality, integrity and availability. GWEO security arrangements will be informed by Security Risk Assessments and achieved in compliance with Commonwealth Explosives legislation and regulations, Defence GWEO policy and Defence security policy.

Rationale

2. Defence GWEO both enables critical Defence capability and is illegal for possession by the general population. Consequently, GWEO is threatened by the full spectrum of key threats to Defence as identified in the Defence Security Strategy.
3. Threat actors may impact GWEO capability through compromises to the confidentiality, integrity or availability of physical assets or associated information:
 - a. Confidentiality – including unauthorised access to/disclosure of classified information or classified assets.
 - b. Integrity – including malicious alteration of critical GWEO information (eg stock listing, stock location, stock quantities, targeting data, embedded software in maintenance equipment) or malicious modification to physical GWEO.
 - c. Availability – through denial of information systems, or denial of access to physical assets (eg through theft, destruction, isolation).
4. GWEO, by its nature, will readily fall into multiple 'Asset Categories' when assessing and determining the business impact levels (BIL) associated with it compromise, loss or damage. Bulk explosive ordnance and ammunition is specifically

recognised as a dangerous asset within the PSPF¹ but, depending on the specific GWEO in question, will also be considered valuable, attractive, classified, important and/or significant.

5. The compromise of Defence GWEO represents a direct impact upon Defence capability and presents significant and intolerable security and safety risk to Australia. Principle 79 and associated controls provide GWEO specific supplementation (to the broader DSPF Principles and Controls) and guidance to assist GWEO Managers and custodians to appropriately secure their GWEO inventory and associated information. The four controls under this Principle have been aligned to the four sections of the DSPF and, unless explicitly stated, do not negate the requirements of the broader DSPF. Where conflict between this control and broader DSPF controls is identified, advice should be sought from the relevant Control Owners.

Expected outcomes

6. GWEO and associated information is appropriately secured throughout the capability life cycle to prevent its compromise.
7. Only appropriately cleared, authorised and trained personnel have access to GWEO and associated information.
8. Defence has controls and procedures in place to deter and detect GWEO security threats.
9. Defence responds rapidly to detected threats to, and compromises of, GWEO and associated information.

¹ PSPF Policy 15 Physical Security for Entity Resources - Table 2
Principle 79

Escalation Thresholds

Risk Rating	Responsibility
Low	O4 or APS6 or equivalent in relevant Group/Service
Moderate	O5 or EL1 or equivalent in relevant Group/Service
Significant	Director General (DG) or O6 or EL2 or equivalent in relevant Group/Service
High	Defence Security Committee (DSC) via Commander Joint Logistics (CJLOG)
Extreme	DSC via CJLOG

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.

Document administration

Identification

DSPF Principle	Guided Weapons and Explosive Ordnance Security
Principle Owner	First Assistant Secretary Defence Security
DSPF Number	Principle 79
Version	3
Publication date	27 June 2023
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 79.1 – GWEO Security Governance & Planning Control 79.2 – GWEO Information Security Control 79.3 – GWEO Personnel Security Control 79.4 – GWEO Physical Security
Control Owner	Commander Joint Logistics

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security planning; Security governance for international sharing; Entity physical resources; and Entity facilities. <u>Legislation:</u> Explosives Transport Regulations 2002 (Cth) Australian Code for the Transport of Explosives by Road and Rail (AEC 3)
Read in conjunction with	N/A
See also DSPF Principle(s)	• Classification and Protection of Official Information • Security for Projects • Security for Capability Planning • Personnel Security Clearance • Defence Industry Security Program • Information Systems Lifecycle Management • Personnel Security Clearance • Temporary Access to Classified Information and Assets • Working Offsite • Physical Transfer of Information and Assets • Physical Security • Physical Security Certification and Accreditation • Access Control • Contracted Security Guards • Identification, Search and Seizure Regime • Security Incidents and Investigations • Escorting Security Protected or Classified Assets • SAFEBASE

Implementation Notes, Resources and Tools	• Defence Logistics Manual (DEFLOGMAN) ○ DEFLOGMAN Part 2 Volume 5 Chapter 17 Stocktaking of Defence Assets and Inventory ○ DEFLOGMAN Part 2 Volume 9 Chapter 1 Management of Explosive Ordnance ○ DEFLOGMAN Part 2 Volume 9 Chapter 6 Management of Inert Explosive Ordnance ○ DEFLOGMAN Part 2 Volume 9 Chapter 7 Defence Explosive Ordnance Assurance Framework • Electronic Supply Chain Manual (ESCM) ○ eSCM Volume 4 Section 8 Chapter 1 Management, Accounting and Assurance of Explosive Ordnance at Unit Level ○ eSCM Volume 4 Section 10 Chapter 6 COMSARM Stocktaking Processes and Procedures ○ eSCM Volume 13 Computer Systems Armament • eDEOP 100 Volume 2 Part 3 Chapter 3 - Defence Explosive Ordnance Assurance Framework • eDEOP 101 - Department of Defence Explosives Regulations • Security Equipment Guides and Security Equipment Evaluated Products via the Security Toolkit • Joint Framework for Base Accountabilities

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	27 June 2023	FAS DS	Complete Revision



Defence Security Principles Framework (DSPF)

Guided Weapons and Explosive Ordnance Security Governance and Planning

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document administration

Identification

DSPF Control	Guided Weapons and Explosive Ordnance Security Governance and Planning
Control Owner	Commander Joint Logistics (CJLOG)
DSPF number	Control 79.1
Version	3
Publication date	27 June 2023
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Guided Weapons and Explosive Ordnance Security
Related DSPF Control(s)	DSPF Governance and Executive Guidance

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	27 June 2023	CJLOG	Complete revision. Control 79.1 split into four separate Controls with content aligned with the four pillars of the DSPF – Governance, Information Security, Personnel Security, and Physical Security.



Defence Security Principles Framework (DSPF)

Guided Weapons and Explosive Ordnance Information Security

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document administration

Identification

DSPF Control	Guided Weapons and Explosive Ordnance Information Security
Control Owner	Commander Joint Logistics (CJLOG)
DSPF number	Control 79.2
Version	3
Publication date	27 June 2023
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Guided Weapons and Explosive Ordnance Security
Related DSPF Control(s)	10.1 – Classification and Protection of Official Information 11.1 – Security for Projects 16.1 – Defence Industry Security Program 25.1 – Information Systems Business Impact Levels and Aggregation

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	27 June 2023	CJLOG	GWEO Information Security amplification and guidance gathered herein as a consequence of the complete revision of Control 79.1 and splitting of it into four separate controls under Principle 79.



Defence Security Principles Framework (DSPF)

Guided Weapons and Explosive Ordnance Personnel Security

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document administration

Identification

DSPF Control	Guided Weapons and Explosive Ordnance Personnel Security
Control Owner	Commander Joint Logistics (CJLOG)
DSPF number	Control 79.3
Version	3
Publication date	27 June 2023
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Guided Weapons and Explosive Ordnance Security
Related DSPF Control(s)	40.1 – Personnel Security Clearance 41.1 – Temporary Access to Classified Information and Assets

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	27 June 2023	CJLOG	GWEO Personnel Security amplification and guidance gathered herein as a consequence of the complete revision of Control 79.1 and splitting of it into four separate controls under Principle 79.



Defence Security Principles Framework (DSPF)

Guided Weapons and Explosive Ordnance Physical Security

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

Annex A – Security Requirements for the Display and Demonstration of Inert Guided Weapons and Explosive Ordnance

Annex A – Appendix 1 – Security Requirements for the Display and Demonstration of Inert Guided Weapons and Explosive Ordnance

Annex B – Storage and Management of Privately Owned Explosive Ordnance

Document administration

Identification

DSPF Control	Guided Weapons and Explosive Ordnance Security
Control Owner	Commander Joint Logistics (CJLOG)
DSPF number	Control 79.4
Version	3
Publication date	27 June 2023
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Guided Weapons and Explosive Ordnance Security
Related DSPF Control(s)	

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	27 June 2023	CJLOG	Extensive Rewrite to align content with the broader DSPF



Defence Security Principles Framework (DSPF)

Annex A to Guided Weapons and Explosive Ordnance Physical Security – Security Requirements for the Display and Demonstration of Inert Guided Weapons and Explosive Ordnance

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

Appendix 1 – Security Requirements for Display and Demonstration of Inert Guided Weapons and Explosive Ordnance

Document administration

Identification

DSPF Annex	Control of Inert Explosive Ordnance
Annex Version	4
Annex Publication date	27 June 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control 79.4)
DSPF Control	Guided Weapon and Explosive Ordnance Physical Security
DSPF Number	Control 79.4

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	10 August 2020	AS SPS	Removal of BIL reference table
4	27 June 2023	CJLOG	Renumbering to align with revised Principle and Controls



Defence Security Principles Framework (DSPF)

Appendix 1 to Annex A of Guided Weapons and Explosive Ordnance Physical Security – Security Requirements for Display and Demonstration of Inert Guided Weapons and Explosive Ordnance

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Appendix has no Attachments.

Document administration

Identification

DSPF Annex	Security Requirements for Display and Demonstration of Inert Guided Weapons and Explosive Ordnance
Appendix Version	3
Appendix Publication date	27 June 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control 79.4)
DSPF Control	Guided Weapon and Explosive Ordnance Physical Security
DSPF Number	Control 79.4

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	27 June 2023	CJLOG	Renumbering to align with revised Principle and Controls



Defence Security Principles Framework (DSPF)

Annex B to Guided Weapon and Explosive Ordnance Physical Security – Storage and Management of Privately Owned Explosive Ordnance

Redacted version: Classified content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Annexes and Attachments

This DSPF Annex has no Attachments.

Document administration

Identification

DSPF Annex	Storage and Management of Privately Owned Explosive Ordnance
Annex Version	3
Annex Publication date	27 June 2023
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control 79.4)
DSPF Control	Guided Weapon and Explosive Ordnance Physical Security
DSPF Number	Control 79.4

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	CJLOG	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	27 June 2023	CJLOG	Renumbered as part of rewrite of Principle 79 and Control 79.1



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Radioactive Sources

General principle

1. Security Enhanced Sources must be secured from theft, loss or unauthorised access in full compliance with the Commonwealth Code of Practice for the Security of Radioactive Sources (RPS 11).

Rationale

2. Defence deals with its radioactive sources in accordance with the conditions attached to the Defence Source Licence, which is issued by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA). The normal security protocols within Defence, which are in place for safety purposes, are considered to be adequate to ensure the physical security of the majority of radioactive sources.

3. A sealed radioactive source consists of radioactive material that is either permanently contained in a capsule or is closely bound in solid form. They are categorised on the basis of their risk, from Category 1 (high) to Category 5 (low). The loss or compromise of any sealed radioactive source will have safety and security ramifications that could negatively impact on Defence's personnel and its reputation.

4. A Security Enhanced Source is defined as a source from Category 1, 2 or 3. Such sources are dangerous to human life in exposure events of a few minutes (Category 1) to a few hours (Category 2) to a few days (Category 3). As such, these sources pose a significant risk to national security if acquired by persons of malicious intent.

Expected outcomes

5. Security Enhanced Sources will be protected against theft, loss or unauthorised access to the full extent of our obligations and in accordance with National and International requirements.

6. Security Enhanced Sources held by Defence will be managed in accordance with the Defence Radiation Safety Manual, Chapter 3, Annex C.

7. Security Enhanced Sources for which Defence is responsible will be secured in full compliance with the [Code of Practice for the Security of Radioactive Sources ARPANSA Radiation Protection Series No.11](#).

8. Where there is a conflict between safety and security requirements, the issue is to be referred to Director, Defence Radiation Safety and Environment, Joint Logistics Command for determination of the requirement.

Escalation Thresholds

Risk Rating	Responsibility
Low	O4 or APS6 or equivalent in relevant Group/Service
Moderate	O5 or EL1 or equivalent in relevant Group/Service
Significant	Director General (DG) or O6 or EL2 or equivalent in relevant Group/Service
High	Defence Security Committee (DSC) via Commander Joint Logistics (CJLOG)
Extreme	DSC via CJLOG

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Radioactive Sources
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 80
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	None
Control Owner	Commander Joint Logistics (CJLOG)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security planning; Security governance for international sharing; Entity physical resources; and Entity facilities. Legislation: <u>Australian Radiation Protection and Nuclear Safety Act 1998</u> (the ARPANS Act) <u>Australian Radiation Protection and Nuclear Safety Regulations 1999</u> (the ARPANS Regulations) <u>Code of Practice for the Security of Radioactive Sources – ARPANSA Radiation Protection Series No.11</u> (RPS 11)
Read in conjunction with	Defence Radiation Safety Manual (the DRSM)
See also DSPF Principle(s)	Personnel Security Clearance Physical Security Certification and Accreditation Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	<u>Australian Radiation Protection and Nuclear Safety Act 1998 (the ARPANS Act)</u> <u>Australian Radiation Protection and Nuclear Safety Regulations 1999 (the ARPANS Regulations)</u> <u>Code of Practice for the Security of Radioactive Sources – ARPANSA Radiation Protection Series No.11 (RPS 11)</u> Defence Radiation Safety Manual (the DRSM)

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	21 May 2019	FAS S&VS	Additional clarification added to Rationale
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Escorting Security Protected or Classified Assets

General principle

1. Where security considerations demand, specific security-protected assets are to be escorted by appropriately qualified and authorised escorts.

Rationale

2. Loss or theft of security-protected or classified assets impacts Defence capability and reputation.
3. Security-protected or classified assets (such as Weapons and Explosive Ordnance) are highly sought after by criminal and extremist organisations and are vulnerable to theft during transport.

Expected outcomes

4. Security Risk Assessments are used to determine the escort requirements for the transportation of security-protected or classified assets in accordance with the Principle's subordinate Control policy.
5. Escorts are appropriately qualified to secure consignments against theft, loss or misuse during transport;
6. Escorts are aware of their roles and responsibilities; and
7. Any security incidents associated with the transport of security-protected or classified assets are reported appropriately.

Escalation Thresholds

8. The Assistant Secretary, Security Policy and Services (AS SPS) has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Weapons and Explosive Ordnance Escorting Risks

Risk Rating	Responsibility
Low	EL2/O-6 or equivalent in relevant Group/Service
Moderate	SES1/O-7 or equivalent in relevant Group/Service
Significant	Defence Security Committee (DSC) – through AS SPS
High	DSC – through AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

All Other Security Protected and Classified Assets Escorting Risks

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	DSC – through AS SPS
Extreme	DSC – through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: Chief of Joint Operations or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.

Document administration

Identification

DSPF Principle	Escorting Security Protected or Classified Assets
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 81
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 81.1
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security governance for contracted service providers; Security governance for international sharing; Eligibility and suitability of personnel; Entity physical security; and Entity facilities. Legislation: For all relevant state and territory private security guard legislation, see DSPF Principle 75 – <i>Contracted Security Guards</i>. <u>Explosive Transport Regulations 2002 (Cth)</u> <i>Australian Code for the Transport of Explosives by Road and Rail (AEC 3)</i>
Read in conjunction with	N/A
See also DSPF Principle(s)	Physical Transfer of Information and Assets Physical Security Contracted Security Guards Security Incidents and Investigations Weapons Security Explosive Ordnance Security Security of Radioactive Sources
Implementation Notes, Resources and Tools	DI(G) LOG 4-1-006: Safety of Explosive Ordnance DI(G) LOG 4-5-012: Regulation of technical integrity of Australian Defence Force materiel <i>Australian Code for the Transport of Explosives by Road and Rail (AEC)</i> eDEOP 100 -Defence Explosive Ordnance Publication eDEOP 101 -Department of Defence Explosives Regulations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Escorting Security Protected or Classified Assets

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this enterprise-wide control

Escalation Thresholds

2. The AS SPS has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Weapons and Explosive Ordnance Risks

Risk Rating	Responsibility
Low	EL2/O-6 or equivalent in relevant Group/Service
Moderate	SES1/O-7 or equivalent in relevant Group/Service
Significant	Defence Security Committee (DSC) – through AS SPS
High	DSC – through AS SPS
Extreme	DSC – through AS SPS

All Other Security Protected and Classified Assets Escorting Risks

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	DSC – through AS SPS
Extreme	DSC – through AS SPS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Note: Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.

Control

3. This DSPF part provides the base requirements for escorting. Additional controls may apply for the transport of weapons, Explosive Ordnance (EO) and assets with high Business Impact Levels (BILs). For further information, refer to:
 - a. DSPF Principle 78 – *Weapons Security*;
 - b. DSPF Principle 79 – *Explosive Ordnance Security*; and
 - c. DSPF Principle 71 – *Physical Transfer of Information and Assets*.
4. A Movement Security Plan (MSP) should be developed before undertaking escorting activities. A Security Risk Assessment (SRA) should be conducted as part of this process. For further information on Transportation and MSP requirements, see Annex D and Annex E to DSPF Control 71.1 – *Physical Transfer of Information and Assets*.
5. With the exception of mandatory provisions (bold must statements), an SRA can also be used to determine whether a departure from the requirements found throughout this DSPF part is permissible. This risk assessment must take the following into consideration:
 - a. The distance required to transport the security protected asset;
 - b. The quantity of security protected assets (including EO) being transported; and

- c. Relevant threat assessments. Threat assessments can be found on the Defence Secret Network

Note: in some circumstances, activity specific threat assessments can be requested. See DS&VS Security Threat Assessments.

- 6. For further guidance on SRAs, see DS&VS Security Risk Management.

When to Escort

- 7. There **must** be an escort for the vehicle transport of any quantity of:
 - a. Small arms (other than personal issue);
 - b. EO; or
 - c. security-protected assets assigned a BIL of 4 (Extreme) or above (or classified SECRET and above).
- 8. A risk assessment can be conducted to determine if escorts are required for the transport of security-protected assets assigned a BIL of 3 (High) and below (classification of PROTECTED and below).
- 9. Escorts are not required:
 - a. For direct hand carriage of classified information (e.g. between two office buildings), in accordance with DSPF Principle 71 – *Physical Transfer of Information and Assets*;
 - b. Innocuous, replica and edged weapons;
 - c. Large Defence Weapons;
 - d. Weapon systems that are permanent fixtures of a platform.
 - e. EO recovery activities by EO disposal personnel; and
 - f. During the sea or air legs of commercial international or domestic transfer

Note: The above requirement does apply, however, for any road or rail transport of security-protected assets before and after any sea/air movement.

Who Can Escort

- 10. An escort should have:
 - a. an understanding of the escorting responsibilities as specified in this DSPF part and their specific escorting instructions;
 - b. any qualifications and training required to carry out their escorting duties (e.g. weapons training for armed escorts); and

- c. as a minimum, the same driver qualifications as the driver of the cargo or escort vehicle in order to drive the vehicle in an emergency.

11. When considering fatigue management, escorts and drivers may switch roles if the driver has the requisite qualifications and training to act as an escort; however, for long hauls, it is recommended that additional drivers are available.

Note: escorts should be made aware of their responsibilities and the extent of their powers to prevent unauthorised access to the consignment.

Case Study: Estate and Infrastructure Group often manage offsite classified waste disposal for Defence sites. APS members are regularly employed to act as escorts during these activities. In accordance with their MSP, the escorts are required to follow the waste vehicles and witness the disposals. They are instructed to alert the local police of unauthorised attempts to access the waste and report incidents in accordance with DSPF Principle 77 – Security Incidents and Investigations.

Officer in Charge

12. Where there is more than one escort, the most senior escort is designated Officer in Charge (OIC) of the escort party and should travel in the escort vehicle. For Defence personnel, the OIC should be at least a Junior Non-Commissioned Officer (NCO) (Leading Seaman, Corporal, or Lance Corporal) or an Australian Public Service (APS) equivalent. For large or sensitive consignments it is recommended that the OIC be at least a Senior NCO or APS equivalent. If Australian Federal Police (AFP), AFP Protective Services (AFP-PS) or state and territory police are providing escorts, they will allocate an OIC at a level they deem appropriate.

Armed Escorts

13. The risk associated with a consignment may lead to a determination that armed escorts are required in non-operational settings. If armed escorts are required, AFP, AFP-PS or state and territory police services should be used in preference to private contract guards. Australian Defence Force (ADF) members providing escorts should not be armed. For further information on the use of private contract guards refer to DSPF Control 75.1 – *Contracted Security Guards*.

Police Escorts

14. It is recommended that civilian police escorts be used in addition to regular Defence escorts for transporting EO assigned a confidentiality BIL of 4 (Extreme) or classified SECRET or above.

Case Study: An Army officer is transporting security-protected equipment between two bases. After assessing the risk, she arranges for ADF members from her own unit to provide escorts with the most senior of them taking on the OIC role. However, if she determined through her assessment that the risk was too high, she might choose to arrange a police escort. In both cases, she ensures the escorts are aware of the risks and responsibilities outlined in the MSP.

How to Escort

Written Escort Instructions

15. The issuing entity is to issue written security instructions to the escort. The written instructions are not to reveal the nature or classification of the security-protected asset.

16. Written escort instructions may be included in the MSP.

Escort Requirements

17. The number of escorts required increases depending on the number of cargo vehicles being used to transport a consignment. The number of escorts required is based on a 1:3 ratio, i.e. one escort per three cargo vehicles (or part thereof). Therefore, if there are more than three cargo vehicles there should be an escort for every subsequent multiple of three cargo vehicles (or part thereof). The escort for the rearmost group of vehicles should travel at the rear of the convoy in the escort vehicle.

18. Security-protected assets requiring an escort should only be transported in an Australian Government or Defence contractor vehicle. There are limited situations (e.g. when a Defence employee is traveling interstate, overseas, or out-of-area and an Australian Government vehicle is unavailable) in which specific security protected assets can be transported in private vehicles (e.g. personally-owned vehicles, taxis, and hire cars).

Note: External service providers involved in the transportation of EO may be able to operate under the requirements detailed in Annex A to this Control – Escorting Requirements for Explosive Ordnance External Service Providers (refer paragraph 24).

Escort Vehicle Requirements

19. Escort vehicles **must** be crewed by a driver and an escort.

20. In multi-vehicle convoys, radio communications must be provided to all vehicles and escorts.

21. If security-protected assets requiring an escort are to be transported on public roads (including bases with open access), there should be at least one escort vehicle when:

- a. more than one cargo vehicle is used;
- b. the following quantities are transported in a single cargo vehicle:
 - (1) one or more items of large assets assigned a BIL of 4 (Extreme) or above (or classified SECRET and above);

Note: Refer to DSPF Control 71.1 – *Physical Transfer of Official Information, Security Protected and Classified Assets* for identification of what types of assets should be transported rather than transferred, (i.e. not sent via SCEC-approved courier).

- (2) seven or more pistols or non-automatic shoulder-fired weapons;
- (3) two or more automatic shoulder-fired weapons;
- (4) 10 or more sub-calibre training aids capable of firing a projectile by means of a powder charge;
- (5) Defence weapon controlled repair parts corresponding to and of the same amount as the weapons listed above;

Note: Some exceptions to escort vehicle requirements apply to personal-issue weapons (refer paragraph 23).

- (6) bulk EO (as defined in DSPF Control 79.1 – *Explosive Ordnance Security*); or

Note: There may be a case where the amount of EO is less than 'bulk' but requires more than one vehicle for safety purposes. An example is mixed EO of different compatibility groups. Safety requirements are available in Defence Explosive Ordnance Publication 103.

- (7) single unsecured canopied cargo vehicle is used for transportation of any amount.

Note: A canopied vehicle is considered vulnerable and not secure if the canopy is made from canvas or similar such 'soft' materials. Cargo vehicles with canopies that are rigid and lockable do not apply in this regard.

22. The number of escort vehicles required increases dependent on the number of cargo vehicles used to transport a consignment. The number is based on a 1:10 ratio, one escort vehicle per 10 cargo vehicles (or part thereof). Therefore, if there are more than 10 cargo vehicles there should be an escort vehicle for every subsequent multiple of 10 cargo vehicles (or part thereof). The escort vehicle for the rearmost group of cargo vehicles should travel behind the rear cargo vehicle. It is recommended that unsecured canopied cargo vehicles within a convoy are followed directly by an escort vehicle.

Case Study: A facility holding Defence servers is closing down and a manager from Chief Information Officer Group (CIOG) is responsible for moving servers to a new site. The servers have a BIL of 4 (Extreme) and will easily fit into two cargo vehicles. Since the journey is short and in a well policed area, he determines that contracted guards would be suitable for this activity. There are fewer than 10 cargo vehicles, so only one escort vehicle is required.

Personal-issued Weapons

23. Where an individual or a small group of no more than six people is travelling with no more than two personal issued, non-bladed weapons each (e.g. a rifle and a pistol) there is no requirement for an escort vehicle; however there **must** be an escort designated who is not the driver of the vehicle.

EO External Service Provider Transport Operations

24. Where an external service provider has the following measures in place, it may follow the requirements detailed in Annex A to this Control – Escorting Requirements for Explosive Ordnance External Service Providers for the escorting of EO in lieu of the requirements above:

- a. It **must** be Defence Industry Security Program (DISP) accredited and maintain compliance with the Australian Code for the Transport of Explosives by Road and Rail (AEC) and the [Explosives Transport Regulations 2002 \(ETR\)](#);
- b. It **must** have cargo vehicles installed with satellite tracking and duress alarm systems for Category 2 or higher risk loads;
- c. It **must** have inter-vehicle communications within a vehicle convoy in accordance with the AEC 3;
- d. It **must** have communications to the base EO depot for Category 1 loads and higher risk loads;
- e. It **must** have secure cargo areas in accordance with the AEC; and
- f. It **must** have appropriate security clearances in place for its staff (refer DSPF Control 79.1 – *Explosive Ordnance Security*).

Note: AEC Chapter 2 provides information of the different categories of EO.

Roles and Responsibilities

Commanders and Managers

25. Commanders and Managers are responsible for ensuring that people nominated to escort security-protected assets have the necessary security clearances and training, and are fully briefed on their responsibilities and their response in the event that the shipment comes under attack, items are lost or stolen, or unauthorised access occurs.

Contract Managers

26. In instances where a MSP identifies the need for a licensed security guard to act as an escort, Defence contract managers are responsible for ensuring that contracts with external service providers require that the security guards are licensed in accordance with the relevant state and territory private security guard legislation and DPSF Principle 75 – *Contracted Security Guards*.

The Issuing Entity

27. The issuing entity is responsible for the security of the consignment in accordance with this DSPF part until the gaining entity takes possession.

28. The issuing entity is responsible for:

- a. providing appropriately qualified numbers of escorts for the assignment;
- b. ensuring that people nominated as escorts have the necessary security clearances and training;
- c. providing adequate communications between all parties associated with the transportation (e.g. drivers, escorts and gaining entities) to enable communication in circumstances involving time delays, accidents or other incidents while in transit;
- d. briefing the escort party on the MSP and other orders;
- e. making all escorts aware of their legal powers of arrest unless those escorts are AFP, state or territory police officers or AFP-PS officers; and
- f. obtaining a signed statement from each member of the escort party indicating that they fully understand their responsibilities.

Escorts

29. Escorts, who are escorting security-protected assets, are responsible for:

- a. executing the MSP;
- b. reasonably preventing unauthorised access to the consignment;
- c. where physically possible, remaining with and observing the consignment at all times;
- d. guarding the consignment during halts in the journey;
- e. making parking arrangements with the nearest Defence authority or civilian police during night halts, extended halts or breakdown;
- f. exercising appropriate powers in the protection of life and property, including powers of arrest if necessary;

- g. maintaining a chronological log of events including:
 - (1) time of arrival and departure;
 - (2) stop-over points;
 - (3) transshipment points;
 - (4) security arrangements at each stop;
 - (5) any security incidents that occurred; and
- h. providing the log of events to the issuing entity after delivery of the escorted items.

Key Definitions

30. **Hand Carriage.** The personal carriage of classified information or security-protected assets by Defence personnel or external service providers who have the required security clearance to hold the information or asset.

31. **Escorts.** Civilian police officers, ADF members, APS employees or external service providers who guard or secure a load or consignment from theft, vandalism, sabotage or espionage. An escort may be armed or unarmed and does not drive escort or cargo vehicles, except in an emergency.

32. **Escort Vehicles.** Vehicles used in addition to cargo vehicle(s) in order to provide increased vigilance and protection.

33. **Cargo Vehicles.** Vehicles that are actively carrying a load of security-protected assets, including weapons and explosive ordnance.

34. **Weapon.** An offensive or defensive instrument of combat.

***Note:** The above is a general ordinary language definition. This DSPF part is concerned with Defence Weapons and Cadet Firearms as defined below. Within this Control, use of the stand-alone term 'weapon' refers to both 'Defence weapon' and 'Cadet firearm'.*

35. **Defence Weapon.** A weapon owned by Defence to meet the operational, training and support requirements of the Permanent and Reserve members of the ADF. For the purposes of differentiating storage and transportation security requirements, Defence weapons are subcategorised into:

- a. **Small arms** Defence weapons. Defence weapons that are:
 - (1) only capable of firing a round smaller than 20 millimetres calibre, regardless of being either man-portable or platform-mounted; or
 - (2) which are of a calibre greater than 20 millimetres, but are man-portable, such as section-level grenade launchers and rocket launchers;

- b. **Large Defence Weapons.** Defence weapons which can fire a round of 20 millimetre calibre or greater and are not considered man-portable;
 - c. **Superseded Defence Weapons.** Defence weapons that are no longer managed as a part of the operational inventory but are retained by Defence for any purpose;
 - d. **Replica Defence Weapons.** Inert instruments made to replicate the size, weight and/or shape of a live firing Defence weapon, or its component parts. Replica weapons include red guns, white guns, instructional weapons and instructional replicas;
 - e. **Controlled parts.** Defence weapon components and sub-assemblies that require the same security measures as a complete Defence weapon. They are those parts of weapons that are the most difficult to manufacture and substitute, and without which the weapon is inoperable;
 - f. **Edged Defence Weapons.** Edged implements used for making or repelling an attack; includes combat knives and bayonets, but does not include ceremonial swords and ceremonial lances.
 - g. **Innocuous Defence Weapons.** Defence weapons that have been rendered incapable of discharging a projectile to the satisfaction of engineering standards within Defence (for further information see Rendering Weapons Innocuous, above. Innocuous Defence weapons include Weapon Training Simulation System (WTSS) weapons, some sectionalised training aids and any Defence weapons in the subcategories above which have been rendered innocuous; and
 - h. **Captured Weapons.** Weapons captured or seized on operations that fall within one or more of the subcategories above are to be treated as Defence weapons for the purposes of storage, transportation and disposal.
36. **Security-protected Asset.** A non-financial, reportable or accountable information or asset that requires greater than standard fire and theft protection due to either:
- a. being allocated Protective Marking
 - b. an unacceptable business impact that would result from the unauthorised modification (i.e. loss of integrity) of the information or asset, irrespective of whether that modification can be detected or not;
 - c. an unacceptable business impact that would result from the information or asset being unavailable (i.e. loss of availability) for a given period of time; or
 - d. being categorised as a weapon or explosive ordnance.

37. **Movement Security Plan (MSP).** A set of security measures detailed for the transport of security-protected assets, including weapons and explosive ordnance. A single MSP can be used to cover periodic movement of security-protected assets between the same parties, at non-changing departure and destination points (refer DSPF Control 71.1 -Physical Transfer of Information and Assets).

38. **Issuing Entity.** The Commander or Manager of a military or business unit, or authorised external service provider, responsible for issuing security-protected assets to a gaining entity.

39. **Gaining Entity.** The Commander or Manager of a military or business unit, or authorised external service provider responsible for taking possession of security-protected assets from an issuing entity.

Further Definitions

40. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – Escorting Requirements for Explosive Ordnance External Service Providers

Document administration

Identification

DSPF Control	Escorting Security Protected or Classified Assets
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 81.1
Version	3
Publication date	29 September 2020
Type pf control	Enterprise-wide
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Principle 81
Control Owner	Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Contracted Security Guards Security Incidents and Investigations Weapons Security Explosive Ordnance Security Security of Radioactive Sources

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	29 September 2020	AS SPS	Escort requirements for LIREW and the definition of a Defence Weapon aligned with DSPF 78.1 – <i>Weapons Security</i>



Defence Security Principles Framework (DSPF)

Annex A – Escorting Requirements for Explosive Ordnance External Service Providers

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Escorting Requirements for Explosive Ordnance External Service Providers
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control 81.1).
DSPF Control	Escorting Security Protected or Classified Assets
DSPF Number	Control 81.1

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Procurement

General principle

1. Project Managers and Contract Managers are to ensure entities, to which Defence has granted access to Official Information or assets, take appropriate security measures to safeguard the information or assets. Security is to be considered and planned for throughout all stages of the procurement process.

Rationale

2. The procurement of goods and services has the potential to render Defence vulnerable to increased security threats and risks as contractors:
- a. become knowledgeable about Defence capabilities through involvement in Defence projects;
 - b. are granted access to Defence bases and facilities, Official Information and assets, and Information and Communications Technology (ICT) systems; and
 - c. provide security-related goods or services.

Expected outcomes

3. Security risks are not outsourced, and remain with the Defence Group or Service responsible for the procurement activity.
4. Project Managers and Contract Managers manage the security risks that result from allowing persons engaged under a contract access to Defence bases and facilities, Official Information and assets, and ICT systems.
5. Security risks associated with procurement activities are considered, assessed and managed in accordance with the DSPF.
6. The appropriate level of Defence Industry Security Program (DISP) membership is obtained and maintained, where required.
7. Defence Groups and Services ensure applicable security obligations contained in the DSPF are specified in contracts.

8. Appropriate strategies are established for the transition of security arrangements prior to the completion or termination of contracts.

Note: A reference to contracts includes standing offers and panel arrangements.

Escalation Thresholds

Risk Rating	Responsibility
Low	Assistant Secretary Materiel Procurement Branch (AS MPB)
Moderate	AS MPB
Significant	First Assistant Secretary Procurement and Contracting (FAS P&C)
High	Defence Security Committee (DSC) – through FAS P&C
Extreme	DSC – through FAS P&C

Note: The DSPF Security Requirements have been incorporated into Defence's procurement policy framework and need to be incorporated in all contracting and procurement templates. Incorporation of security requirements into contracting templates/suites is the responsibility of the areas responsible for the template/suite, in accordance with the policy.

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Procurement
Principle Owner	First Assistant Secretary Security & Vetting Service (FAS S&VS)
DSPF Number	Principle 82
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	None
Control Owner	Assistant Secretary Materiel Procurement Branch (AS MPB)

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Eligibility and suitability of personnel and Access to information
Read in conjunction with	Commonwealth Procurement Rules (CPRs) Defence Procurement Policy Manual
See also DSPF Principle(s)	Assessing and Protecting Official Information Security for Projects Security for Capability Planning Foreign Release of Official Information Defence Industry Security Program Information Systems (Physical) Security ICT Certification and Accreditation Personnel Security Clearance Physical Transfer of Information and Assets Physical Security Certification and Accreditation Contracted Security Guards Security Incidents and Investigations Weapons Security Explosive Ordnance Security
Implementation Notes, Resources and Tools	<i>Note:</i> From 1 July 2018, existing contracts may be subject to a 12-month Transition Period during which the Defence Security Manual (DSM) will continue to apply as the authoritative statement of Defence security policy. Refer to Annex A of this DSPF Principle and the Contracts Review Process Guide for further information. Australia National Audit Office, Better Practice Guide, Developing and managing contracts PSPF 6 – Security governance for contracted goods and service providers Commonwealth Procurement Rules (CPRs) Defence Procurement Policy Manual CASG Security Procurement and Contracting Tools and Templates Procurement and Contracting Help Desk Support

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Defence Security Principles Framework (DSPF)

Annex A to Procurement – Transition Period

Redacted version: Sensitive content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Protected Network (DPN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Transition Period
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Principle).
DSPF Principle	Procurement
DSPF Number	Principle 82

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

SAFEBASE Security Alert Level System

General Principle

1. The SAFEBASE Security Alert Level System communicates threats of violent acts on Defence bases, sites and establishments (herein referred to as bases) and is underpinned by effective security planning.

Rationale

2. Acts of violence from terrorism, politically or issue-motivated groups and maverick individuals pose a threat to Defence's people and assets. It is important that Defence informs people on Defence premises of expected threats to support their decisions about security and safety.

3. Understanding and communicating changes to assessed violent threats operates alongside and enhances other DSPF Principles and Controls. Changes to SAFEBASE Security Alert Levels (herein referred to as alert levels) may be employed as an agile risk mitigation method that contributes to protecting Defence's people and assets.

Expected Outcomes

4. Changes to SAFEBASE alert levels may apply locally (to a single base), regionally (to a number of bases in a defined geographic region) or nationally (Defence-wide).

5. Senior Australian Defence Force Officers (SADFOs), Base Managers and Heads of Resident Units effectively communicate alert levels to people on their bases.

6. SAFEBASE alert levels are time-bound and reviewed for appropriateness.

7. Defence's SAFEBASE alert levels support and enable security measures that:

- a. can be implemented within the timeframes expected under the relevant alert level;
- b. are cost-effective, appropriate to the local context, and can be effected within a base's existing resources;

- c. focus on protecting against the threat at hand underpinned by localised, effective security risk management and up-to-date base security plans; and
 - d. ensure the base's core business can continue as required.
8. Roles and responsibilities at each SAFEbase alert level have been communicated to Defence personnel and persons engaged under a contract on Defence premises and align with the *Joint Framework for Base Accountabilities*.

Escalation Thresholds

Note: Security risk in the DSPF is usually escalated through the risk escalation thresholds. However, this DSPF Principle has no escalation thresholds. Security risk is to be managed in accordance with the *Joint Framework for Base Accountabilities* and through the application of DSPF Principles and Controls.

SAFEbase – Alert Level Authorities

Level	Authority to raise or lower at a local base	Authority to raise or lower at the regional level	Authority to raise or lower at the national level
Aware	Chief Security Officer or SADFO	Chief Security Officer	Chief Security Officer
Alert	Chief Security Officer or SADFO	Chief Security Officer	Chief Security Officer
Act	Chief Security Officer or SADFO	Chief Security Officer	Chief Security Officer

Note: The Chief Security Officer (First Assistant Secretary Security and Vetting Service) is authorised to override a SADFO's changes to a base's alert level.

Document administration

Identification

DSPF Principle	SAFEbase Security Alert Level System
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 83
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 83.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	<u>PSPF Core Requirements:</u> Security planning and risk management; Security governance for contracted goods and service providers; and Entity physical resources. Legislation: <u>Defence Act 1903</u> (Cth) <u>Workplace Health and Safety Act 2011</u> (Cth)
Read in conjunction with	Joint Framework for Base Accountabilities OPLAN SNAVE
See also DSPF Principle(s)	Counterintelligence Physical Security Physical Security Certification and Accreditation Access Control Contracted Security Guards Identification, Search and Seizure Regime Weapons Security Explosive Ordnance Security
Implementation Notes, Resources and Tools	• Australian Government physical security management protocol: https://www.protectivesecurity.gov.au/ • DS&VS security risk literature and planning tools via the Security Toolkit • Security Equipment Guides (SEGs) via the Security Toolkit. • ASIO Tech Notes via the Security Toolkit. • <u>Security Equipment Evaluated Product List</u> (SEEPL). This list contains products endorsed by the Security Construction and Equipment Committee (SCEC). • Contact 1800DEFENCE, your Executive Security Authority (ESA), or your DS&VS regional office for further information.

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	25 March 2019	FAS S&VS	SAFEBASE redesigned system: simplified to three alert levels; additional customisation options; and clarification of authorities and notification responsibilities.
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

SAFEBASE Security Alert Level System

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) in the Defence Security & Vetting Service (DS&VS) is the owner of this enterprise-wide Control.

Escalation Thresholds

Note: Security risk in the DSPF is usually escalated through the risk escalation thresholds. However, this DSPF Control has no escalation thresholds. Security risk is to be managed in accordance with the Joint Framework for Base Accountabilities and through the application of DSPF Principles and Controls.

SAFEBASE – Alert Level Authorities

Level	Authority to raise or lower at a local base	Authority to raise or lower at the regional level	Authority to raise or lower at the national level
Aware	Chief Security Officer or SADFO	Chief Security Officer	Chief Security Officer
Alert	Chief Security Officer or SADFO	Chief Security Officer	Chief Security Officer
Act	Chief Security Officer or SADFO	Chief Security Officer	Chief Security Officer

Note: The Chief Security Officer (First Assistant Secretary Security and Vetting Service) is authorised to override a SADFO's changes to a base's alert level.

Process

Overview

2. Every Defence base, site and establishment (herein referred to as bases) in Australia is to use Defence's Security Alert Level system, SAFEBASE. The system consists of three levels:

- (1) *Aware* (yellow): Threat advice of a violent act against Defence bases is generalised. No specific time or location is notified.
- (2) *Alert* (orange): Threat advice indicates a specific timeframe for a violent act against specific bases.
- (3) *Act* (red): A violent act on the base is either happening or imminent.

3. Changes to SAFEBASE Security Alert Levels (herein referred to as alert levels) may apply locally (to a single base), regionally (to a number of bases in a defined geographic region) or nationally (Defence-wide).

4. Senior Australian Defence Force Officers (SADFOs), Base Managers (BMs) and Heads of Resident Units should ensure alert levels are communicated appropriately to people on their base to warn them of the threat, as well as, security plans and procedures.

Example: Bases may communicate these messages through the use of signage, email alerts, or established Base Warning Alert Systems.

Note: for the purposes of SAFEBASE, Site Managers will have SADFO responsibilities at bases where no SADFO is appointed.

5. Additional guidance on alert levels can be found on the DS&VS Security Portal Intranet Page.

Authority to Raise and Lower the Alert Levels

6. The Chief Security Officer, or an approved delegate, is authorised to set the SAFEBASE alert level at the national, regional or local level in response to threat and risk assessments.

Note: The First Assistant Secretary Security and Vetting Service (FAS S&VS) is the Chief Security Officer.

7. SADFOs are authorised to set the SAFEBASE alert level at the local level (their local base) in response to security threats and risk advice.

8. SADFOs **must** acknowledge and act on Chief Security Officer-authorized changes to relevant alert levels.

***Note:** There may be restrictions that prevent the complete dissemination of threat information (such as operational considerations, classifications or handling caveats). When authorising the change of alert level, the Chief Security Officer will aim to provide as much actionable information as possible and clear instructions on any dissemination limitations.*

Raising Levels

9. Decisions to change SAFEbase alert levels should be threat-based and informed by consultation with intelligence and law enforcement agencies, Headquarters Joint Operations Command (HQJOC), and local base authorities.

10. Decisions to raise a base's alert level from Aware to Alert should be based on credible threat intelligence that:

- a. the base will be the target of a violent act; and
- b. the violent act is expected within a specific timeframe (for example, within a week or a month).

11. Decisions to raise a base's alert level to Act should be based on credible threat intelligence that:

- a. a violent act is currently happening on the Defence base; or
- b. a violent act against the base is imminent, based on advice from DS&VS, the Chief Security Officer, intelligence and law enforcement agencies, or HQJOC.

Lowering Levels

12. The Chief Security Officer is authorized to de-escalate a SAFEbase alert level nationally, regionally and locally.

13. The Chief Security Officer is authorized to override a SADFO-authorized alert level.

14. SADFOs can de-escalate at the local level when a threat is no longer apparent, or on resolution of an incident, and must notify the HQJOC Joint Operations Room (JOR) within six hours.

SAFEbase Level Requirements

15. Security Management Plans should include plans for each SAFEbase alert level, and should be developed in accordance with the *Joint Framework for Base Accountabilities* (JFBA) (including Emergency Response Plans and Base Continuity Plans), and OPLAN SNAVE.

Note: OPLAN SNAVE describes the broader ADF response plan to counter either a no-warning armed domestic attack on, or emerging potential threat against, Defence bases.

Aware level

16. At the *Aware* level:

- (1) Defence is receiving generalised intelligence with no specific indication of an act against any particular Defence base.
- (2) DS&VS disseminates threat advice as appropriate, and operations at Defence bases are expected to continue as usual.

Case Study: DS&VS has received generalised threat advice from Australian intelligence agencies. A terrorist attack remains probable, but no intelligence of a specific time or location has been received.

Alert levels remain at *Aware*. DS&VS disseminates its threat advice to bases to inform security risk management. Based on this advice, BMs review and adjust, in consultation with SADFOs, security management plans to mitigate security risks. Minor incidents are resolved without the need to elevate the alert level.

Normal business operations continue. Base planning prepares staff and emergency control personnel to respond to a violent security incident.

Alert level

17. At the *Alert* level:

- (1) The SADFO makes a decision to take command of the base in accordance with the JFBA, and additional protective measures are activated in accordance with the Base Security Plan.
- (2) Upon elevating the alert level, the SADFO must notify the HQJOC JOR immediately. HQJOC may decide to enact OPLAN SNAVE.
- (3) HQJOC JOR will coordinate with and notify other stakeholders, including the Chief Security Officer.
- (4) The Chief Security Officer will review the alert level weekly.
- (5) Affected bases operate at higher alert levels with expected limitations on business and operations.

Case Study: The SADFO of a RAAF base in Queensland has been informed of planned protests on public grounds outside the base. Protests have been held without issue outside this base previously and protest organisers have coordinated their activities with the local authorities. However, in consultation with local law enforcement, the SADFO learns that some members of this protest group have been violent at past protests at other Defence bases.

The SADFO decides to raise the alert level to Alert, assumes command in accordance with the JFBA and enacts plans to mitigate the risk of violence against Defence personnel. For this specific base, this includes increased patrols, increased security awareness communications, and the locking of nonessential access points.

The SADFO alerts HQJOC JOR of the elevated alert level. HQJOC JOR notifies all key stakeholders, including the Chief Security Officer, and monitors the situation.

The base continues to operate at an alert level of Alert until the protest ends. After reviewing the situation, the SADFO returns the base to an Aware level and notifies HQJOC JOR.

Act level

18. At the Act level:

- (1) the SADFO makes a decision to take command of the base in accordance with the JFBA and activates emergency responses and procedures.
- (2) the SADFO must notify and coordinate with local law enforcement authorities upon elevation. Civilian police have primacy.
- (3) the SADFO must alert and coordinate with the HQJOC JOR as soon as reasonably practicable and OPLAN SNAVE may be enacted by HQJOC.
- (4) HQJOC JOR will coordinate with and notify other stakeholders, including the Chief Security Officer.
- (5) The Chief Security Officer will review the alert level every 48 hours.
- (6) The Act level should be maintained for as long as the violent act is underway or expected to be imminent. It is expected that this alert level is sustained for no longer than 48 hours.

Case Study: *The Australian Federal Police (AFP) have just disrupted a terrorist cell in a city in New South Wales, which had been planning to attack a Defence base in the nearby region. Defence's Chief Security Officer is informed that the AFP was able to arrest most of the cell's leaders, but has reason to believe some of its members escaped.*

After receiving this threat advice, the Chief Security Officer instructs SADFOs in the nearby region to raise their base's alert level to Alert. Local SADFOs communicate the increased threat to base personnel and implement additional security measures in accordance with their security management plan.

The next day, four unauthorised persons enter one of the bases and ignore instructions from the contracted guards. They are carrying backpacks and the guards are concerned that they may contain weapons.

In response, the SADFO contacts local law enforcement in accordance with the base's emergency plans and raises the SAFEbase level to Act. The SADFO then notifies HQJOC JOR. Emergency Services arrive at the scene shortly.

While the SADFO is overseeing emergency procedures, HQJOC JOR notifies key stakeholders, including Defence's Chief Security Officer. The Chief Security Officer liaises with the intelligence and law enforcement agencies to assess the ongoing threat.

Local law enforcement are able to quickly resolve the situation and all intruders are now in custody. There is no longer a direct threat and the SADFO decides to lower the alert level to Alert, and notifies HQJOC JOR.

Updated threat advice from the intelligence and law enforcement agencies convinces the Chief Security Officer that there is no further specific threat of violence against bases in the region. The Chief Security Officer instructs regional bases to lower their SAFEbase levels to Aware.

Assurance requirements

19. The Chief Security Officer will report on all instances of alert level elevations to the Secretary and Chief of Defence Force.
20. SADFOs and BMs are to report on all security incidents that arise during elevated alert levels, in accordance with DSPF Principle 77 – *Security Incidents and Investigations*.
21. SADFOs and BMs should regularly review their base security plans, exercises, and emergency incident response plans in accordance with the JFBA.

Document administration

Identification

DSPF Control	SAFEBASE Security Alert Level System
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 83.1
Version	3
Publication date	31 July 2020
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Defence Security Alert Level System
Related DSPF Control(s)	Counterintelligence Physical Security Physical Security Certification and Accreditation Access Control Contracted Security Guards Identification, Search and Seizure Regime Weapons Security Explosive Ordnance Security

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	25 March 2019	AS SPS	SAFEBASE redesign system: simplified to three alert levels; additional customisation options; and clarification of authorities and notification responsibilities.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF



Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Fuel Security

General principle

1. Bulk petroleum fuel must be secured from theft, loss or unauthorised access.

Rationale

2. Bulk fuel, because of its flammability, has the capacity to cause large fires and explosions presenting significant risks to people, the environment and capability assurance. Tampering with fuels storage and handling equipment by untrained persons can result in such risk being realised. In addition, fuel is a valuable commodity and is known to be targeted for theft by unscrupulous organisations or individuals. Systematically managing the security risk environment for Defence Fuel Installations and Defence Fuel Supply Chain (DFSC) activities provides a secure environment in which operations may be successfully and safely conducted. Additionally, it assures Defence fuel stocks and associated plants are protected from unauthorised actions.

Expected outcomes

3. DFSC workers, including authorised visitors and contractors, are protected from security related risks associated with external threats.
4. Access to Defence bulk fuel sites, facilities and/or fuel supply chain vehicles is controlled in accordance with prescribed internal and external (legislative) requirements.
5. Defence property within the DFSC (including intellectual property and data) is protected from harm or loss.
6. Fuel operations within the DFSC comply with all requirements of Defence Security policy.
7. Defence personnel and persons engaged under a contract are fully compliant with the *Defence Fuels Management System (DFMS) Element 11.0: Security Management*.

Escalation Thresholds

Risk Rating	Responsibility
Low	APS6 / O4 or equivalent in relevant Group / Service
Moderate	EL1 / O5 or equivalent in relevant Group / Service
Significant	Director General (DG) / EL2 / O6 or equivalent in relevant Group / Service
High	Defence Security Committee (DSC) via Commander Joint Logistics (CJLOG)
Extreme	DSC via CJLOG

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Fuel Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 84
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	Commander Joint Logistics

Related information

Government Compliance	PSPF Core Requirements: Entity physical resources and Entity facilities. Legislation: <i>The following legislation always applies.</i> • <u>Work Health and Safety Act 2011</u> • <u>Work Health and Safety Regulations 2011</u> • <u>Environment Protection and Biodiversity Conservation Act 1999</u> <i>In specific circumstances the following can also apply;</i> • <u>Aviation Transport Security Act 2004</u> • <u>Maritime Transport and Off-shore Facilities Security Act 2003</u> • <i>Specific Airports Acts and Regulations</i> • <i>Specific Ports and Marine Environment management legislation</i> • <i>The Australian Code for the Transport of Dangerous Goods by Road and Rail</i> • <i>State based Pipelines management legislation</i>
Read in conjunction with	All policy and procedures as prescribed by single Service requirements (Navy, Army or Air Force as applicable) in relation to security of Defence assets and activities. All Elements of the DFMS in relation to the safe handling of fuel.
See also DSPF Principle(s)	Personnel Security Clearance Temporary Access to Classified Information and Assets Identity Security Physical Security Certification and Accreditation Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	Defence Fuel Management System – Element 11.0: Security Management

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy