Australian Government
Department of Defence
Intelligence & Security

AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL

SEPTEMBER 2009

May be announced to the public.
May be released to the public.

All Australian Government information, whether security classified or not, is protected from unauthorised disclosure under the *Crimes Act 1914*. Australian Government information may only be released in accordance with the *Australian Government Protective Security Manual*.

Foreword

The Government's use of the Internet is ubiquitous. It helps all levels of government in Australia to deliver services and conduct business flexibly and efficiently. The Internet has become an essential tool for all government officials. Operating in cyberspace, however, exposes government information and systems to serious security risks – appropriate measures must be taken to mitigate these risks.

The cyber security threat is not an emerging threat – it is here with us now.

Global Internet-connectivity provides the opportunity for our Internet-connected systems to be exploited from anywhere in the world. Furthermore, the Internet readily provides information about vulnerabilities and how to exploit them. Consequently, the capabilities of malicious entities on the Internet continue to grow, posing a serious and persistent threat to the security of government information and systems.

All government department and agency heads are responsible for the security of the information their personnel handle in their daily business and operations. Each department and agency is not only entrusted with the protection of its own information, but must also ensure information provided by private and government individuals and organisations, including international partners, is protected to the same standard as their own information.

While much attention is focussed on cyber security threats to your information, existing traditional threats have not disappeared. We must remain vigilant in securing our information whether our systems are connected to the Internet or not.

The Australian Government Information Security Manual provides a framework that enables you to address both new and existing security risks to your systems while allowing you to conduct your business effectively. While this manual sets down minimum requirements for information security, it provides the flexibility to adapt the requirements to suit your own business needs by using a rigorous risk management process.

Finally, I encourage you strongly to apply the security measures and procedures described herein and to ensure you have effective information security governance arrangements in place – doing so will provide assurance that the information that is entrusted to you is properly protected.

Ian McKenzie
Director
Defence Signals Directorate

Table of Contents

About Information Security

Australian Government Information Security Manual

Understanding and Using this Manual

PRINCIPLE

1.1.1. Information relating to the releasability of this manual and processes for risk managing controls is needed to ensure that it can be as relevant to as many stakeholders as possible.

OBJECTIVE

1.1.2. To assist agencies in using this manual in a risk managed approach to ensure that appropriate protection for information that is processed, stored or communicated by their systems.

CONTEXT

Scope

1.1.3. This section provides information on how to interpret the content and the layout of content within the *Australian Government Information Security Manual* (ISM) for the protection of information that is processed, stored and communicated by government systems.

Target audience

1.1.4. The target audience for this manual is information security practitioners within, or contracted to, an agency. This includes, but is not limited to:

- security executives / chief information security officers (CISOs)
- agency security advisors (ASAs)
- information technology security advisors (ITSAs)
- information technology security managers (ITSMs)
- information technology security officers (ITSOs), and
- infosec-registered assessors.

Framework

1.1.5. This manual uses a framework throughout to present information in a consistent manner. The framework consists of a number of headings within each section. These are described below.

- Principle – the reason for the inclusion of a section within this manual.
- Objective – the aim of implementing requirements within a section.
- Context – the scope, applicability and any exceptions for a section.
- Risks – the threat, vulnerability, asset and impact associated with a security risk to information.
- Controls – risk reduction measures with associated compliance requirements for reducing the level of security risk to an acceptable level.
- Guidance – optional risk reduction measures for further reducing security risk that is already at an acceptable level.
- Rationale – the reasoning behind controls and compliance requirements.

Continued on next page

- References – references to external sources of information that can assist in the interpretation or implementation of controls.
- Examples – scenarios to assist with interpreting controls in practical circumstances.

Paragraph numbering

1.1.6. This manual provides paragraph numbering consisting of several fields separated by periods. The fields are ordered as follows: part number, chapter number and then paragraph number.

Applicability indicators

1.1.7. This manual provides applicability indicators for non-security classified and security classified information, equipment and processes.

1.1.8. Applicability indicators are provided in the form of three elements in the title of each requirement. The first element indicates if the requirement is applicable to non-security classified information, the second element indicates the non-national security classifications that are applicable and the third element indicates the national security classifications that are applicable.

1.1.9. For example, a requirement relating to non-security classified information and security classified information would be indicated by [U,IC-HP,R-TS], a requirement relating explicitly to PROTECTED systems would be indicated by [–,P,–] and a requirement relating to UNCLASSIFIED and RESTRICTED systems would be indicated by [U,–,R].

Compliance language

1.1.10. The requirements in this manual use language as defined by the International Engineering Task Force's (IETF's) request for comments (RFC) 2119 to indicate differing degrees of compliance.

Applicability of controls

1.1.11. Whilst this manual provides controls for technologies not all systems will use all of these technologies. As such when a system is developed the agency will determine the appropriate scope of the system and which controls within this manual are applicable. If a control within this manual is outside the scope of the system then variation processes are not applicable. However, if a control is within the scope of the system yet the agency chooses not to implement the control then they will need to follow the variation procedures as outlined below.

Controls with a 'required' compliance requirement

1.1.12. A control with the 'required' compliance requirement indicates that the control is mandatory and cannot be risk managed. These controls relate predominately to the use of high grade cryptographic equipment (HGCE) and associated key management procedures.

Controls with a 'must' compliance requirement

1.1.13. A control with a 'must' or 'must not' compliance requirement indicates that use, or non-use, of the control is mandatory. However, an agency head or their delegate can choose to accept a variation through a waiver or dispensation as long as appropriate procedures are followed.

Controls with a 'should' compliance requirement

1.1.14. A control with a 'should' or 'should not' compliance requirement indicates that use, or non-use, of the control is strongly advised. However, valid reasons to vary from the control could exist in particular circumstances; the full implications need to be considered before choosing a different course.

Guidance with a 'recommended' compliance requirement

1.1.15. Guidance with a 'recommended' compliance requirement indicates that the guidance is optional and is not auditable. However, ITSMs are encouraged to consider the implementation of guidance based on the unique circumstances and risk appetite of their agency.

Dispensations for controls with a 'must' compliance requirement

1.1.16. Agencies can choose to implement alternative controls to those identified in this manual to reduce associated security risks. In such cases the accreditation authority will need to be convinced that the proposed alternative controls adequately reduce the security risks identified within this manual to an acceptable residual level.

1.1.17. If the residual security risk is considered acceptable by the accreditation authority they can grant a dispensation for a control with a 'must' compliance requirement.

Non-compliance with multiple controls

1.1.18. When an agency is non-compliant with multiple controls within this manual the system owner may choose to logically group the areas of non-compliance when following the processes for non-compliance as outlined in this section. For example, producing one security risk assessment for multiple 'should' controls that the agency is non-compliant with instead of a specific security risk assessment for each control.

RISKS

1.1.19. An agency varies from a control in this manual with a 'must' or 'should' compliance requirement, resulting in security vulnerabilities being introduced to or remaining unaddressed in a system.

1.1.20. An agency notices an inconsistency in the ISM and proceeds to implement a solution without first seeking clarification from the Defence Signals Directorate (DSD), resulting in a solution that may not reduce the security risks identified by the ISM.

1.1.21. An agency implements the risk reduction measures as outlined in this manual without considering agency specific circumstances, resulting in the risk treatments not accurately addressing their unique situation.

1.1.22. An agency develops a sub-standard security risk assessment and risk treatment strategy, which provides insufficient detail to properly address information security incidents when they arise.

CONTROLS

[U,IC-HP,R-TS] Non-compliance with controls

1.1.23. Agencies choosing to be non-compliant with a control with a 'must' or 'must not' compliance requirement **must** be granted a waiver or dispensation for their non-compliance.

1.1.24. Agencies choosing to be non-compliant with controls in this manual **must**:

a. document:
   1) the reason(s) for non-compliance
   2) an assessment of the residual security risk(s), and
   3) the date by which to review the decision; and
b. ensure that the agency head (or their delegate) has accepted the security risks associated with non-compliance.

[U,IC-HP,R-TS] Consultation prior to granting waivers

1.1.25. If a waiver relates to a system that processes, stores or communicates information from another agency, that agency **must** be consulted before a waiver is granted.

1.1.26. If a waiver relates to a system that processes, stores or communicates information from a foreign government, that government **must** be consulted before a waiver is granted.

[U,IC-HP,R-TS] Notification of waivers

1.1.27. If a waiver is granted the agency **must** notify:

a. the Auditor-General, Australian National Audit Office
b. the Secretary, Attorney-General's Department
c. the Director, DSD, and
d. the Director-General, Australian Security Intelligence Organisation (ASIO) (only for national security information or systems).

[U,IC-HP,R-TS] Non-compliance with controls

1.1.28. Agencies **must** retain a copy of all decisions to be non-compliant with controls from this manual.

[U,IC-HP,R-TS] Inconsistencies in this manual

1.1.29. Agencies **should** contact DSD if any apparent inconsistencies in the ISM need clarification.

[U,IC-HP,R-TS] Additional controls to this manual

1.1.30. Whilst this manual provides a baseline of controls agencies **should** determine agency and system specific security risks that could warrant controls in addition to those specified in this manual.

GUIDANCE

[U,IC-HP,R-TS] Reviewing waiver decisions

1.1.31. It is **recommended** that agencies granting a waiver review the decision at least annually.

[U,IC-HP,R-TS] Consistency with risk management standards

1.1.32. It is **recommended** that when agencies need to develop security risk assessments and risk treatment strategies that they be consistent with risk management standards.

RATIONALE

Non-compliance with controls

1.1.33. Allowing agencies to vary from the compliance requirements in this manual allows for a risk management approach for the protection of information that is processed, stored or communicated by their systems.

1.1.34. Associated security risks, and where appropriate, rationale are provided for each requirement to assist agency information security personnel in determining the applicability of requirements to their systems.

Inconsistencies in this manual

1.1.35. It is strongly preferred that when there is an apparent inconsistency in this manual that ITSMs contact DSD to seek clarification.

Additional controls to this manual

1.1.36. While a baseline of security risks with associated levels of security risk and corresponding risk treatments are provided in this manual, agencies will almost certainly have differing circumstances to those considered during the security risk assessment. Such variations could be in the form of differing risk sources and threats, assets and vulnerabilities, or exposure and severity. In such cases an agency will need to follow its own risk management procedures to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds.

Consistency with risk management standards

1.1.37. For security risk management to be of true value to an agency it should be relate to the specific circumstances of an agency and its systems as well as being based on an industry recognised approach or risk management guidelines, such as those produced by the Australian Government, Standards Australia and the International Organization for Standardization.

1.1.38. The International Organization for Standardization is currently developing an international risk management standard, including principles and guidelines on implementation, outlined in ISO/FDIS 31000:2009, *Risk Management – Principles and Guidance on Implementation*. The terms and definitions for this standard can be found in ISO/IEC Guide 73, *Risk Management – Vocabulary – Guidelines*.

REFERENCES

1.1.39. This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest baseline (i.e. the latest hardcopy, errata and interim policy releases). This manual, additional information, tools and discussion topics can be accessed from the OnSecure website at https://members.onsecure.gov.au.

1.1.40. Supplementary information to this manual can be found in the following documents:

TOPIC	DOCUMENTATION	AUTHOR
Australian Government Access Only (AGAO)	PSM, pt C, *Information Security*	Attorney-General's Department
Australian Eyes Only (AUSTEO)	*Inter-Agency Security Supplement to the PSM*, s 3	Attorney-General's Department
Business continuity	HB 221:2004, *Business Continuity Management*	Standards Australia
Cabinet information security	*Cabinet Handbook*, ch. 7, Security and handling of cabinet documents	Department of Prime Minister and Cabinet
Cable security	Australian Communications-Electronic Security Instruction (ACSI) 61(C), *Guidelines for the Installation of Communications and Information Processing Equipment and Systems*	Defence Signals Directorate
Communications security roles and responsibilities	ACSI 53, *Communications Security Handbook*	Defence Signals Directorate
Communications security incident reporting	ACSI 107, *Reporting and Evaluating COMSEC Incidents*	Defence Signals Directorate
Emanations security	ACSI 71(C), *A guide to the Assessment of Electromagnetic Security in Military and High-risk Environments*	Defence Signals Directorate
Information handling procedures	PSM, pt C, *Information Security*	Attorney-General's Department

Continued on next page

TOPIC	DOCUMENTATION	AUTHOR
Information security management	AS/NZS ISO/IEC 27001:2006 or ISO/IEC 27001:2005 AS/NZS 17799:2006 or ISO/IEC 27002:2005	Standards Australia
Information security responsibilities	PSM, pt A, *Protective Security Policy*	Attorney-General's Department
Information security risk management	HB 231:2004, *Information Security Risk Management Guidelines*	Standards Australia
Information technology security management	AS 13335:2003, *Information Technology – Guidelines for the Management of Information Technology Security*	Standards Australia
Key management – commercial grade	AS 11770.1:2003, *Information Technology – Security Techniques – Key Management – Framework*	Standards Australia
Key management – high grade	ACSI 105, *Cryptographic Controlling Authorities and Keying Material Management*	Defence Signals Directorate
Management of electronic records that may be used as evidence	HB 171:2003, *Guidelines for the Management of Information Technology Evidence*	Standards Australia
Physical security requirements	PSM, pt E, *Physical Security*	Attorney-General's Department
Privacy requirements	*Privacy Act 1988*	Attorney-General's Department
Reporting of security incidents	PSM, pt G, *Guidelines on Security Incidents and Investigations*	Attorney-General's Department
Risk management	PSM, pt B, *Guidelines on Managing Security Risk*	Attorney-General's Department
	AS/NZS 4360:2004, *Risk Management* HB 231:2004, *Information Security Risk Management Guidelines* HB 436:2004, *Risk Management Guidelines*	Standards Australia
	ISO/DIS 31000, *Risk Management – Principles and Guidance on Implementation* ISO/IEC Guide 73, *Risk Management – Vocabulary – Guidelines for use in Standards*	International Organization for Standardization
	NIST SP 800-30, *Risk Management Guide for Information Technology Systems*	National Institute of Standards and Technology

Continued on next page

TOPIC	DOCUMENTATION	AUTHOR
Security classification labelling	PSM, pt C, *Information Security*	Attorney-General's Department
Security clearances	PSM, pt D, *Personnel Security*	Attorney-General's Department
Storage and archival of information	*Archives Act 1983*	National Archives of Australia

Applicability, Authority and Compliance

PRINCIPLE

1.1.41. This manual and any subsequent policy releases form a baseline of information security requirements for government systems.

OBJECTIVE

1.1.42. To outline how the ISM sets out annually updated security risks, controls, guidance and rationale to assist agencies in protecting the security of information that is processed, stored and communicated by government systems.

CONTEXT

Scope

1.1.43. The ISM is a standard that forms part of a suite produced by DSD relating to information security. Its role is to promote a consistent approach to information security across all Australian Government, State and Territory agencies and bodies. It provides a security risk assessment for information that is processed, stored or communicated by government systems with corresponding risk treatments to reduce the level of security risk to an acceptable level.

Applicability

1.1.44. This manual applies to the same agencies and bodies as the *Australian Government Protective Security Manual* (PSM), namely:

- Australian Government agencies that are subject to the *Financial Management and Accountability Act 1997* (FMA Act)
- bodies that are subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) which have received notice in accordance with that Act that the PSM and by extension the ISM applies to them as a general policy of the Australian Government
- other bodies established for a public purpose under the law of the Commonwealth and other Australian Government agencies, where the body or agency has received a notice from the relevant Minister that the PSM and by extension the ISM applies to them
- State and Territory agencies that hold or access national and non-national security classified information, and
- organisations that have entered a Deed of Agreement with the Australian Government to have access to national or non-national security classified information.

Authority

1.1.45. The *Intelligence Services Act 2001* (ISA Act) states that two functions of DSD are:

- to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means, and
- to provide assistance to Commonwealth and State authorities in relation to cryptography, and communication and computer technologies.

1.1.46. Given DSD's functions the PSM, which sets out the policies, practices and procedures to achieve an appropriate security environment within the Australian Government, references the ISM for the protection of information that is processed, stored or communicated by government systems.

1.1.47. The ISM, like the PSM, has no legislative basis, however it represents the considered advice of DSD provided in accordance with its designated functions under the ISA Act. Unless legislation itself, or a direction given under legislation or by some other lawful authority, compels an agency to comply with the PSM and by extension the ISM, the ISM is simply a manual to structure and assist in the implementation of government policy. In the absence of any such legislative or other requirements, an agency is not required as a matter of law to comply with the ISM.

Compliance

1.1.48. As outlined above the ISM applies to five difference categories of agencies and bodies, encompassing all Commonwealth agencies and bodies, as well as relevant State and Territory agencies holding or accessing national and non-national security classified information. The Australian Government Solicitor believes that, by the terms expressed in the five categories, it is likely to cover the full extent of Commonwealth agencies and bodies.

1.1.49. In the view of the Australian Government Solicitor, all the Commonwealth agencies and bodies to which the PSM, and likewise the ISM, are expressed to apply in categories one, two, three and five, will be legally obligated to comply in one of the following ways:

- through the employees of the agency or body being engaged under the *Public Service Act 1999* (Public Service Act), which obliges APS employees to implement the Government's policies
- by being subject to a notification by the relevant Minister, issued under either section 28 or section 43 of the CAC Act, that the PSM and by extension the ISM applies to them
- by being subject to a notification or direction that the PSM and by extension the ISM applies to the agency, which has been issued by the relevant Minister pursuant to a power in a relevant Act (such as in the agency's enabling legislation); and
- as a result of the operation of a Deed of Agreement between the body or authority and the Commonwealth which obliges compliance with the PSM and by extension the ISM.

1.1.50. The position however is different in relation to category four, by which the PSM and by extension the ISM is expressed to apply to State and Territory agencies that hold or access national and non-national security classified information. By its terms, the memorandum of understanding regarding security classified information signed between the Commonwealth and the States and Territories is not legally binding. It will therefore not give rise to any legal rights or obligations in respect of a failure by a party to comply with its other terms.

Compliance by smaller agencies

1.1.51. As smaller agencies may not always have sufficient staffing or budgets to comply with the requirements of this manual, they may choose to consolidate their resources with another larger host agency to undertake a joint approach to compliance.

1.1.52. In such circumstances smaller agencies may choose to either operate on systems fully hosted by another agency using their information security policies and information security resources or share information security resources to jointly develop information security policies and systems for use by both agencies. As such, the requirements within this manual can be interpreted as either relating to the host agency or to both agencies depending on the approach taken.

1.1.53. In situations where agencies choose a joint approach to compliance, especially when an agency agrees to fully host another agency, the agency heads may choose to seek a memorandum of understanding regarding their information security responsibilities.

Legislation and other Australian Government policy

1.1.54. Compliance with the requirements in this manual is to be undertaken subject to any obligations imposed by relevant legislation or law and subject to any overriding Australian Government policy instruction.

1.1.55. While this manual does contain examples of when some laws may be relevant for agencies, there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.

Personal information collected by government

1.1.56. For the purposes of this manual personal information, as defined within the *Privacy Act 1988* (Privacy Act), that is provided to government by private citizens is not considered to be official information. As such, agencies will need to determine the appropriate controls for protecting such information in order to ensure compliance with the Information Privacy Principles of the Privacy Act. In doing so agencies may choose to handle the information in a similar manner as official information of a specific security classification although this does not automatically mean the personal information takes on that security classification. For example, agencies may choose to apply the controls for X-IN-CONFIDENCE information, with the exception of email requirements, to personal information provided by private citizens when the information resides on their systems.

1.1.57. If an agency manipulates personal information provided by a private citizen for a government purpose this manipulated information becomes official information and will need to go through a classification process to determine appropriate security measures. Furthermore, if this manipulated information needs to be provided to private citizens it will need to be reclassified to an UNCLASSIFIED level, if not already, and declassified before being released into the public domain.

Standalone systems that don't process government information

1.1.58. When agencies deploy standalone systems that are air gapped from corporate agency systems and are provided exclusively to access the Internet, the requirements within this manual are not applicable. This does not include agency Web servers on the Internet or other systems providing government information for public consumption, such systems are considered to be UNCLASSIFIED systems.

Auditing of compliance by the Australian National Audit Office

1.1.59. All requirements within this manual, except 'recommended' guidance, are capable of being audited for compliance by the Australian National Audit Office.

RISKS

1.1.60. An agency fails to comply with interim policy releases for this manual resulting in a lack of awareness of new or modified requirements to assist in reducing security risks to information that is processed, stored or communicated by government systems to an acceptable level.

CONTROLS

[U,IC-HP,R-TS] Compliance

1.1.61. Agencies undertaking system design activities for in-house or out-sourced projects **must** use the latest baseline of this manual for information security requirements.

1.1.62. When DSD makes a determination that newly introduced policy within this manual, or an interim release, is of particular importance, agencies **must** comply with any specified compliance requirements and timeframes.

GUIDANCE

[–,–,–] Compliance

1.1.63. Agencies operating standalone systems that are air gapped from corporate agency systems and are provided exclusively to access the Internet are **recommended** to implement the requirements for UNCLASSIFIED systems.

RATIONALE

Compliance

1.1.64. In complying with the latest baseline of this manual agencies will always be aware of the current threat environment for government systems and the associated acceptable level of security risk.

1.1.65. DSD will continue to monitor security risks and new technologies emerging and if a significant security risk is identified could specify compliance with any newly introduced policy within a shorter timeframe.

1.1.66. As systems that are provided exclusively to access the Internet only process, store and communicate information from the public domain they do not need to be secured to protect the confidentially of information. However, agencies are still encouraged to consider the availability and integrity of such systems as whilst their hacking won't result in the unauthorised disclosure of information it will cause additional work for personnel to restore the service for use.

REFERENCES

1.1.67. Further information on the applicability, authority and compliance with the PSM and by extension the ISM can be found on OnSecure at https://members.onsecure.gov.au in the letter from the Australian Government Solicitor to the Protective Security Coordination Centre with reference 07328264 and the title *Applicability of the Australian Government Protective Security Manual to government agencies and bodies*.

Information Security Within Government

Organisations

PRINCIPLE

1.2.1. Agency information security personnel need to develop an understanding of organisations within the Australian Government which undertake a role in protecting the security of government systems.

OBJECTIVE

1.2.2. To ensure that agency information security personnel are aware of organisations that play a role in protecting the security of government information and systems.

CONTEXT

Scope

1.2.3. This section covers information on organisations involved in providing information security advice to agencies.

Defence Signals Directorate

1.2.4. DSD is required under the ISA Act to perform various functions, including the provision of material, advice and other assistance to Commonwealth and State authorities on matters relating to the security of information that is processed, stored or communicated by electronic or similar means. DSD also provides assistance to Commonwealth and State authorities in relation to cryptography, communications and computer technologies.

1.2.5. In addition, DSD plays an important role in working with industry to develop new cryptographic products. It has also established the Australasian Information Security Evaluation Program (AISEP) in order to deal with the increasing requirement to evaluate information security products.

1.2.6. An agency can contact DSD for advice and assistance relating to the implementation of the ISM through an ITSM or its ASA. ITSMs and ASAs can address questions to DSD by email at assist@dsd.gov.au or phone on (02) 6265 0197.

1.2.7. An agency can contact DSD to provide feedback on the ISM via email at ISM@dsd.gov.au.

1.2.8. Agencies can also contact DSD for advice and assistance on information security incidents. DSD's response will be commensurate with the urgency of the information security incident. There is a 24 hour, seven day a week service available if necessary. The Network Vulnerability Operations section can be contacted by email at incidents@dsd.gov.au or phone on (02) 6266 0009.

1.2.9. Finally, agencies can contact DSD for advice and assistance on the purchasing, provision, deployment, operation and disposal of HGCE. The Crypto Liaison section can be contacted by email at ISG.CryptoLiaison@defence.gov.au

Australian Security Intelligence Organisation

1.2.10. The T4 Protective Security team within ASIO provides the following services to the Australian Government on a cost-recovery basis:

- protective security advice
- technical surveillance counter-measures
- physical security certifications
- protective security risk reviews, and
- physical security equipment testing.

1.2.11. T4 Protective Security can be contacted by phone on (02) 6234 1217, fax (02) 6234 1218 or email t4ps@t4.gov.au.

1.2.12. The postal address for T4 Protective Security is:
T4 Protective Security
GPO Box 2176
Canberra ACT 2601.

Other organisations

1.2.13. The table below contains a brief description of the other organisations which have a role in relating to information security within government.

ORGANISATION	SERVICES
Attorney-General's Department – Protective Security Coordination Centre	Risk management and general protective security. The Protective Security Coordination Centre's training centre provides protective security training.
Department of the Prime Minister and Cabinet	National security advice to government.
Australian Government Information Management Office (AGIMO)	Development, coordination and oversight of Australian Government policy on electronic commerce, online services and the Internet.
Department of Foreign Affairs and Trade	Policy and advice for security overseas.
Australian National Audit Office	Performance audits and better practice guides for areas including information security
Australian Federal Police – Australian High Tech Crime Centre	Law enforcement in relation to electronic crime and other high tech crimes.
Office of the Federal Privacy Commissioner	Advice on how to comply with the Privacy Act and related legislation.
Australian Computer Emergency Response Team	Computer incident prevention, response and mitigation strategies.
Defence Intelligence Organisation (DIO)	Certification of secure compartmented intelligence facilities (SCIFs).
Australian Communications and Media Authority	Provides information on Australian standards for cabling.
National Archives of Australia	Provides information on the archival of government information.

RISKS

1.2.14. Agency information security personnel are unaware of the role organisations play with regards to information security, resulting in a lack of resources to assist them developing an effective information security posture for their agency.

GUIDANCE

[U,IC-HP,R-TS] Organisations providing information security services

1.2.15. It is **recommended** that agency information security personnel familiarise themselves with the information security roles and services provided by Australian Government organisations.

REFERENCES

1.2.16. The following websites can be used to obtain additional information about organisations involved in the security of government systems:

- http://www.dsd.gov.au
- http://www.asio.gov.au/Work/Content/ProtectiveSecurity.aspx
- http://www.ag.gov.au/www/agd/agd.nsf/Page/Security_training
- http://www.pmc.gov.au
- http://www.agimo.gov.au
- http://www.dfat.gov.au
- http://www.anao.gov.au
- http://www.ahtcc.gov.au
- http://www.privacy.gov.au
- http:/www.auscert.org.au
- http://www.defence.gov.au/dio, and
- http://www.naa.gov.au.

Information Security Governance

Roles and Responsibilities

The Agency Head

PRINCIPLE

2.1.1. Agency heads show leadership through awareness of their information security responsibilities.

OBJECTIVE

2.1.2. To ensure that agency heads are aware of their responsibilities for information security within their agency and that it receives appropriate endorsement and coverage.

CONTEXT

Scope

2.1.3. This section covers the role of an agency head with respect to information security.

Chief executive officer

2.1.4. In some agencies and bodies, especially those established under the CAC Act, the person responsible for the agency or body may be referred to as the chief executive officer (CEO). In such cases the policy for the agency head is equally applicable to the CEO.

Devolving authority

2.1.5. When the agency head's authority in this area has been devolved to a board, committee or panel, the requirements of this section relate to the chair or head of that body.

RISKS

2.1.6. An agency head fails to provide sufficient endorsement to information security within their agency, resulting in the agency's information security personnel being unable to effectively undertake their duties to protect information that is processed, stored or communicated by their systems.

2.1.7. An agency head devolves their authority to vary from requirements within the ISM without due consideration of the responsibility that is being devolved.

CONTROLS

[U,IC-HP,R-TS] Support for information security

2.1.8. The agency head **must** provide support for the development, implementation and ongoing maintenance of information security processes and infrastructure within their agency.

[U,IC-HP,R-TS] Delegation of authority

2.1.9. Where the agency head devolves their authority to approve variations from requirements in this manual the delegate **must** be at least a member of the Senior Executive Service or an equivalent management position.

GUIDANCE

[U,IC-HP,R-TS] Delegation of authority

2.1.10. It is **recommended** that when the agency head devolves their authority to approve variations from requirements in the manual the delegate be the CISO.

RATIONALE

Support for information security

2.1.11. Without the full support of the agency head information security personnel are less likely to have access to sufficient resources and authority to successfully implement information security within their agency. As a result information is less likely to be afforded the protection specified by both the PSM and the ISM.

2.1.12. If an information security incident that results in the disclosure of information occurs due to preventable circumstances, the relevant agency head will ultimately be held responsible.

Delegation of authority

2.1.13. When an agency head chooses to devolve their authority to approve of variations from requirements in this manual, they should do so with careful consideration of all the associated risks, as they remain responsible for the decisions made by their delegate.

2.1.14. The CISO is the most appropriate choice for delegated authority as they are a senior executive and hold specialised knowledge in information security and security risk management.

REFERENCES

2.1.15. Further information on the roles and responsibilities of agency heads can be found within each *Roles and Responsibilities* section of the PSM.

The Chief Information Security Officer

PRINCIPLE

2.1.16. The CISO of an agency is responsible for coordinating communication between security and business functions as well as overseeing the application of information security controls and security risk management processes within the agency.

OBJECTIVE

2.1.17. To ensure that CISOs are aware of their responsibilities in regard to information security and to assist them in ensuring the issue receives appropriate endorsement and coverage.

CONTEXT

Scope

2.1.18. This section covers the role of a CISO with respect to information security within an agency.

Appointing a CISO

2.1.19. The requirement to appoint a member of the Senior Executive Service, or an equivalent management position, to the role of CISO does not require a new dedicated position be created in each agency. This role is intended to be performed by the security executive mandated by the PSM.

2.1.20. The PSM describes the security executive as being responsible for coordinating security at a strategic level within an agency. The introduction of the CISO role and associated responsibilities is aimed at providing a more meaningful title for a subset of the security executive's responsibilities that relate to information security within their agency.

2.1.21. Large agencies may choose to appoint two security executives to cover the full range of physical, personnel and information security duties within their agency. In such cases the CISO will focus on information security whilst the other security executive, typically known as the chief security officer (CSO), will focus specifically on physical and personnel security.

RISKS

2.1.22. An agency without a CISO fails to have an agency-wide coordinated approach to information security.

2.1.23. A non-senior executive level person is appointed to the role of CISO resulting in inadequate access to, and influence over, senior executive decision makers within an agency.

2.1.24. A CISO is unable to translate security risks into business risks resulting in a lack of interest in security from business owners within an agency.

2.1.25. A CISO is unaware of the scope of their responsibilities resulting in information security receiving inadequate support within the agency.

2.1.26. A CISO fails to ensure that their agency's compliance with information security policies and standards resulting in a decline in the security culture within the agency.

2.1.27. A CISO fails to control the information security budget resulting in funding being drawn away to other agency business functions.

2.1.28. A CISO fails to set performance indicators and measurement metrics for information security within an agency resulting in insufficient information being available for senior decision makers within the agency.

2.1.29. A CISO fails to ensure that communication between information security and business components of the organisation resulting in business functions perceiving information security as a business inhibitor instead of a business enabler.

2.1.30. A CISO fails to plan for and handle incident and disaster situations within an agency resulting in security classified information being lost or disclosed.

2.1.31. A person not familiar with the concepts of information security and security risk management is delegated the accreditation authority role resulting in inadequate knowledge and experience being applied to accreditation processes.

2.1.32. A CISO for an agency cannot be easily contacted resulting in important information not being able to be communicated to the CISO by external agencies.

2.1.33. A CISO is unable to develop practical information security policy to enable the agency to achieve its business objectives resulting in lost business opportunities.

CONTROLS

[U,IC-HP,R-TS] Requirement for a CISO

2.1.34. Agencies **must** appoint a person to the role of CISO or have the role undertaken by an existing person within the agency.

2.1.35. The CISO role **must** be undertaken by a member of the Senior Executive Service or an equivalent management position.

2.1.36. The CISO **must** be:

a. cleared for access to all information processed by the agency's systems, and
b. able to be briefed into any compartmented information on the agency's systems.

2.1.37. The CISO **should** be responsible for overseeing the management of information security personnel within the agency.

[U,IC-HP,R-TS] Responsibilities – Reporting

2.1.38. The CISO **should** report directly to the agency head on matters of information security within the agency.

[U,IC-HP,R-TS] Responsibilities – Security programs

2.1.39. The CISO **should** develop and maintain a comprehensive strategic level information security and security risk management program within the agency aimed at protecting the agency's information.

2.1.40. The CISO **should** be responsible for the development of an information security communications plan.

2.1.41. The CISO **should** create and facilitate the agency security risk management process.

[U,IC-HP,R-TS] Responsibilities – Ensuring compliance

2.1.42. The CISO **should** be responsible for ensuring compliance with the information security policies and standards within the agency.

2.1.43. The CISO **should** be responsible for ensuring agency compliance with the ISM through facilitating a continuous program of accreditation based on security risk management.

2.1.44. The CISO **should** be responsible for the implementation of information security measurement metrics and key performance indicators within the agency.

[U,IC-HP,R-TS] Responsibilities – Coordinating security

2.1.45. The CISO **should** facilitate information security and business alignment and communication through an information security steering committee or advisory board which meets formally and on a regular basis, and comprises key business and information and communications technology (ICT) executives.

2.1.46. The CISO **should** be responsible for coordinating information security and security risk management projects between business and information security teams.

2.1.47. The CISO **should** work with business teams to facilitate security risk analysis and security risk management processes, including the identification of acceptable levels of risk consistently across the agency.

[U,IC-HP,R-TS] Responsibilities – Working with ICT projects

2.1.48. The CISO **should** provide strategic level guidance for agency ICT projects and operations.

2.1.49. The CISO **should** liaise with agency architecture teams to ensure alignment between security and agency architectures.

2.1.50. The CISO **should** be the accreditation authority when an agency system undergoes accreditation.

[U,IC-HP,R-TS] Responsibilities – Working with vendors

2.1.51. The CISO **should** coordinate the use of external information security resources to the agency including contracting and managing the resources.

[U,IC-HP,R-TS] Responsibilities – Budgeting

2.1.52. The CISO **should** be responsible for controlling the information security budget.

[U,IC-HP,R-TS] Responsibilities – Information security incidents

2.1.53. The CISO **should** be fully aware of all information security incidents within the agency.

[U,IC-HP,R-TS] Responsibilities – Disaster recovery

2.1.54. The CISO **should** coordinate the development of disaster recovery policies and standards within the agency to ensure that business-critical services are supported appropriately in the event of a disaster.

[U,IC-HP,R-TS] Responsibilities – Training

2.1.55. The CISO **should** be responsible for overseeing the development and operation of information security awareness and training programs within the agency.

[U,IC-HP,R-TS] Contacting CISOs

2.1.56. Agencies **should** maintain an email address for their CISO in the form of CISO@agency.gov.au for Australian Government agencies, or CISO@agency.state.gov.au for State and Territory agencies.

GUIDANCE

[U,IC-HP,R-TS] Responsibilities – Providing security knowledge

2.1.57. It is **recommended** that the CISO provide authoritative security advice and familiarity with a range of national and international standards and best practice.

RATIONALE

Requirement for a CISO

2.1.58. The role of the CISO is based on industry best practice and has been introduced to ensure that information security is managed at the senior executive level within agencies.

Responsibilities

2.1.59. The CISO within an agency is responsible predominately for facilitating communications between information security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives within the agency.

2.1.60. The CISO is also responsible for providing strategic level guidance for the agency security program and ensuring compliance with national policy, standards, regulations and legislation.

The Agency Security Advisor

PRINCIPLE

2.1.61. The appointment of an ASA within an agency ensures that physical and personnel security is implemented to appropriately protect information within agencies.

OBJECTIVE

2.1.62. To ensure that ASAs are aware of their obligations relating to information security within this manual.

CONTEXT

Scope

2.1.63. This section covers the role that an ASA undertakes with respect to information security.

RISKS

2.1.64. An ASA fails to implement physical and personnel security within an agency resulting in the agency's information being inadequately protected from loss or unauthorised disclosure.

CONTROLS

[U,IC-HP,R-TS] Responsibilities – Reporting

2.1.65. The ASA **should** report directly to the CISO on matters of information security within the agency.

[U,IC-HP,R-TS] Responsibilities – Providing security knowledge

2.1.66. The ASA **should** pro-actively work with the CISO, ITSMs and ITSOs within an agency to ensure that physical and personnel security requirements are appropriately implemented to protect information within their agency.

RATIONALE

Responsibilities

2.1.67. The purpose of the ASA is to implement physical and personnel controls relating to the protection of an agency's information.

2.1.68. The requirements and qualifications for ASAs are outlined within the PSM.

The Information Technology Security Advisor

PRINCIPLE

2.1.69. The designation of an ITSM as the ITSA within an agency ensures that information security measures are coordinated across the entire agency.

OBJECTIVE

2.1.70. To provide information regarding additional responsibilities for an ITSM when they are designated the ITSA for their agency.

CONTEXT

Scope

2.1.71. This section covers the role of an ITSM when designated as the ITSA with an agency. Information on the responsibilities of ITSMs can be found in the *Information Technology Security Managers* section in this chapter.

The ITSA

2.1.72. The ITSM within an agency that has overall responsibility for information technology security management across the agency is designated as the ITSA. This title reflects the responsibility this ITSM has as the first point of contact for the CISO and external agencies on any information technology security management matters within the agency.

RISKS

2.1.73. An agency appoints multiple ITSMs within their agency but does not designate one of the ITSMs as the ITSA resulting in a lack of coordination and oversight of information security measures within the agency.

2.1.74. An immediate threat to an agency's systems is identified and an ITSA cannot be contacted to assist in the coordination of protective measures for their agency's systems.

CONTROLS

[U,IC-HP,R-TS] Requirement for an ITSA

2.1.75. Agencies **must** designate an ITSM within their agency as the ITSA.

[U,IC-HP,R-TS] Responsibilities – Reporting

2.1.76. The ITSA **should** report directly to the CISO on matters of information security within the agency.

[U,IC-HP,R-TS] Responsibilities – Coordination of other ITSMs

2.1.77. Where an agency appoints multiple ITSMs, the ITSA **should** be responsible for the coordination and oversight of the other ITSMs within the agency.

[U,IC-HP,R-TS] Contacting ITSAs

2.1.78. Agencies **should** maintain an email address for their ITSA in the form of ITSA@agency.gov.au for Australian Government agencies, or ITSA@agency.state.gov.au for State and Territory agencies.

RATIONALE

Requirement for an ITSA

2.1.79. Designating an ITSM within an agency whose has an additional responsibility of coordinating other ITSMs ensures that information security measures and efforts within an agency are undertaken in a coordinated manner.

2.1.80. The ITSM when fulfilling the designation of ITSA still maintains full responsibilities for their role as an ITSM in addition to ITSA responsibilities.

Information Technology Security Managers

PRINCIPLE

2.1.81. The appointment of ITSMs within an agency ensures that administrative information security measures are appropriately considered and addressed within the agency.

OBJECTIVE

2.1.82. To provide ITSMs with information regarding their information security roles and responsibilities.

CONTEXT

Scope

2.1.83. This section covers the role of an ITSM with respect to information security within an agency.

Information technology security managers

2.1.84. ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of ITSOs. The main area of responsibility of an ITSM is that of the administrative controls relating to information security within the agency.

RISKS

2.1.85. An agency appoints an ITSM who is not familiar with the concepts and practice of information security, resulting in an uncoordinated or incomplete approach to information security within the agency.

2.1.86. An ITSM not cleared to access all information and compartments on the agency's systems is appointed, hindering their ability to conduct thorough security risk assessments.

2.1.87. An ITSM is contracted from a private company who places the interests of the company before that of the agency, resulting in information security issues not being appropriately addressed or reported upon.

2.1.88. An ITSM fails to manage and address identified security risks resulting in an increased level of security risk as the threat environment continues to evolve.

2.1.89. An ITSM fails to provide information security advice to agency ICT projects, or an agency ICT projects failing to seek advice from an ITSM, resulting in system developers and personnel not integrating appropriate security controls into their projects.

2.1.90. A system owner attempts to maintain the accreditation of their systems without input from an ITSM, resulting in an outdated or incomplete perspective of the threat environment relevant to their system.

2.1.91. An ITSM fails to oversee the appropriate implementation of security controls within an agency resulting in an inconsistent and ad-hoc approach to information security within the agency.

2.1.92. An ITSM fails to assist the CISO with the information security budget resulting in the CISO being unaware of the current security risks and priorities resulting in inappropriate resource allocations within the agency.

2.1.93. An ITSM fails to coordinate and report on applicable information security issues to senior management resulting in a lack of awareness by senior management of information security issues and activities within the agency.

2.1.94. An ITSM fails to respond to information security audit findings resulting in system deficiencies not being rectified leading to future information security incidents.

2.1.95. An ITSM fails to guide the disaster recovery process resulting in unacceptable losses to information in the event of a realised disaster within the agency.

2.1.96. An ITSM fails to provide appropriate information security awareness and training for personnel resulting in an information security culture not being fostered within the agency.

CONTROLS

[U,IC-HP,R-TS] Requirement for ITSMs

2.1.97. Agencies **must** appoint at least one ITSM within their agency.

2.1.98. ITSMs **should not** have additional responsibilities beyond those needed to fulfil the role as outlined within this manual.

2.1.99. The ITSM role **should** be undertaken by personnel with an appropriate level of authority based on the size of the agency or their area of responsibility within the agency.

2.1.100. Where an agency has outsourced its ICT services, ITSMs **should** be independent of the company providing the ICT services.

2.1.101. Where an agency has outsourced its ICT services, they **should** ensure that the outsourced company provides a single point of contact within the company who will act as an equivalent to an ITSM within their company on behalf of that agency.

2.1.102. ITSMs **must** be:

a. cleared for access to all information processed by the agency's systems, and
b. able to be briefed into any compartmented information on the agency's systems.

[U,IC-HP,R-TS] Responsibilities – Security programs

2.1.103. ITSMs **should** work with the CISO to develop an information security program within the agency.

2.1.104. ITSMs **should** undertake and manage projects to address identified information security risks.

[U,IC-HP,R-TS] Responsibilities – Working with ICT projects

2.1.105. ITSMs **should** identify systems that require security measures and assist in the selection of appropriate information security measures for such systems.

2.1.106. ITSMs **should** work with system owners to determine appropriate information security policies for their systems.

2.1.107. ITSMs **must** be responsible for assisting system owners to obtain and maintain the accreditation of their systems.

2.1.108. ITSMs **should** consult with ICT project personnel to ensure that information security is factored into the evaluation, selection, installation and configuration of hardware and software.

2.1.109. ITSMs **should** work with agency enterprise architecture teams to ensure that security risk assessments are built into system architectures and to identify, evaluate and select information security solutions to meet the agency's information security objectives.

[U,IC-HP,R-TS] Responsibilities – Working with vendors

2.1.110. ITSMs **should** liaise with vendors and agency purchasing and legal areas to establish mutually acceptable contracts and service-level agreements.

[U,IC-HP,R-TS] Responsibilities – Implementing security

2.1.111. ITSMs **must** be responsible for ensuring the development, maintenance, updating and implementation of security risk management plans (SRMPs), system security plans (SSPs) and any standard operating procedures (SOPs) where higher level, multi-system or agency-wide systems are used.

2.1.112. ITSMs **should** conduct security risk assessments on the implementation of new or updated information security hardware or software on the existing environment and develop treatment strategies if necessary.

2.1.113. ITSMs **should** recommend and coordinate the implementation of information security controls to support and enforce information security policies.

2.1.114. ITSMs **should** provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture.

2.1.115. ITSMs **should** provide technical and managerial expertise for the administration of information security management tools.

[U,IC-HP,R-TS] Responsibilities – Budgeting

2.1.116. ITSMs **should** work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives.

[U,IC-HP,R-TS] Responsibilities – Reporting

2.1.117. ITSMs **should** coordinate, measure and report on technical aspects of information security management.

2.1.118. ITSMs **should** monitor and report on compliance with information security policies, as well as the enforcement of information security policies within the agency.

2.1.119. ITSMs **should** provide regular reports on information security incidents and other areas of particular concern to the CISO.

2.1.120. ITSMs **should** assess and report on threats, vulnerabilities, and residual security risks and recommend remedial actions.

[U,IC-HP,R-TS] Responsibilities – Auditing

2.1.121. ITSMs **should** assist system owners and information security personnel in understanding and responding to information security audit failures reported by auditors.

[U,IC-HP,R-TS] Responsibilities – Disaster recovery

2.1.122. ITSMs **should** assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans.

[U,IC-HP,R-TS] Responsibilities – Training

2.1.123. ITSMs **should** provide information security communication, awareness and training for all agency personnel.

2.1.124. ITSMs **should** develop technical information materials and workshops on information security trends, threats, best practices and control mechanisms as appropriate.

[U,IC-HP,R-TS] Responsibilities – Providing security knowledge

2.1.125. ITSMs **should** maintain a current and up to date security knowledge base comprising of a technical reference library, security advisories and alerts, information on information security trends and practices, and laws and regulations.

2.1.126. ITSMs **should** provide expert guidance on security matters for ICT projects.

2.1.127. ITSMs **should** provide technical advice for the information security steering committee, change management committee and other agency and inter-agency committees as required.

GUIDANCE

[U,IC-HP,R-TS] Requirement for ITSMs

2.1.128. Where an agency is spread across a number of geographical sites, it is **recommended** that the agency appoint a local ITSM at each site.

RATIONALE

Requirement for ITSMs

2.1.129. When agencies outsource their ICT services, it is strongly recommended that ITSMs be independent of any company providing ICT services. This will prevent any conflict of interest for an ITSM in conducting their duties.

2.1.130. Appointing local ITSMs when an agency is spread across a number of geographic sites will ensure that the agency has a point of presence at sites to assist with monitoring information security for systems and responding to any information security incidents.

Responsibilities

2.1.131. ITSMs are generally considered the information security experts within an agency and as such their contribution to improving the information security of systems, providing input to agency ICT projects, assisting other security practitioners within the agency, contributing to information security training and responding to information security incidents is a core aspect of their work.

2.1.132. An ITSM is likely to have the most up to date and accurate understanding of the threat environment relating to systems. As such, it is essential that this information is passed to system owners to ensure that it is considered during accreditation activities.

Information Technology Security Officers

PRINCIPLE

2.1.133. The appointment of ITSOs within an agency ensures that technical information security measures are appropriately considered and addressed within the agency.

OBJECTIVE

2.1.134. To provide ITSOs with information regarding their information security roles and responsibilities.

CONTEXT

Scope

2.1.135. This section covers the role that ITSOs undertake with respect to information security.

Appointing an ITSO

2.1.136. The ITSO role may be combined with that of the ITSM. Small agencies may choose to assign both ITSM and ITSO responsibilities to one person under the title of the ITSA. Furthermore, agencies may choose to have this role performed by existing system administrators with an additional reporting chain to an ITSM for the information security aspects of their role. Finally, agencies may choose to have the responsibilities of an ITSO undertaken externally as part of outsourcing of their ICT services.

RISKS

2.1.137. An agency fails to appoint an ITSO resulting in technical controls not being implemented on systems within the agency.

2.1.138. An ITSO is appointed who does not have adequate skills, experience or knowledge to effectively carry out their duties resulting in technical information security controls being inadequately supported within the agency.

2.1.139. An ITSO fails to conduct effective security administration of systems resulting in an uncoordinated or incomplete approach to information security within the agency.

2.1.140. An ITSO fails to research threats and vulnerabilities of systems in conjunction with security risk assessments resulting in system security controls failing to address the changing threat environment.

2.1.141. An ITSO fails to ensure that system security, audit trails and logs and system configurations are regularly reviewed, resulting in modifications to configurations and intrusion attempts going unnoticed.

2.1.142. An ITSO fails to respond to information security incidents resulting in information security breaches remaining unaddressed.

2.1.143. An ITSO fails to respond to information security audit findings resulting in system deficiencies not being rectified.

2.1.144. An ITSO fails to develop the disaster recovery process resulting in unacceptable losses to information in the event of a realised disaster within the agency.

2.1.145. An ITSO fails to communicate information security requirements to system owners and personnel resulting in an information security culture not being fostered within the agency.

CONTROLS

[U,IC-HP,R-TS] Requirement for ITSOs

2.1.146. Agencies **must** appoint at least one ITSO within their agency.

2.1.147. The ITSO role **should** be undertaken by personnel with an appropriate level of authority based on the size of the agency or their area of responsibility within the agency.

2.1.148. ITSOs **must** be:

a. cleared for access to all information processed by the agency's systems, and
b. able to be briefed into any compartmented information on the agency's systems.

[U,IC-HP,R-TS] Responsibilities – System security administration

2.1.149. ITSOs **should** validate and authorise user and access administration on systems in accordance with the defined policies, standards and procedures of the agency.

2.1.150. ITSOs **should** perform system security administration on designated systems, including operating systems and network devices, in accordance with the defined policies, standards and procedures of the agency, as well as with industry best practice and vendor guidelines.

2.1.151. ITSOs **should** perform installation and configuration management of systems, including policy assessment and compliance tools, network security applications and host-based security systems.

2.1.152. ITSOs **should** ensure patches are applied and remove known system weaknesses as a means of hardening systems in accordance with information security policies and standards.

2.1.153. ITSOs **should** validate and authorise change requests, escalating such requests when appropriate as part of the change management process.

[U,IC-HP,R-TS] Responsibilities – Security assessments

2.1.154. ITSOs **should** perform vulnerability assessments to ensure that systems are protected against known and potential threats and are free from known vulnerabilities.

2.1.155. ITSOs **should** research threats and vulnerabilities and, where appropriate, take actions to mitigate threats and remediate vulnerabilities.

2.1.156. ITSOs **should** assist operational staff to locate and repair information security problems and failures.

[U,IC-HP,R-TS] Responsibilities – Information security incidents

2.1.157. ITSOs **should** respond to and, where appropriate, resolve or escalate reported information security incidents in accordance with the incident response plan (IRP).

2.1.158. ITSOs **should** report unresolved network security exposures, misuse of resources or non-compliance situations to an ITSM.

2.1.159. ITSOs **should** respond to and follow up on security events in system and event logs.

2.1.160. ITSOs **should** collate information security incident and event data to produce monthly exception and management reports.

[U,IC-HP,R-TS] Responsibilities – Auditing

2.1.161. ITSOs **should** manage and audit system event logs.

2.1.162. ITSOs **should** implement or coordinate remediation activities required by information security audits, as necessary.

[U,IC-HP,R-TS] Responsibilities – Disaster recovery

2.1.163. ITSOs **should** develop and maintain disaster recovery plans, processes and procedures in accordance with defined policies, standards and business requirements for agency systems.

[U,IC-HP,R-TS] Responsibilities – Training

2.1.164. ITSOs **should** communicate with system owners and personnel to increase their awareness of applicable information security policies and standards.

GUIDANCE

[U,IC-HP,R-TS] Requirement for ITSOs

2.1.165. It is **recommended** that ITSOs don't have additional responsibilities beyond those needed to fulfil the role as outlined within this manual.

RATIONALE

Requirement for ITSOs

2.1.166. Appointing a person whose sole responsibility is to ensure that the technical security of systems is considered essential for agencies to comply with the controls in this manual.

Responsibilities

2.1.167. ITSOs are generally considered specialists in security controls for security systems, operating systems and network devices with an agency and as such their contribution to improving the information security of systems, providing input to agency ICT projects, assisting other security practitioners within the agency, contributing to information security training and responding to information security incidents is a core aspect of their work.

System Owners

PRINCIPLE

2.1.168. System owners obtain and maintain the accreditation of systems, and are responsible for ensuring that associated information security documentation is developed and maintained.

OBJECTIVE

2.1.169. To provide system owners with information regarding their information security roles and responsibilities.

CONTEXT

Scope

2.1.170. This section covers the role that system owners undertake with respect to information security.

RISKS

2.1.171. A system owner performs all information security related duties without an adequate understanding of the threat environment, resulting in a lack of understanding of information security vulnerabilities.

2.1.172. A system is implemented without appropriate information security documentation, resulting in a lack of oversight of information security issues.

2.1.173. An agency activates a system without accreditation providing a launching platform for attacks against other systems.

CONTROLS

[U,IC-HP,R-TS] Seeking assistance from information security personnel

2.1.174. The system owner **should** seek assistance from ITSMs, ITSOs and the ASA in the performance of their information security related responsibilities.

[U,IC-HP,R-TS] Accreditation responsibilities

2.1.175. The system owner **must** be responsible for obtaining and maintaining the accreditation of a system by:

a. working with an ITSM in developing a SSP that complies with the relevant agency information security policy (ISP), this manual and the PSM
b. ensuring that the impact of system modifications or add-on security mechanisms are managed properly
c. identifying any system changes that could imply a need for reaccreditation, and
d. ensuring that information security documentation is complete, accurate and up to date.

[U,IC-HP,R-TS] Documentation responsibilities

2.1.176. The system owner **must** be responsible for ensuring the development, maintenance, updating and implementation of SRMPs, SSPs and any SOPs for systems under their ownership.

RATIONALE

Seeking assistance from information security personnel

2.1.177. While the system owner is responsible for the development, maintenance and implementation of SRMPs, SSPs and any SOPs, their exposure to information security issues can be too narrowly focused and restricted to the systems with which they are familiar. Involving ITSMs, ITSOs and the ASA in the process ensures that a high-level threat environment picture and holistic approach to information security can be mapped to the system owner's understanding of security risks for their specific system.

Accreditation responsibilities

2.1.178. The system owner is responsible for the operation of their system and as such they need to ensure that systems are accredited to meet the agency's operational requirements. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken in an appropriate manner, documented adequately and that reaccreditation activities are completed.

System Users

PRINCIPLE

2.1.179. Policies, plans and procedures are developed for system users to ensure that a consistent and holistic approach is applied to information security across an agency.

OBJECTIVE

2.1.180. To provide system users with information regarding their information security roles and responsibilities.

CONTEXT

Scope

2.1.181. This section covers the role that system users undertake with respect to information security.

Types of system users

2.1.182. This section covers responsibilities for all system users i.e. users with general access (general users), and users with privileged access (privileged users).

RISKS

2.1.183. A system user abuses the policies, plans and procedures for a system they are using, resulting in an information security incident.

2.1.184. A privileged user abuses their privileged access and introduces a vulnerability to a system, resulting in an information security incident.

2.1.185. Personnel are given privileged access without a designated role that needs such access and accidentally causes a change to a system, resulting in a vulnerability being introduced or an information security incident.

CONTROLS

[U,IC-HP,R-TS] Responsibilities of system users

2.1.186. All system users **must** comply with the relevant policies, plans and procedures for the systems they are using.

[U,IC-HP,R-TS] Responsibilities of privileged users

2.1.187. All privileged users **must**:

a. protect privileged account authenticators at the same security classification of the system it secures
b. not share authenticators for privileged accounts without approval
c. be responsible for all actions under their privileged accounts
d. use privileged access only to perform authorised tasks and functions, and
e. report all potentially information security related issues to an ITSM.

RATIONALE

Responsibilities of system users

2.1.188. If agencies fail to develop and maintain a security culture where system users are complying with relevant policies, plans and procedures for the systems they are using there is an increased security risk of a system user unwittingly assisting with an attack against a system.

Responsibilities of privileged users

2.1.189. If privileged users provide authentication information for privileged access to systems to non-approved users, or use their privileged access for personal gain, there is a serious chance of vulnerabilities being introduced to the systems. To further reduce these security risks, agencies can restrict the number of privileged users and closely audit their access.

Information Security Documentation

Documentation Fundamentals

PRINCIPLE

2.2.1. An agency's documentation framework includes information security documentation covering agency-wide information security policy, security risk management, system specific security controls and procedures, and incident response plans.

OBJECTIVE

2.2.2. To assist agencies to develop information security documentation in a manner that allows for easy creation, reference and maintenance to effectively support the accreditation process and system monitoring activities.

CONTEXT

Scope

2.2.3. This section covers at a high level the information security documentation that each agency will need to develop. More specific information on each document can be found in discrete sections of this chapter.

Exception for document types and associated titles

2.2.4. While this manual refers to an information security documentation framework consisting of an ISP, SRMP, SSP, SOPs and an IRP, it does not imply that agencies need to develop single discrete documents with the same titles. However, by using these single discrete documents with the recommended titles agencies can simplify the accreditation processes for their systems.

RISKS

2.2.5. An agency fails to appropriately classify and secure information security documentation which as a result is stolen or copied, giving an attacker an in-depth knowledge of the agency's information security posture.

2.2.6. An agency lacks sufficient information security documentation, has documentation written to an insufficient standard, or has documentation with an insufficient scope, resulting in the security measures of a planned system being unable to be assessed as part of accreditation process.

2.2.7. An agency produces information security documentation for a system that is inconsistent with other documentation for the system resulting in conflicting processes and procedures leading to confusion and an information security incident.

2.2.8. An agency produces information security documentation for a system that is inconsistent with their ISP resulting in conflicting processes and procedures leading to confusion and an information security incident.

2.2.9. An agency fails to develop an overarching document detailing the information security document framework, resulting in the potential for documentation to be overlooked or forgotten leading to security measures agreed during accreditation processes not being maintained for the life of the system.

2.2.10. Agency information security documentation is developed without an understanding of information security, or the agency's business requirements, resulting in documentation that is inaccurate or irrelevant and consequently does not add to or possibly diminishes the effectiveness of the agency's security practices.

2.2.11. An agency outsources the development of information security documentation and fails to review and accept the documentation once it has been created, resulting in a failure to notice that the documentation does not correctly address information security and business objectives.

2.2.12. Information security documentation is developed, but not formally signed off at an appropriate level, resulting in documentation that has insufficient agency support to be effective.

2.2.13. An agency fails to keep information security documentation up to date, resulting in documentation and corresponding practices that do not accurately address the current threat environment for the agency's systems.

CONTROLS

[U,IC-HP,R-TS] Classifying information security documentation

2.2.14. Agencies **must** classify their information security documentation in accordance with the requirements of the PSM.

[U,IC-HP,R-TS] Information security policy

2.2.15. Agencies **must** have an ISP for their agency.

[U,IC-HP,R-TS] Security risk management plan

2.2.16. Agencies **must** ensure that every system is covered by a SRMP.

[U,IC-HP,R-TS] System security plan

2.2.17. Agencies **must** ensure that every system is covered by a SSP.

[U,IC-HP,R-TS] Standard operating procedures

2.2.18. Agencies **should** ensure that, where necessary, SOPs are developed for systems.

[U,IC-HP,R-TS] Incident response plan

2.2.19. Agencies **must** develop an IRP and supporting procedures.

[U,IC-HP,R-TS] Documentation content

2.2.20. Agencies **should** ensure that their SRMP, SSP, SOPs and IRP are logically connected and consistent for each system.

2.2.21. Agencies **should** ensure that their SRMP, SSP, SOPs and IRP are logically connected and consistent with the agency's ISP.

[U,IC-HP,R-TS] Using a documentation framework

2.2.22. Where an agency lacks an existing, well-defined documentation framework, they **should** use the document names defined in this manual.

2.2.23. Agencies **should** create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.

[U,IC-HP,R-TS] Outsourcing development of content

2.2.24. When information security documentation development is outsourced, agencies **should**:

a. review the documents for suitability
b. retain control over the content, and
c. ensure that all policy requirements are met.

[U,IC-HP,R-TS] Obtaining formal sign-off

2.2.25. All information security documentation **should** be formally approved and signed off by a person with an appropriate level of seniority and authority.

[U,IC-HP,R-TS] Documentation maintenance

2.2.26. Agencies **should** develop a regular schedule for reviewing all information security documentation.

GUIDANCE

[U,IC-HP,R-TS] Using higher level documentation to avoid repetition

2.2.27. Where there is some commonality between systems, it is **recommended** that agencies create higher level documents describing the common aspects.

[U,IC-HP,R-TS] Using a documentation framework

2.2.28. Where an agency uses alternative documentation names to those defined within this manual for their information security documentation it is **recommended** that they convert the documentation names to those used in this manual.

[U,IC-HP,R-TS] Developing content

2.2.29. It is **recommended** that agencies ensure that information security documentation is developed by people with a good understanding of both the subject matter and the agency's business.

[U,IC-HP,R-TS] Obtaining formal sign-off

2.2.30. It is **recommended** that agencies ensure that:

a. all high-level information security documentation is approved by the agency head or their delegate, and
b. all system-specific documents be approved by the owner of the system (a senior executive manager) and an ITSM.

[U,IC-HP,R-TS] Documentation maintenance

2.2.31. It is **recommended** that agencies ensure that information security documentation is reviewed:

a. at least annually
b. in response to significant changes in the environment, business or system, and
c. with the date of the most recent review being recorded on each document.

RATIONALE

Classifying information security documentation

2.2.32. Information security documentation frequently contains information that could significantly increase security risk to the systems to which it relates. As such, it needs to be classified and handled appropriately.

Information security policy

2.2.33. The ISP is an essential part of information security documentation as it outlines the high-level policy objectives. The ISP can form part of the overall agency security policy.

Security risk management plan

2.2.34. The SRMP is considered to be a best practice approach to identifying and reducing potential security risks. Depending on the documentation framework chosen, multiple systems could refer to, or build upon, a single SRMP.

System security plan

2.2.35. The SSP describes the implementation and operation of controls within the system as derived from the ISM and the SRMP. Depending on the documentation framework chosen, some details common to multiple systems could be consolidated in a higher level SSP.

Standard operating procedures

2.2.36. SOPs provide a step-by-step guide to undertaking information security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by system users without strong technical knowledge of the system's mechanics. Depending on the documentation framework chosen, some procedures common to multiple systems could be consolidated into a higher level SOP.

Incident response plan

2.2.37. The purpose of developing an IRP is to ensure that when an information security incident occurs a plan is in place to appropriately respond to the situation. In most situations the aim of the response will be to preserve any evidence relating to the information security incident and to prevent the impact of the information security incident from escalating within the agency.

Using higher level documentation to avoid repetition

2.2.38. When agencies develop higher level information security documentation to describe common aspects of systems it allows system-specific security documents to be incorporated into or act as supplements to the higher level documents, rather than repeating the information.

Using a documentation framework

2.2.39. The implementation of an overarching information security document framework ensures that all documentation is accounted for and maintained appropriately. Furthermore, it can be used to describe linkages between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

Outsourcing development of content

2.2.40. Agencies outsourcing the development of information security documentation need to be aware of the contents of the documentation produced. As such, they will still need to review and control the documentation contents to make sure it is appropriate and meets their requirements.

Obtaining formal sign-off

2.2.41. Without appropriate sign-off within an agency, the information security personnel will have a reduced ability to ensure appropriate security procedures are in place for systems. Having sign-off at an appropriate level assists in reducing this security risk as well as ensuring that senior management is aware of information security issues and security risks to the agency's business.

Documentation maintenance

2.2.42. The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation up to date to reflect the changing environment, they do not have a means of ascertaining that their security measures and processes continue to be effective. Resources could be devoted to areas that have reduced effectiveness or are no longer relevant.

Developing content

2.2.43. Ensuring personnel developing information security documentation are sufficiently knowledgeable of information security issues and business requirements will assist in achieving the most useful and accurate set of documentation.

Information Security Policies

PRINCIPLE

2.2.44. The development of an ISP is an essential component of any information security documentation framework which allows senior managers to set the overall security direction and principles for an agency.

OBJECTIVE

2.2.45. To provide direction on the content and development of an ISP.

CONTEXT

Scope

2.2.46. This section relates to the development of ISPs. Information relating to other mandatory documentation can be found in the *Documentation Fundamentals* section.

RISKS

2.2.47. An agency fails to develop an ISP, resulting in a lack of awareness of information security policies, standards and responsibilities.

2.2.48. An agency develops an ISP with an insufficient scope, or level of detail, resulting in an insufficient baseline for the development of a SRMP.

2.2.49. An agency developing an ISP fails to consult existing policies and standards, resulting in a lack of awareness and consideration of other policies or standards that may be important for the agency.

CONTROLS

[U,IC-HP,R-TS] Contents of the ISP

2.2.50. The ISP **should** describe the information security policies, standards and responsibilities of an agency and set any specific minimum requirements, which will then inform the development of SRMPs.

GUIDANCE

[U,IC-HP,R-TS] Development process

2.2.51. It is **recommended** that agencies follow the process defined below when developing an ISP.

STAGE	DESCRIPTION
1	Gain management support for the development of an ISP.
2	Determine the overall scope, objectives and structure of the ISP.
3	Identify all existing applicable policies and standards and record them in the ISP.
4	Compare the identified objectives with the existing policies and standards to identify policy gaps.
5	Write policy statements to address each gap and record them in the ISP.
6	Identify general and specific responsibilities for information security management.
7	Gain management approval and sign-off.
8	Publish and communicate the ISP to personnel.

[U,IC-HP,R-TS] Organising policy frameworks

2.2.52. It is **recommended** that an agency, having defined their overall policy, produce a more detailed policy framework including:

a. agency accreditation processes
b. responsibilities
c. configuration control
d. access control
e. networking and connections with other systems
f. physical security and media control
g. emergency procedures and information security incident management
h. change management, and
i. education and training.

[U,IC-HP,R-TS] Writing policy statements

2.2.53. It is **recommended** that agencies write appropriate policy statements that are high-level, enduring statements of principle, leaving the selection of controls to be addressed by the SRMP and implementation details to be addressed in SSPs and SOPs.

[U,IC-HP,R-TS] Identifying existing policies and standards

2.2.54. It is **recommended** that agencies consult the PSM and any agency-specific policies in addition to this manual for existing policies or standards that could be applicable.

RATIONALE

Contents of the ISP

2.2.55. Describing the information security policies, standards and responsibilities within the ISP will ensure that sufficient information is available to inform the development of SRMPs.

2.2.56. Agencies may wish to consider the following when developing their ISP:

- the policy objectives
- how the policy objectives will be achieved
- the guidelines and legal framework under which the policy will operate
- the stakeholders
- what resourcing will be available to support the implementation of the policy, and
- what performance measures will be established to ensure that the policy is being implemented effectively.

Development process

2.2.57. Following the recommended development process and considering the recommended policy areas and frameworks will assist in developing an ISP with an appropriate scope and sufficient level of detail to act as a baseline for further information security documentation.

Identifying existing policies and standards

2.2.58. Consulting other documents for existing policies or standards such as the PSM will assist in identifying policies or standards that are applicable to the agency and should be present in the ISP developed.

Security Risk Management Plans

PRINCIPLE

2.2.59. The SRMP is the foundation upon which information security for a system is built and implemented as it assists agencies to identify security risks and develop appropriate risk reduction strategies for their systems.

OBJECTIVE

2.2.60. To provide direction on the content and development of SRMPs.

CONTEXT

Scope

2.2.61. This section relates to the development of SRMPs, focusing on risks associated with the security of systems. Information relating to other mandatory documentation can be found in the *Documentation Fundamentals* section.

RISKS

2.2.62. An agency develops a SRMP with an insufficient scope, content or level of detail, resulting in the agency being unaware of foreseeable security risks and having inadequate risk reduction strategies in place.

CONTROLS

[U,IC-HP,R-TS] Contents of SRMPs

2.2.63. The SRMP **should** contain a security risk assessment and a corresponding treatment strategy.

GUIDANCE

[U,IC-HP,R-TS] Agency risk management

2.2.64. It is **recommended** that agencies incorporate their SRMP into their wider agency risk management plan.

[U,IC-HP,R-TS] Risk management standards

2.2.65. It is **recommended** that agencies develop their SRMP in accordance with Australian or international standards for risk management.

RATIONALE

Risk management standards

2.2.66. Agencies are advised to use Australian or international standards for risk management as they describe a best practice approach to risk management.

2.2.67. Currently the only Australian/New Zealand or international standard on risk management is AS/NZS 4360:2004, *Risk Management*. However, the International Organization for Standardization is currently developing an international standard, ISO/FDIS 31000:2009.

REFERENCES

2.2.68. Information on the development of SRMPs can be found in HB 231:2004, *Information Security Risk Management Guidelines*. In particular, section 5 discusses documentation content. It is available from Standards Australia at http://www.standards.org.au.

2.2.69. PSM Part B, *Guidelines on Managing Security Risk*, contains example templates that can be used for representing information within a SRMP.

System Security Plans

PRINCIPLE

2.2.70. The development of SSPs is an essential component of any information security documentation framework as they describe the controls to be implemented for a system as derived from the ISM as well as any additional controls as determined by the SRMP.

OBJECTIVE

2.2.71. To provide direction on the content and development of SSPs.

CONTEXT

Scope

2.2.72. This section relates to the development of SSPs. Information relating to other mandatory documentation can be found in the *Documentation Fundamentals* section.

Stakeholders

2.2.73. There can be many stakeholders involved in defining a SSP, including representatives from the:

- project, who must deliver the capability (including contractors)
- owners of the information to be handled
- system users for whom the capability is being developed
- management audit authority
- information management planning areas, and
- infrastructure management.

RISKS

2.2.74. An agency seeks an information security assessment of a system but is unable to complete the activity due to insufficient information being provided to the assessor.

2.2.75. An agency implements a system without a comprehensive SSP, resulting in significant security risks remaining unaddressed.

CONTROLS

[U,IC-HP,R-TS] Contents of SSPs

2.2.76. The SSP **must** provide an assessor conducting an information security assessment with sufficient information to assess the security of the system.

GUIDANCE

[U,IC-HP,R-TS] Contents of SSPs

2.2.77. It is **recommended** that agencies select controls from the ISM to be included in the SSP based on the scope of the system with additional system specific controls being included as a result of the associated SRMP or higher-level SSP.

Standard Operating Procedures

PRINCIPLE

2.2.78. The development of SOPs is an essential component of any information security documentation framework as they are one of the main tools used by personnel to comply with and implement the agency's SSPs.

OBJECTIVE

2.2.79. To provide direction on the content and development of SOPs.

CONTEXT

Scope

2.2.80. This section relates to the development of security related SOPs. Information relating to other mandatory documentation can be found in the *Documentation Fundamentals* section.

RISKS

2.2.81. An agency fails to develop SOPs for ITSMs, ITSOs, system administrators and system users, resulting in security duties not being undertaken or being undertaken in an inappropriate manner.

2.2.82. An agency develops SOPs that are inconsistent with their associated SSPs, resulting in confusion as to the correct processes to be undertaken.

2.2.83. An agency develops a SOP with an insufficient scope or level of detail, resulting in uncertainty of procedures.

2.2.84. An agency develops SOPs for system users; however, the system users are not required to read or understand the SOP before being granted access to systems.

2.2.85. An agency fails to provide guidance to system users of their information security responsibilities and consequences of non-compliance, resulting in system users naively or purposefully undertaking actions that assist in, or cause, information security incidents.

CONTROLS

[U,IC-HP,R-TS] Development of SOPs

2.2.86. Agencies **should** develop SOPs for each of the following roles:

a. ITSM
b. ITSO
c. system administrator, and
d. system users.

[U,IC-HP,R-TS] Relationship between SSPs and SOPs

2.2.87. Agencies **should** ensure that SOPs are consistent with all relevant SSPs.

[U,IC-HP,R-TS] ITSM SOPs

2.2.88. The following procedures **should** be documented in the ITSM's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Information security incidents	Reporting and managing information security incidents, including involvement in physical security incident management where the incident could impact on information security.

[U,IC-HP,R-TS] ITSO SOPs

2.2.89. The following procedures **should** be documented in the ITSO's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Access control	Authorising access rights to applications and data.
Asset musters	Labelling, registering and mustering assets, including removable media.
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users.
Configuration control	Approving and releasing changes to the system software or configurations.
Data transfers	• Managing the review of removable media containing data that is to be transferred off-site. • Managing the review of incoming media for viruses or unapproved software.
Hardware destruction	Managing the destruction of unserviceable equipment and media.
System integrity audit	• Reviewing system user accounts, system parameters and access controls to ensure that the system is secure. • Checking the integrity of system software. • Testing access controls. • Inspecting equipment and cabling.
System maintenance	Managing the ongoing security and functionality of system software and hardware, including: • maintaining awareness of current software vulnerabilities • testing and applying software patches/updates/signatures, and • applying appropriate hardening techniques.
User account management	Authorising new system users.

[U,IC-HP,R-TS] System administrator SOPs

2.2.90. The following procedures **should** be documented in the system administrator's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Access control	Implementing access rights to applications and data.
Configuration control	Implementing changes to the system software or configurations.
System backup and recovery	• Backing up data, including audit logs. • Securing backup tapes. • Recovering from system failures.
User account management	• Adding and removing system users. • Setting system user privileges. • Cleaning up directories and files when a system user departs or changes roles.

[U,IC-HP,R-TS] System user SOPs

2.2.91. The following procedures **should** be documented in the system user's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Roles and responsibilities	Who is responsible for what aspects of information security.
Warning	A warning that: • system users' actions can be audited, and • system users will be held accountable for their actions.
Passwords	Guidelines on choosing and protecting passwords.
Need-to-know	Guidelines on enforcing need-to-know on the system.
Information security incidents	What to do in the case of a suspected or actual information security incident.
Security classification	The highest security classification for information that can be processed on the system and handling procedures for such information.
Temporary absence	How to secure systems when temporarily absent.
End of day	How to secure systems at the end of the day.
Media control	Procedures for controlling and sanitising media, including requirements for an ITSM or delegate to vet all incoming and outgoing media.
Hardcopy	Procedures for labelling, handling and disposing of hard copy.
Visitors	Preventing unintended display of information to visitors.
Maintenance	What to do for hardware and software maintenance.

[U,IC-HP,R-TS] System users

2.2.92. System users **should** sign a statement that they have read and agree to abide by the system user SOPs.

GUIDANCE

[U,IC-HP,R-TS] Development procedure

2.2.93. It is **recommended** that agencies follow the process defined below when developing a SOP.

STAGE	DESCRIPTION
1	Locate the SSP.
2	Working with one strategy in the SSP at a time, allocate the responsibility for adhering to that rule to: • ITSMs • ITSOs • system administrators, or • system users.
3	Write each rule or procedure in full in the appropriate section of the SOP.

[U,IC-HP,R-TS] System user guidance

2.2.94. It is **recommended** that agencies provide guidance to system users that includes the following:

a. only access data, control information and software to which they have authorised access and a need-to-know
b. immediately report all information security incidents and potential threats and vulnerabilities involving systems to an ITSM
c. protect their authentication information and report any compromise or suspected compromise to an ITSM
d. ensure that media and system output is properly classified, marked, controlled, stored and sanitised
e. protect workstations from unauthorised access
f. inform the support section when access to a particular system is no longer needed, and
g. observe rules and regulations governing the secure operation and authorised use of systems.

RATIONALE

Development of SOPs

2.2.95. In order to ensure that personnel undertake their duties in an appropriate manner, with a minimum of confusion, it is important that the roles of ITSMs, ITSOs, system administrators and system users are covered by SOPs. Furthermore, taking steps to ensure that SOPs are consistent with SSPs will reduce the potential for confusion resulting from conflicts in policy and procedures.

Development procedure

2.2.96. If the recommended SOP development procedure and content guidelines are followed it will increase the likelihood that the SOPs will contain a sufficient scope and level of detail to be appropriate and easily understood by the target audience.

Incident Response Plans

PRINCIPLE

2.2.97. The development of an IRP is an essential component of any information security documentation framework as it ensures that when an information security incident occurs within an agency, appropriate procedures are followed to contain, evaluate and treat the information security incident as well as preventing a reoccurrence.

OBJECTIVE

2.2.98. To provide direction on the content and development of an IRP.

CONTEXT

Scope

2.2.99. This section relates to the development of IRPs to address information security, and not physical incidents within agencies. Information relating to other mandatory documentation can be found in the *Documentation Fundamentals* section.

RISKS

2.2.100. An agency develops an IRP with an insufficient scope or level of detail, resulting in uncertainty during or following an information security incident and leading to actions being undertaken that failed to adequately respond to or exacerbate the situation.

2.2.101. An agency develops an IRP with an inadequate definition of what constitutes an information security incident, resulting in suspicious behaviour on systems going unnoticed.

CONTROLS

[U,IC-HP,R-TS] Contents of IRPs

2.2.102. Agencies **must** include, as a minimum, the following content within their IRP:

a. broad guidelines on what constitutes an information security incident
b. the minimum level of information security incident response and investigation training for system users and system administrators
c. the authority responsible for initiating investigations of an information security incident
d. the steps necessary to ensure the integrity of evidence supporting an information security breach
e. the steps necessary to ensure that critical systems remain operational, and
f. how to formally report information security incidents.

2.2.103. Agencies **should** include within their IRP:

a. clear definitions of the types of information security incidents that are likely to be encountered
b. the expected response to each information security incident type
c. the authority within the agency that is responsible for responding to information security incidents
d. the criteria by which the responsible authority would initiate or request formal, police or ASIO investigations of an information security incident
e. which other agencies or authorities need to be informed in the event of an investigation being undertaken, and
f. the details of the system contingency measures or a reference to these details if they are located in a separate document.

[U,IC-HP,R-TS] Developing supporting procedures

2.2.104. Agencies **should** develop and maintain procedures supporting the plan to:

a. detect potential information security incidents
b. establish the cause of any information security incident, whether accidental or deliberate
c. detail the action to be taken to recover and minimise the exposure from an information security incident
d. report information security incidents, and
e. document any recommendations on preventing a recurrence.

GUIDANCE

[U,IC-HP,R-TS] Defining information security incidents

2.2.105. It is **recommended** that agencies ensure that information security incidents within the IRP are defined by the agency's risk management objectives, including examples of how information security incidents can be detected.

RATIONALE

Contents of IRPs

2.2.106. The guidance provided on the content of IRPs will ensure that agencies have a baseline to develop an IRP with sufficient flexibility, scope and level of detail to address the majority of information security incidents that could arise.

Emergency Procedures

PRINCIPLE

2.2.107. The confidentially of information can be protected in an emergency situation through the development of policies, plans and procedures to reduce uncertainty during an evacuation and assist in protecting information from inappropriate disclosure.

OBJECTIVE

2.2.108. To provide direction on the content and development of emergency procedures.

CONTEXT

Scope

2.2.109. This section covers information relating to the development of policies, plans and procedures for securing work areas during emergency situations. Information relating to other mandatory documentation can be found in the *Documentation Fundamentals* section.

RISKS

2.2.110. During an emergency situation agency personnel leave behind information or unsecured ICT assets, resulting in disclosure to people not authorised to view the information.

CONTROLS

[–,HP,C-S] Contents of emergency procedures

2.2.111. Agencies **should** develop a set of policies, plans and procedures for when personnel evacuate a site which covers the securing or sanitisation, including destruction as necessary, of security classified information and assets.

[–,–,TS] Contents of emergency procedures

2.2.112. Agencies **must** develop a set of policies, plans and procedures for when personnel evacuate a site which covers the securing or sanitisation, including destruction as necessary, of security classified information and assets.

GUIDANCE

[U,IC-P,R] Contents of emergency procedures

2.2.113. It is **recommended** that agencies develop a set of policies, plans and procedures for when personnel evacuate a site which covers the securing or sanitisation, including destruction if necessary, of information and assets.

RATIONALE

Contents of emergency procedures

2.2.114. Developing emergency procedures and ensuring personnel awareness of the procedures will reduce uncertainty during an evacuation and assist in protecting information from inappropriate disclosure.

Information System Accreditation

Conducting Accreditations

PRINCIPLE

2.3.1. Accreditation allows an accreditation authority to give formal recognition and acceptance of the associated residual security risks to information that is processed, stored or communicated by a system.

OBJECTIVE

2.3.2. To provide information on the requirements for information system accreditation and the processes involved.

CONTEXT

Scope

2.3.3. This section covers information on the high-level process of accreditation.

About accreditation

2.3.4. Accreditation is the process by which an authoritative body, the accreditation authority, gives formal recognition and acceptance of the residual security risk to a system and is the prerequisite for the operation of an information system.

2.3.5. The accreditation process involves reviewing information security documentation, assessing the implementation and effectiveness of security controls, determining the residual security risk relating to the operation of a system and seeking acceptance of the residual security risk by an appropriate authority.

National and non-national security classifications

2.3.6. When a system processes both national and non-national security classified information, the security requirements for one security classification category will often meet the requirements for security classifications from the other category. The table below provides an indication of how requirements map to each other.

SYSTEM ACCREDITED FOR	ALSO MEETS REQUIREMENTS FOR
TOP SECRET	• HIGHLY PROTECTED • PROTECTED • X-IN-CONFIDENCE
SECRET	• HIGHLY PROTECTED • PROTECTED • X-IN-CONFIDENCE
CONFIDENTIAL	• PROTECTED • X-IN-CONFIDENCE
HIGHLY PROTECTED	• RESTRICTED
PROTECTED	• RESTRICTED
X-IN-CONFIDENCE	• No national security classifications

Transferring accreditation status

2.3.7. Accreditation status is not transferable, although the process of accreditation can be simplified for a similar system due to an existing system having already undergone an information security assessment. In such cases this will give agencies a baseline from which to begin the accreditation process for the similar system. In such circumstances agencies may choose to assess deltas from the previous information security assessment instead of repeating a complete assessment.

RISKS

2.3.8. An agency fails to undertake an accreditation of a system, resulting in a system that exposes information to security risks that no senior person in the agency has approved as being at an appropriate and acceptable level.

2.3.9. An agency fails to undertake accreditation of a system before it is used operationally, resulting in an un-tested and vulnerable information security posture.

2.3.10. An agency connects a system to another agency or third-party system that lacks appropriate protection, resulting in the other system being used as a launching platform for attacks against the agency's system.

2.3.11. An agency fails to follow appropriate processes in conducting accreditation of a system, resulting in an un-tested and vulnerable information security posture for an agency.

2.3.12. An agency allows its system to process information at a higher security classification than that for which it is accredited for, resulting in inadequate security being used to protect the information.

2.3.13. An agency uses a system for processing AUSTEO or AGAO information that is not under the control of an Australian national, or has not undergone accreditation to process such information, resulting in the exposure of sensitive information.

CONTROLS

[U,IC-HP,R-TS] Conducting accreditations

2.3.14. Agencies **must** ensure that each of their systems is awarded accreditation.

2.3.15. Agencies **must** ensure that that all systems are awarded accreditation prior to connecting them via a gateway/cross domain solutions (CDS).

2.3.16. Agencies **must** ensure that that all systems are awarded accreditation before they are used operationally.

[U,IC-HP,R-TS] Accreditation framework

2.3.17. Agencies **must** develop an accreditation framework for their agency.

[U,IC-HP,R-TS] Initial accreditation

2.3.18. Agencies **should** use the latest baseline of this manual when developing the SSP as part of the initial accreditations of their systems.

[U,IC-HP,R-TS] Transferring accreditation status

2.3.19. When an agency conducts delta information security assessments from a similar system that has been awarded accreditation, the period between accreditation and reaccreditation **should not** exceed that remaining before the reference system is due for reaccreditation.

[U,IC-HP,R-TS] Due diligence

2.3.20. Where an agency's system exchanges information with a third-party system, the agency **must** ensure that the receiving party has appropriate measures in place to provide a level of protection commensurate with the security classification or sensitivity of their information.

2.3.21. An agency **must** ensure that a third party is aware of the agency's information security expectations by defining expectations in documentation that includes, but is not limited to:

a. contract provisions, or
b. a memorandum of understanding.

2.3.22. An agency **must** ensure that a third party complies with the agency's information security expectations through a process providing assurance to agency management that the operation of information security within the third party meets, and is expected in the future to meet, these expectations.

[U,IC-HP,R-TS] Processing restrictions

2.3.23. Agencies **must not** allow a system to process, store or communicate information above the security classification for which the system has received accreditation.

[U,IC-HP,R-TS] Accrediting systems bearing a caveat or compartment

2.3.24. A system that processes, stores or communicates caveated or compartmented information **must** be accredited for such caveated or compartmented information.

[–,IC-HP,R-TS] Requirements for Australian control

2.3.25. Agencies **must** ensure that systems processing, storing or communicating AUSTEO or AGAO information remain under the control of an Australian national working for the Australian Government at all times.

RATIONALE

Conducting accreditations

2.3.26. Accreditation ensures and recognises that sufficient security measures, policies and procedures have been put in place to protect information that is processed, stored or communicated by the system. As such when systems are awarded accreditation the accreditation authority accepts that the residual security risks relating to information is appropriate for the security classification of the information.

Initial accreditation

2.3.27. In performing accreditations against the latest baseline of this manual, agencies are ensuring that they are taking the most recent threat environment into consideration.

2.3.28. DSD continually monitors the threat environment and conducts research into the security impact of emerging information security trends. In addition, DSD continually seeks and encourages feedback from agencies and private industry on emerging information trends. These research and engagement activities are reflected in the security risks and associated risk reduction controls in this manual. With each release of this manual, controls can be added, rescinded or modified depending on changes in the threat environment.

Due diligence

2.3.29. When an agency is connecting a system to another party they need to be aware of the security measures the other party has implemented to protect their information. More importantly, the agency needs to know where the other party may have varied from controls in this manual.

2.3.30. Methods that an agency may use to ensure that other agencies and third parties comply with the agency's information security expectations include:

- conducting an accreditation of the system being connect to
- seeking an information security review by an infosec-registered assessor, or
- seeking a copy of an existing information security assessment report in order to make their own accreditation decision.

2.3.31. Ultimately, the agency needs to accept any security risks associated with connecting their system to the other party's system. This includes the other party's system potentially being used as a platform to attack their system or spilling information onto their system requiring subsequent cleanup processes.

Accrediting systems bearing a caveat or compartment

2.3.32. When processing caveated or compartmented information on a system, agencies need to ensure that the system has received accreditation for the information. Furthermore, when agencies are dealing with AUSTEO or AGAO information they need to be aware of the requirement for an Australian national to remain in control of the system at all times.

Planning for Accreditation

PRINCIPLE

2.3.33. Appropriate planning for accreditation involves the consideration of accreditation requirements prior to designing, developing and deploying a new system.

OBJECTIVE

2.3.34. To ensure that appropriate consideration is given to accreditation activities during system design and development stages to facilitate the process and reduce potential delays to accreditation activities at a later date.

CONTEXT

Scope

2.3.35. This section covers information on the planning for accreditation activities within an agency.

RISKS

2.3.36. An agency system owner fails to contact an ITSM to seek guidance on the accreditation process, resulting in the system owner wasting effort and resources on a process with which they are not familiar.

2.3.37. An agency system owner fails to contact their accreditation authority to indicate their intention to begin the accreditation process, resulting in the accreditation authority being unaware of a new system being designed and developed for which they will be responsible.

2.3.38. An agency plans to connect its system to another agency or third party's system without undertaking due diligence activities, resulting in the agency being unaware of security risks it is accepting and additional risk reduction strategies that could have been put in place by the agency or third party it is connecting to.

CONTROLS

[U,IC-HP,R-TS] Pre-accreditation activities

2.3.39. Prior to beginning accreditation the system owner **should**:

a. advise the accreditation authority of their intent to establish a system, and
b. request advice relating to the accreditation process from an ITSM.

2.3.40. For multi-national and multi-agency systems, the accreditation authority **should** be determined by a formal agreement between the parties involved prior to beginning accreditation activities.

GUIDANCE

[U,IC-HP,R-TS] Due diligence

2.3.41. It is **recommended** that agencies review information security assessment reports, including the release date, when determining the security risks associated with connecting to other systems.

[U,IC-HP,R-TS] Information security documentation development

2.3.42. It is **recommended** that all relevant stakeholders work together to develop the information security documentation, which includes the SRMP, SSP, any SOPs and the IRP.

RATIONALE

Pre-accreditation activities

2.3.43. The purpose of contacting an ITSM prior to the beginning of any accreditation process is to ensure that current contacts are established and that the agency is aware of any changes that could have taken place to the process since the last accreditation of one of its systems.

Due diligence

2.3.44. Agencies should be cautious when planning to connect to systems belonging to other agencies as their controls may not be similar to their own. As such, it is important that the connecting agency reads the other agency's information security assessment report and accepts any variations or security risks that could be introduced to their own information security posture.

Information Security Assessments

PRINCIPLE

2.3.45. An information security assessment process is undertaken to review information security documentation, assess the actual implementation and planned effectiveness of controls for a system and report on any residual security risks relating to the operation of the system to the accreditation authority.

OBJECTIVE

2.3.46. To ensure that agencies are aware of what activities are undertaken during an information security assessment and who is responsible for undertaking such activities.

CONTEXT

Scope

2.3.47. This section covers information on the process of undertaking an information security assessment.

Exception for undertaking information security assessments

2.3.48. In exceptional circumstances the accreditation authority may elect not to have an information security assessment conducted on a system before making an accreditation decision. The test to be satisfied in such circumstances is that if the system is not operated immediately it would have a devastating and potentially long lasting effect on the operations of the agency.

Who can undertake an information security assessment

2.3.49. With the exception of TOP SECRET systems, both ITSMs and infosec-registered assessors can undertake information security assessments. Information security assessments for TOP SECRET systems can only be undertaken by DSD.

2.3.50. For organisations supporting agencies, the information security assessment can be undertaken by an ITSM or by an infosec-registered assessor.

2.3.51. For multi-national and multi-agency systems, the nation or agency responsible for the information security assessment is determined by a formal agreement between the parties involved.

2.3.52. For agencies with systems that process, store or communicate caveated or compartmented information there could be a mandated agency responsible for the information security assessment that is different to that of the system owner.

Who can assist with an information security assessment

2.3.53. A number of other agencies and personnel within agencies are often consulted during the information security assessment process.

2.3.54. Agencies or personnel that can be consulted on physical security aspects of information security include:

- ASIO for TOP SECRET sites
- DIO for TOP SECRET SCIFs
- Department of Foreign Affairs and Trade (DFAT) for systems located at overseas posts and missions, and
- the ASA for all other systems.

2.3.55. The ASA can be consulted on personnel security aspects of information security.

2.3.56. An ITSM or communications security officer can be consulted on communications security (COMSEC) aspects of information security.

Information security assessment process

2.3.57. An information security assessment is conducted as part of the wider accreditation process. The aim of an information security assessment is to review the information system architecture (including the information security documentation), assess the actual implementation and effectiveness of controls for a system (an information security certification) and to report on any residual security risks relating to the operation of the system to the accreditation authority.

Information security assessment outcomes

2.3.58. The outcome of an information security assessment is a report outlining the residual security risks to the operation of a system and an accreditation recommendation for the accreditation authority.

Independent information security assessments

2.3.59. An information security assessment can be conducted by an ITSM within an agency; however, the agency may choose to add an extra level of objectivity by engaging the services of an infosec-registered assessor to undertake any of the three stages of an information security assessment.

2.3.60. Connections to certain inter-agency systems could require an independent information security assessment from an infosec-registered assessor as a prerequisite to the accreditation of the system. Such requirements can be obtained from the inter-agency system owners.

Delta information security assessments

2.3.61. Agencies are encouraged to maximise reuse opportunities from pre-existing information security assessment outcomes when accrediting or reaccrediting their systems.

2.3.62. Situations in which delta information security assessments can be undertaken to leverage existing outcomes include where:

- a system has failed to achieve accreditation and changes have been made to the system to reseek an accreditation decision
- a system is being deployed based on a pre-existing system that has already undergone an information security assessment, and
- a system is undergoing reaccreditation.

2.3.63. Such delta information security assessments would focus on assessing deltas between the two systems or assessing that where controls were originally identified as being deficient or lacking, they have been subsequently changed or implemented and are operating effectively.

RISKS

2.3.64. An agency uses a system owner to conduct an information security assessment resulting in a conflict of interest in the outcome of the process.

2.3.65. An agency fails to undertake an information security assessment of each of its systems, resulting in the security status of the systems being unknown and unmanageable and exposing the information associated with those systems to an unknown level of security risk.

2.3.66. An agency uses a gateway/CDS that has not undergone an information security assessment, resulting in its security status being unknown and unmanageable and exposing the information associated with the gateway/CDS to an unknown level of security risk.

2.3.67. An agency hires a service provider to provide gateway/CDS services who has not had an information security assessment, resulting in its security status being unknown and unmanageable and exposing the information associated with the gateway/CDS to an unknown level of security risk.

2.3.68. An agency connects to another agency or third party's gateway/CDS that has not had an information security assessment conducted, resulting in attackers exploiting the agency's system through the connected gateway/CDS.

2.3.69. A system owner fails to implement their SSP resulting in an information security assessment being unable to confirm that controls have been implemented for the system.

2.3.70. A detailed review of information security documentation is not undertaken resulting in uncertainty as to whether the SSP complies with this manual.

2.3.71. A system owner fails to document in their SSP all variations with the baseline of this manual used resulting in other agencies and being unaware of security risks they are accepting when connecting to the system.

2.3.72. A system owner determines that controls identified in this manual do not relate to the function of a system yet fails to document in the SSP which controls were not applicable, resulting in other agencies being unaware of the specific security risks addressed by the accreditation process.

CONTROLS

[U,IC-P,R] Information security assessments

2.3.73. All systems **should** undergo an information security assessment as part of the accreditation process.

[–,HP,C-TS] Information security assessments

2.3.74. All systems **must** undergo an information security assessment as part of the accreditation process.

[U,IC-P,R] Information security assessments of commercial providers

2.3.75. Agencies **should** ensure that any companies contracted to provide Internet gateway/CDS services have undergone an information security assessment by an infosec-registered assessor.

[–,HP,C] Information security assessments of commercial providers

2.3.76. Agencies **must** ensure that any companies contracted to provide Internet gateway/CDS services have undergone an information security assessment by an infosec-registered assessor.

[U,IC-HP,R-TS] Information system architecture review

2.3.77. Prior to undertaking the information system architecture review the system owner **must** approve the information system architecture and associated information security documentation.

2.3.78. The information system architecture **should** be reviewed by the assessor to ensure that it is based on sound information security principles and meets information security requirements.

2.3.79. The ISP **should** be reviewed by the assessor to ensure that policies have been developed or identified by the agency to protect information that is processed, stored or communicated by its systems.

2.3.80. The SRMP **must** be reviewed by the assessor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.

2.3.81. The SSP **must** be reviewed by the assessor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.

2.3.82. The SSP **must** be reviewed by the assessor to ensure that all relevant controls specified in this manual are included and that any variations have had their applicable non-compliance processes followed.

2.3.83. The SSP **should** include an indication of which controls from this manual have been varied from or waived and an outcome of associated variation processes.

2.3.84. The SSP **should** include an indication of which controls from this manual were out of scope for the system.

2.3.85. The SOPs **should** be reviewed by the assessor to ensure that it includes:

a. ITSO and system administrator tasks
b. proactive security checking tasks, and
c. proactive security auditing tasks.

2.3.86. The IRP **should** be reviewed by the assessor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.

[U,IC-HP,R-TS] Information security certification

2.3.87. Prior to undertaking the information security certification the system owner **must** implement the SSP for the system.

2.3.88. The implementation of system controls, as outlined in the SSP, **must** be certified by the assessor to determine whether they have been implemented and are operating effectively.

2.3.89. The assessor **must** ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.

[U,IC-HP,R-TS] Residual security risk assessment

2.3.90. Following the information system architecture review and information security certification, an assessor **should** produce a report outlining the residual security risks relating to the operation of the system including a recommendation to the accreditation authority on whether to award accreditation or not.

GUIDANCE

[U,IC-HP,R-TS] Independent information security assessments

2.3.91. It is **recommended** that agencies ensure that the assessor of any stage of an information security assessment is not also the system owner.

[U,IC-HP,R-TS] Information system architecture review

2.3.92. It is **recommended** that the system owner provide a compliance supplement or annex to the SSP outlining its compliance with the controls within this manual.

2.3.93. It is **recommended** that the system owner include the following topics in the compliance supplement to the SSP:

a. the baseline of the manual used for determining controls
b. controls that are, and are not, applicable to the system
c. controls that are applicable but have been varied from, and
d. any additional controls implemented as a result of the SRMP.

[U,IC-HP,R-TS] Information security certification

2.3.94. It is **recommended** that the physical security certification be less than 5 years old at the time of the information security certification.

RATIONALE

Information system architecture review

2.3.95. The purpose of the information system architecture review is to determine that the information system architecture is based on sound information security principles and meets information security requirements. Design documents that can be used to assist in this review include, but are not limited to:

- logical/infrastructure diagrams
- concept of operations
- list of mandatory requirements
- critical configurations, and
- risk based requirements.

2.3.96. The review of information security documentation is conducted primarily to ensure the appropriateness of the documentation and the compliance of the SSP with this manual. However, systems are also documented to:

- provide an approved build standard
- provide a baseline for configuration control
- assist in providing an audit path, and
- assist with information security investigations.

2.3.97. The development of a compliance supplement to the SSP is recommended to provide the accreditation authority, and external agencies, with a high-level summary of the compliance of the system with this manual.

2.3.98. Identifying all cases of non-compliance with this manual will also ensure that when another agency is connecting their system they will be aware of the variations made from requirements in this manual. This allows the other agency to subsequently risk manage the connection of their system as part of their own accreditation processes.

Information security certification

2.3.99. The purpose of the information security certification is to determine whether the documented security controls within the SSP, as approved by the system owner and reviewed during the information system architecture review stage, have been implemented and are operating effectively. The outcome of this process is often a certificate confirming that the system was certified as being compliant with its SSP.

Residual security risk assessment

2.3.100. The purpose of the residual security risk assessment is to assess the residual security risk relating to the operation of an information system following the successful, or otherwise, certification of the system to its SSP. In situations were the system is not certified as confirming to its approved SSP the residual risk may not be great enough to preclude an assessor recommending that accreditation be awarded as it will depend on the particular area(s) were the system is non-conformant.

REFERENCES

2.3.101. *Policy and Procedures for the InfoSec-Registered Assessor Program* contains a definition of the range of activities infosec-registered assessors are authorised to perform. It can be obtained from DSD's website at http://www.dsd.gov.au/infosec/evaluation_services/irap.html.

Accreditation Decision

PRINCIPLE

2.3.102. Forming an accreditation decision involves reviewing and assessing the residual security risk to a system once security controls for the system have been implemented.

OBJECTIVE

2.3.103. To inform the accreditation authority of activities involved in formulating an accreditation decision.

CONTEXT

Scope

2.3.104. This section covers information on determining the outcome of the accreditation process.

Accreditation authority

2.3.105. For agencies, the accreditation authority is the agency head or their delegate, for which the CISO is strongly recommended.

2.3.106. For organisations supporting agencies, the accreditation authority is the head of the supported agency or their authorised delegate, for which the CISO is strongly recommended.

2.3.107. For multi-national and multi-agency systems, the accreditation authority is determined by a formal agreement between the parties involved.

2.3.108. For agencies with systems that process, store or communicate caveated or compartmented information there could be a mandated accreditation authority.

2.3.109. In all cases the accreditation authority will be at least a senior executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

2.3.110. Depending on the circumstances and practices of an agency, the agency head could choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions within the agency, for example the CISO and the business owner.

2.3.111. More information on the delegation of the agency head's authority can be found in the *Agency Head* section of the *Roles and Responsibilities* chapter of this manual.

Accreditation outcomes

2.3.112. Accreditation is awarded when the accreditation authority accepts the residual security risk relating to the operation of the system and gives formal approval for the system to operate; however, in some cases the accreditation authority may not accept the residual security risk relating to the operation of the system. This outcome is predominately due to security risks being insufficiently considered and documented within the SRMP resulting in an inaccurate scoping of security measures within the SSP. In such cases the accreditation authority may request that the SRMP and SSP be reassessed, amended and reissued followed by a delta information security assessment before another accreditation decision is made.

2.3.113. In awarding accreditation for a system the accreditation authority may choose to define a reduced timeframe before reaccreditation that is less than that specified in this manual or place restrictions on the use of the system which are enforced until reaccreditation or until changes are made to the system within a specified timeframe.

RISKS

2.3.114. The accreditation authority fails to appropriately consider the outcomes of an information security assessment resulting in the acceptance of residual security risk for a system without understand what security risk they are actually accepting.

CONTROLS

[U,IC-HP,R-TS] Accreditation decision

2.3.115. The accreditation authority **must** accept the residual security risk relating to the operation of a system in order to award accreditation.

GUIDANCE

[U,IC-HP,R-TS] Accreditation decision process

2.3.116. It is **recommended** the accreditation authority undertake the following activities when determining whether to accept the residual security risk relating to the operation of a system and award accreditation:

a. review the SRMP
b. review the information security assessment report recommendations
c. review any variations or waivers from controls specified in this manual, and
d. ensure that any additional security risk reduction strategies are appropriate and effective.

RATIONALE

Accreditation decision process

2.3.117. The accreditation authority may choose to seek the assistance of one or more technical experts in understanding the technical components of the information security assessment report and SRMP.

Maintaining Accreditation

PRINCIPLE

2.3.118. The assurance in the security of a system can be maintained through information security monitoring activities and regular reaccreditations of the system.

OBJECTIVE

2.3.119. To ensure that the security of accredited systems is continually monitored and reviewed to remain relevant given the evolving threat environment and that reaccreditation activities are undertake to ensure that changes to a system are accounted for and residual risks are reassessed and accepted on a regular basis.

CONTEXT

2.3.120. This section covers information on maintaining the accreditation of a system. Information on monitoring the information security posture between accreditations can be found in the *Information Security Monitoring* chapter of this manual.

RISKS

2.3.121. An agency awarded accreditation for a system fails to continually monitor their system, resulting in the system developing into a state no longer resembling the information security posture during the accreditation process.

CONTROLS

[U,IC-HP,R-TS] Monitoring systems

2.3.122. System owners **should** ensure information security monitoring activities are undertaken on accredited systems, as required, to assess the changes to its environment and operation and to determine the implications for the security risk profile of the system.

[U,IC-HP,R-TS] Reaccreditation

2.3.123. Agencies **should** use the latest baseline of this manual when reviewing and updating the SSP as part of the reaccreditation activities for their systems.

2.3.124. Agencies **should** ensure that the period between initial accreditation and reaccreditation, as well as subsequent reaccreditations of each of their systems, does not exceed two years.

2.3.125. Agencies that have not conducted reaccreditation for a system within a three year period **must** conduct a security risk assessment at the three year mark and every year thereafter until the system is reaccredited.

RATIONALE

Reaccreditation

2.3.126. Additional reasons for conducting reaccreditation activities could include:

- changes in the agency's information security policies
- detection of new or emerging threats to agency systems
- the discovery that controls aren't operating as effectively as planned, and
- a major information security incident.

Information Security Monitoring

Information Security Reviews

PRINCIPLE

2.4.1. Conducting regular reviews using information that is comprehensive, current and reliable can assist in proper system maintenance.

OBJECTIVE

2.4.2. To ensure that agencies are responding to the latest threat environment and that systems are configured in accordance with associated up to date information security documentation.

CONTEXT

Scope

2.4.3. This section covers information on conducting reviews of any agency's information security posture.

Information security reviews

2.4.4. An information security review:

- identifies any changes to the business requirements for the subject of the review
- identifies any changes to the security risks faced by the subject of the review
- assesses the effectiveness of the existing counter-measures, and
- reports on any changes necessary to maintain an effective security posture.

2.4.5. An information security review can be scoped to cover anything from a single system to an entire agency's systems.

RISKS

2.4.6. An agency fails to undertake regular information security reviews of its information security posture, resulting in the agency not appropriately addressing the current threat environment.

2.4.7. An agency fails to undertake regular information security reviews of its information security posture, resulting in inconsistencies between the current systems and documented systems.

2.4.8. An agency fails to implement measures identified during an information security review, negating the benefits, effort and resources spent on conducting the review.

CONTROLS

[U,IC-HP,R-TS] Conducting information security reviews

2.4.9. Agencies **should** undertake and document information security reviews of their systems.

[U,IC-HP,R-TS] Basis of review

2.4.10. Agencies **should** base information security reviews on information that is comprehensive, current and reliable.

GUIDANCE

[U,IC-HP,R-TS] How frequently to review

2.4.11. It is **recommended** that agencies review all aspects of information security at least annually.

[U,IC-HP,R-TS] Conducting information security reviews

2.4.12. It is **recommended** that agencies review the components detailed in the table below.

COMPONENT	REVIEW
Information security documentation	The ISP, SRMP, SSP, any SOPs and the IRP.
Operating environment	When an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment.
Procedures	After an information security incident or test exercise.
System security	Items that could affect the security of the system on a regular basis.
Variations and waivers	Prior to the identified expiry date.

[U,IC-HP,R-TS] Who can perform a review

2.4.13. It is **recommended** that agencies have information security reviews performed by personnel independent to the target of the review or by an independent third party such as an infosec-registered assessor.

[U,IC-HP,R-TS] Rigour of a review

2.4.14. It is **recommended** that agencies ensure that the rigour of an information security review is commensurate with the threat environment and if applicable the highest security classification of information that is involved.

RATIONALE

Conducting information security reviews

2.4.15. Conducting information security reviews of agency information security postures on an annual basis can assist with ensuring that agencies are responding to the latest threat environment and that systems are configured in accordance with associated information security documentation.

2.4.16. An agency may choose to undertaken an information security review:

- as a result of a specific information security incident
- due to a change to a system or its environment that significantly impacts on the agreed and implemented information security architecture and policy, or
- as part of a regular scheduled review.

2.4.17. Gathering recommended information prior to an information security review will assist in ensuring that the information security review can be undertaken to a degree that is commensurate with the threat environment and if applicable the highest security classification of information that is involved.

2.4.18. Depending on the scope and subject of the information security review, agencies may gather information on areas such as:

- agency priorities and business requirements
- threat data
- likelihood and consequence estimates
- effectiveness of existing counter-measures

Continued on next page

- other possible counter-measures, and
- best practices.

Vulnerability Analysis

PRINCIPLE

2.4.19. Emerging security vulnerabilities can be addressed by conducting vulnerability analysis activities and addressing security risks identified as a result of the analysis.

OBJECTIVE

2.4.20. To ensure that as new vulnerabilities are found on a daily basis and publicised in the public domain, agencies continually reassess the information security of their systems.

CONTEXT

Scope

2.4.21. This section covers information on conducting vulnerability assessments on systems.

Changes as a result of a vulnerability analysis

2.4.22. When an agency decides to implement changes to a system to address security risks resulting from a vulnerability analysis it will need to follow its change management processes, as for any other change.

RISKS

2.4.23. An attacker exploits an unknown vulnerability, resulting in the compromise of a system.

2.4.24. An attacker uses a known, publicised vulnerability to exploit a system, resulting in the compromise of information.

CONTROLS

[U,IC-HP,R-TS] Vulnerability analysis strategy

2.4.25. Agencies **should** implement a vulnerability analysis strategy by:

a. monitoring public domain information about new vulnerabilities in operating systems and application software
b. considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner
c. running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented, and
d. using security checklists for operating systems and common applications.

[U,IC-HP,R-TS] Resolving vulnerabilities

2.4.26. Agencies **should** analyse and treat any security risks to their systems identified during a vulnerability assessment.

GUIDANCE

[U,IC-HP,R-TS] When to perform vulnerability assessments

2.4.27. It is **recommended** that agencies perform vulnerability assessments on systems:

a. before the system is first used
b. after a significant change to the system, and
c. as specified by an ITSM or the system owner.

RATIONALE

Vulnerability analysis strategy

2.4.28. While agencies are encouraged to monitor public domain information for vulnerabilities that could affect their systems, they should not remain complacent if no specific vulnerabilities relating to deployed products are disclosed.

2.4.29. In some cases, vulnerabilities can be introduced as a result of poor information security practices or accidental activities within an agency. As such, even if no new public domain vulnerabilities in deployed products have been disclosed there is still value to be gained from regular vulnerability analysis activities.

2.4.30. Furthermore, monitoring vulnerabilities, conducting analysis and being aware of industry and product changes and advances, including ISM requirements, provides an awareness of other changes which may adversely impact the security risk profile of the system in operation.

Resolving vulnerabilities

2.4.31. Agencies may wish to consider that discovered vulnerabilities could be a result of their information security practices, accidental activities or malicious activities and not just as the result of a technical issue.

Change Management

PRINCIPLE

2.4.32. Urgent and routine changes to systems can be controlled with the development of appropriate change management plans.

OBJECTIVE

2.4.33. To ensure that agencies develop and adhere to change management processes so that changes affecting information security are not undertaken without due consideration and appropriate authorisation.

CONTEXT

Scope

2.4.34. This section covers information on identifying and managing routine and urgent changes to systems.

Identifying the need for change

2.4.35. The need for change can be identified in various ways, including:

- system users identifying problems or enhancements
- vendors notifying of upgrades to software or hardware
- vendors notifying of the end of life to software or hardware
- advances in technology in general
- implementing new systems that necessitate changes to existing systems
- identifying new tasks requiring updates or new systems
- organisational change
- business process change
- standards evolution
- government policy or Cabinet directives, and
- other incidents or continuous improvement activities.

Types of system change

2.4.36. A proposed change to a system could involve:

- an upgrade to hardware
- an upgrade to application software
- the addition of an extra workstation, or
- major changes to access controls.

2.4.37. A change can be a one-off or occur periodically.

RISKS

2.4.38. An agency fails to control changes to systems, resulting in changes breaking the information security posture of the system and support personnel having no indication or record of the change that caused the breakage.

CONTROLS

[U,IC-HP,R-S] Change management

2.4.39. Agencies **should** ensure that for routine and urgent changes:

a. the change management process as defined in the relevant information security documentation is followed
b. the proposed change is approved by the relevant authority
c. any proposed change that could impact the security of a system is submitted to the accreditation authority for approval, and
d. all associated information security documentation is updated to reflect the change.

[–,–,TS] Change management

2.4.40. Agencies **must** ensure that for routine and urgent changes:

a. the change management process as defined in the relevant information security documentation is followed
b. the proposed change is approved by the relevant authority
c. any proposed change that could impact the security of the system is submitted to the accreditation authority for approval, and
d. all associated information security documentation is updated to reflect the change.

[U,IC-HP,R-S] Change management process

2.4.41. An agency's change management process **should** define appropriate actions to be followed before and after urgent changes are implemented.

[–,–,TS] Change management process

2.4.42. An agency's change management process **must** define appropriate actions to be followed before and after urgent changes are implemented.

[U,IC-HP,R-TS] Changes impacting the security of a system

2.4.43. When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system the agency **must** reaccredit the system.

GUIDANCE

[U,IC-HP,R-TS] Change management process

2.4.44. It is **recommended** that agencies use the following change management process:

a. produce a written change request
b. submit the change request for approval
c. document the changes to be implemented
d. implement and test the approved changes
e. update the relevant information security documentation including the SRMP, SSP and any SOPs
f. notify and educate system users of the changes that have been implemented as close as possible to the time the change is applied, and
g. continually educate system users in regards to changes.

RATIONALE

Change management

2.4.45. As part of any change process it is important that all stakeholders are consulted prior to implementation of the change. In the case of changes that will affect the security of a system, the accreditation authority will need to be consulted and approval sought within the agency.

2.4.46. Change management processes are most likely to be bypassed or ignored when an urgent change needs to be made to a system. In these chases it is essential that the agency's change management process strongly enforces appropriate actions to be taken before and after an urgent change is implemented.

Business Continuity and Disaster Recovery

PRINCIPLE

2.4.47. Business continuity and disaster recovery planning can ensure that the effects of a disaster are minimised and that information can be restored in a timely manner.

OBJECTIVE

2.4.48. To ensure agencies undertake business continuity processes and plan strategies to recover from disasters.

CONTEXT

Scope

2.4.49. This section covers information on business continuity and disaster recovery relating specifically to systems.

RISKS

2.4.50. An agency fails to plan for disaster scenarios resulting in an extended period of time before information can be recovered, if at all, and systems can return to an operational state.

CONTROLS

[U,IC-HP,R-TS] Availability requirements

2.4.51. Agencies **must** determine availability requirements for their systems and implement appropriate measures to support these requirements.

[U,IC-HP,R-TS] Backup strategy

2.4.52. Agencies **should**:

a. backup all information identified as critical to their business
b. store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the requirements for the highest security classification of the information, and
c. test backup and restoration processes regularly to confirm their effectiveness.

GUIDANCE

[U,IC-HP,R-TS] Business continuity plan

2.4.53. It is **recommended** that agencies develop a business continuity plan.

[U,IC-HP,R-TS] Disaster recovery plan

2.4.54. It is **recommended** that agencies develop a disaster recovery plan.

REFERENCES

2.4.55. Additional information relating to business continuity is contained in:

- AS/NZS ISO/IEC 17799:2006, 14, *Business Continuity Management*, and
- HB 221:2004, *Business Continuity Management*.

Information Security Incidents

Detecting Information Security Incidents

PRINCIPLE

2.5.1. Information security incidents can be detected by developing, implementing and maintaining specialised tools and procedures.

OBJECTIVE

2.5.2. To ensure that agencies develop, implement and maintain tools and procedures to detect information security incidents.

CONTEXT

Scope

2.5.3. This section covers information relating to detecting information security incidents. Detecting physical and personnel security incidents are considered to be out of scope.

2.5.4. Additional information relating to detecting information security incidents, and topics covered in this section, can be found in the following sections of this manual:

- *Information Security Reviews*
- *Vulnerability Analysis*
- *Information Security Awareness and Training*
- *Event Logging and Auditing*, and
- *Intrusion Detection and Prevention.*

RISKS

2.5.5. An agency fails to implement appropriate or sufficient tools and procedures to detect information security incidents resulting in a network intrusion or breach going unnoticed.

2.5.6. An agency uses resources to favour prevention over detection of information security incidents, or vice versa, resulting in successful intrusions going unnoticed or an increased number of intrusions being detected but not prevented.

2.5.7. An agency constructs a honeypot or honeynet to assist in capturing intrusion attempts, resulting in legal action being taken against the agency for breach of privacy.

CONTROLS

[U,IC-HP,R-TS] Preventing and detecting information security incidents

2.5.8. Agencies **must** develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating:

a. counter-measures against malicious code
b. intrusion detection strategies
c. audit analysis
d. system integrity checking, and
e. vulnerability assessments.

2.5.9. Agencies **should** use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention versus detection of information security incidents.

RATIONALE

Preventing and detecting information security incidents

2.5.10. The processes identified for assisting in detecting information security incidents will assist in mitigating the most common vectors used to exploit systems.

2.5.11. Many potential information security incidents are noticed by personnel rather than software tools if personnel are well trained and aware of information security issues and indicators of possible information security incidents.

2.5.12. Automated tools are only as good as the level of analysis they perform. If tools are not configured to assess the areas of potential security risk then it will not be evident when a weakness emerges. Additionally, if the tools are not regularly updated to include knowledge of new vulnerabilities their effectiveness will be reduced.

2.5.13. Agencies may consider some of the tools described in the table below for detecting potential information security incidents.

TOOLS	DESCRIPTIONS
Network and host intrusion detection systems (IDSs)	Monitor and analyse network and host activity, usually relying on a list of known attack signatures to recognise potential information security incidents.
Anomaly detection systems	Monitor network and host activities that do not conform to normal system activity.
Intrusion prevention systems	Some IDSs are combined with functionality to repel detected attacks. Caution and assessment of the potential impact need to be exercised if this capability is to be used.
System integrity verification	Used to detect changes to critical system components such as files, directories or services. These changes may alert a system administrator to unauthorised changes that could signify an attack on the system and inadvertent system changes that render the system open to attack.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities.

Managing Information Security Incidents

PRINCIPLE

2.5.14. Information security incident management will assist agencies in responding appropriately to information security incidents, including applying appropriate remedies and future prevention measures.

OBJECTIVE

2.5.15. To ensure that agencies determine information to be documented prior to and after information security incidents, where and how it should be documented, and how to preserve its integrity.

CONTEXT

Scope

2.5.16. This section covers information relating primarily to managing information security incidents. The management of physical and personnel security incidents is considered to be out of scope unless it directly impacts on the protection of systems (e.g. the breaching of physical protection for a server room).

RISKS

2.5.17. An agency fails to document information security incident responsibilities and procedures for systems, resulting in information security incidents being inappropriately handled due to lack of proper documentation and training.

2.5.18. Personnel fail to report an information security incident, resulting in a data spill, malicious attack or some other information security breach going unnoticed and unreported by an ITSM.

2.5.19. An agency fails to record information security incidents, resulting in the frequency and method of information security incidents not being analysed to further improve the information security posture of the agency.

2.5.20. An agency has insufficient processes and procedures for handling data spills, resulting in information being compromised.

2.5.21. An agency conducting forensic investigations into an information security incident fails to ensure the integrity of the information, resulting in the information not being admissible in legal proceedings.

2.5.22. An agency has insufficient processes and procedures for handling malicious code infections, resulting in an infection continuing to spread throughout a system or reinfecting the system once initially removed.

CONTROLS

[U,IC-HP,R-TS] Information security incident management documentation

2.5.23. Agencies **must** detail information security incident responsibilities and procedures for each system in the relevant SSP, SOPs and IRP.

[U,IC-HP,R-TS] Reporting information security incidents

2.5.24. Agencies **must** direct personnel to report information security incidents to an ITSM and the ASA if physical or personnel aspects are involved as soon as possible after the information security incident is discovered, in accordance with agency procedures.

2.5.25. Agencies **should**:

a. encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services
b. establish and follow procedures for reporting software malfunctions
c. put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored, and
d. deal with the violation of agency information security policies and procedures by personnel through a formal disciplinary process.

[U,IC-HP,R-TS] Recording information security incidents

2.5.26. Agencies **should** ensure that all information security incidents are recorded in a register.

2.5.27. Agencies **should** include, at a minimum, the following information in their register:

a. the date the information security incident was discovered
b. the date the information security incident occurred
c. a description of the information security incident, including the people and locations involved
d. the action taken
e. to whom the information security incident was reported, and
f. the file reference.

[U,IC-HP,R-TS] Handling data spills

2.5.28. When a data spill occurs agencies **must** assume that the information has been compromised.

2.5.29. Agencies **must** include in standard procedures for all personnel with access to systems a requirement that they notify an ITSM of any data spillage and access to any data which they are not authorised to access.

2.5.30. Agencies **must** document procedures for dealing with data spills in their IRP.

2.5.31. Agencies **must** treat any data spill as an information security incident and follow the IRP to deal with it.

2.5.32. When a data spill occurs agencies **must** report the details of the data spill to the information owner.

[U,IC-HP,R-TS] Containing data spills

2.5.33. When non-national security information above X-IN-CONFIDENCE or national security information is introduced onto a system not accredited to handle the information, agencies **must not** delete the higher classified information until advice is sought from DSD.

2.5.34. When security classified information is introduced onto a system not accredited to handle the information, agencies **should not** copy, view, print or email the information.

2.5.35. When security classified information is introduced onto a system not accredited to handle the information, agencies **should** segregate the affected system from the network.

[U,IC-HP,R-TS] Allowing continued attacks

2.5.36. Agencies allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence **should** seek legal advice.

[U,IC-HP,R-TS] Integrity of evidence

2.5.37. Agencies **should**:

a. transfer a copy of raw audit trails onto media for secure archiving, as well as securing manual log records for retention, and
b. ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

GUIDANCE

[U,IC-HP,R-TS] Seeking assistance

2.5.38. It is **recommended** that agencies ensure that any requests for DSD assistance are made as soon as possible after the information security incident is detected and that no actions which could affect the integrity of the evidence are carried out prior to DSD's involvement.

[U,IC-HP,R-TS] Recording information security incidents

2.5.39. It is **recommended** that agencies use their register as a reference for future security risk assessments.

[U,IC-HP,R-TS] Handling malicious code infection

2.5.40. It is **recommended** that agencies follow the steps described below when malicious code is detected:

a. isolate the infected system
b. decide whether to request assistance from DSD, and if such assistance is requested and agreed to, delay any further action until advised by DSD to continue
c. scan all previously connected systems—and any media used within a set period leading up to the information security incident—for malicious code
d. isolate all infected systems and media to prevent reinfection
e. change all passwords and key material stored or potentially accessed from compromised systems
f. advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems
g. use current antivirus software to remove the infection from the systems or media, and
h. report the information security incident and perform any other activities specified in the IRP.

RATIONALE

Information security incident management documentation

2.5.41. Ensuring responsibilities and procedures for information security incidents are documented in relevant SSPs, SOPs and IRP will ensure that when an information security incident does occur, agency personnel can respond in an appropriate manner. In addition, ensuring that system users are aware of reporting procedures will assist in capturing any information security incidents that an ITSM, ITSO or system owner fail to notice.

Recording information security incidents

2.5.42. The purpose of recording information security incidents within a register is to highlight the nature and frequency of the information security incidents so that corrective action can be taken. This information can subsequently be used as an input into future security risk assessments of systems.

Handling data spills

2.5.43. Assuming that information is compromised as a result of an information security incident will allow an agency to apply procedures in response to a worst case scenario.

Containing data spills

2.5.44. The spillage of non-national security information above X-IN-CONFIDENCE or national security information onto a system not accredited to handle the information is considered a significant information security incident under the DSD Information Security Incident Reporting (ISIR) scheme.

2.5.45. The segregation of an affected system can be achieved by powering off the system, removing network connectivity to the device or applying access controls on the information associated with the data spill to prevent access. It should be noted that powering off the system could destroy information that would be useful for forensics activities at a later date.

Allowing continued attacks

2.5.46. Agencies allowing an attacker to continue an attack against a system to seek further information or evidence will need to establish with their legal advisor(s) whether the actions are breaching the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

Integrity of evidence

2.5.47. While gathering evidence it is important to maintain the integrity of the information. Even though in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

Handling malicious code infection

2.5.48. The guidance for handling malicious code infections is provided to assist in preventing the spread of the infection and to prevent reinfection. An important consideration includes considering the infection date of the machine, and the possibility that the record could be inaccurate, when determining the appropriate period.

2.5.49. A complete operating system reinstallation, or an extensive comparison of characterisation information, is the only reliable way to ensure that malicious code is eradicated.

REFERENCES

2.5.50. Further information relating to the management of ICT evidence is contained in HB 171:2003, *Guidelines for the Management of Information Technology Evidence*.

Reporting Information Security Incidents

PRINCIPLE

2.5.51. Reporting significant information security incidents to the DSD will ensure that appropriate and timely assistance can be provided and that DSD can maintain an accurate threat environment picture for government systems.

OBJECTIVE

2.5.52. To ensure that agencies use the ISIR scheme for the reporting of significant information security incidents and cryptographic keying material compromises.

CONTEXT

Scope

2.5.53. This section covers information relating specifically to the reporting of information security incidents. It does not cover the reporting of physical or personnel security incidents.

Information security incidents and outsourcing

2.5.54. The requirement to lodge an information security incident report still applies when an agency has outsourced some or all of its information security functionality.

Categories of information security incidents

2.5.55. The ISIR scheme defines two categories of information security incidents: red and yellow. Red information security incidents are considered to be significant whilst yellow information security incidents are considered to be non-significant.

RISKS

2.5.56. An agency experiences a significant information security incident however fails to report the incident to DSD, resulting in a reduction of DSD's capacity to assist the agency and in monitoring the threat environment for government systems.

2.5.57. An agency experiences an information security incident that results in the compromise of cryptographic keying material and fails to notify system users, resulting in system users continuing to rely on exploited information security mechanisms for the confidentiality and integrity of their information.

2.5.58. An agency experiences an information security incident that results in the compromise of high grade cryptographic keying material and fails to notify DSD, resulting in the potential for information security breaches of other HGCE across government.

CONTROLS

[U,IC-HP,R-TS] Reporting of significant information security incidents

2.5.59. Agencies, through an ITSM or their ASA, **must** report significant information security incidents to DSD.

[U,IC-HP,R-TS] Reporting of information security incidents

2.5.60. Agencies **should** formally report information security incidents using the ISIR scheme.

[U,IC-HP,R-TS] Outsourcing and information security incidents

2.5.61. Agencies that outsource the information security functionality for a system to a service provider **should** ensure that the service provider consults with the agency when a significant, or non-significant, information security incident occurs.

[U,IC-HP,R-TS] Cryptographic keying material

2.5.62. Agencies **must** notify all system users of any suspected loss or compromise of keying material.

[U,IC-HP,R-TS] High grade cryptographic keying material

2.5.63. Agencies are **required** to notify DSD of any suspected loss or compromise of keying material associated with HGCE in accordance with ACSI 107.

GUIDANCE

[U,IC-HP,R-TS] Reporting of non-significant information security incidents

2.5.64. It is **recommended** that agencies, through an ITSM or their ASA, report non-significant information security incidents to DSD.

RATIONALE

Reporting of information security incidents

2.5.65. Reporting information security incidents provides a means to assess the overall damage to a system and to take remedial action across government. Information security incident reports are the basis for identifying trends in information security incident occurrences and for developing new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents.

2.5.66. Reporting of information security incidents to DSD through the appropriate channels ensures that appropriate and timely assistance can be provided to the agency. In addition, it allows DSD to maintain an accurate threat environment picture for government systems.

Outsourcing and information security incidents

2.5.67. In the case of outsourcing of information security, the agency is still responsible for the reporting of all significant information security incidents. As such, the agency must ensure that the service provider informs them of all significant information security incidents to allow them to formally report these to DSD. In the case of non-significant information security incidents the agency is encouraged to ensure that the service provider consults with the agency and that they follow up the consultation by submitting the information security incident report to DSD.

Cryptographic keying material

2.5.68. Reporting any information security incident involving the loss or misuse of cryptographic keying material is particularly important. Systems users rely on the use of cryptographic keying material for the confidentiality and integrity of their secure communications.

High grade cryptographic keying material

2.5.69. ACSI 107 applies to all agencies including contractors. Its requirements cover all HGCE used to process information.

2.5.70. For information security incidents involving the suspected loss or compromise of HGCE keying material, DSD will investigate the possibility of compromise, and where possible, initiate action to reduce the impact of the compromise.

REFERENCES

2.5.71. Further details, including reporting requirements, are located on the DSD website at http://www.dsd.gov.au/infosec/assistance_services/incident.html.

2.5.72. Further information on the categories of information security incidents can be found in http://www.dsd.gov.au/_lib/pdf_doc/isir_categories.pdf.

2.5.73. Additional information relating to external reporting requirements is contained in the PSM, pt G, *Guidelines on Security Incidents and Investigations*.

Physical Security

Physical Security for Information Systems

Facilities

PRINCIPLE

3.1.1. The use of physical security controls as part of a defence-in-depth strategy ensures that systems and associated infrastructure can be adequately protected and the need-to-know principle enforced.

OBJECTIVE

3.1.2. To ensure that physical security requirements from the PSM are applied to systems and associated infrastructure.

CONTEXT

Scope

3.1.3. This section covers information on the physical security of facilities. Information on servers and network devices, network infrastructure and hardware products can be found in the following sections of this chapter.

Physical security requirements for storing information

3.1.4. Many of the physical security controls in this manual are derived from requirement 7.65 of Part E of the PSM. This requirement sets out the minimum standard of security container, secure room or lockable commercial cabinet needed for storing information as shown in the table below.

	SECURE AREA	PARTIALLY SECURE AREA	INTRUDER RESISTANT AREA
TS	B	A[1]/B[2]	-
S/HP	C	B	A
C/P	C	C	B
R/IC	Agency discretion	Lockable commercial cabinet	Lockable commercial cabinet

1 – This is the minimum class of security container or secure room when guards are used during non-operational hours.

2 – This is the minimum class of security container or secure room if either a Security Construction and Equipment Committee (SCEC) endorsed security alarm is installed to the ASIO standard, or a security alarm system approved for site specific application by ASIO, is in use during non-operational hours.

Physical security requirements for processing information

3.1.5. In addition to the physical security requirements for storing information, the requirements for processing information are specified under the definitions for Secure Area, Partially Secure Area and Intruder Resistant Area in the PSM. As can be seen from the table above, Secure Areas and Partially Secure Areas are capable of being certified to process up to TOP SECRET information while Intruder Resistant Areas are only capable of being certified to process up to SECRET information.

Secured and unsecured spaces

3.1.6. In the context of this manual a secured space may be a single room or a facility that has security measures in place for the processing of security classified information. These secured spaces can be constructed with assistance from two different ASIO technical notes. These are the Secure/Partial Secure Area technical note and the Intruder Resistant Area technical note. Areas that are not certified as meeting the requirements for a secured space are known as unsecured spaces.

Physical security certification authorities

3.1.7. The certification of an agency's physical security measures is undertaken by the ASA for areas processing up to SECRET information, by ASIO for areas processing up to TOP SECRET information and by DIO for TOP SECRET SCIFs.

Facilities located outside of Australia

3.1.8. Agencies operating sites in posts or missions located outside of Australia can contact DFAT to determine any additional requirements which may exist.

RISKS

3.1.9. An attacker exploits vulnerabilities in the physical security of a facility to gain access to information on a system being operated within the facility.

3.1.10. An attacker exploits vulnerabilities in the physical security of a facility to gain access to information on a deployable system being operated within the facility.

3.1.11. An attacker observes information from outside the perimeter of a secured space.

3.1.12. An attacker brings non-agency owned devices into a secured space to probe defences or to assist in exfiltrating information.

3.1.13. An attacker plants a technical eavesdropping device within an area to assist in overhearing discussions.

CONTROLS

[–,IC-HP,R-TS] Facility physical security

3.1.14. Agencies **must** ensure that any facility containing a system or its associated infrastructure, including deployable systems, meets the minimum physical security requirements for processing information as specified in the PSM.

[U,IC-HP,R-TS] Preventing observation by unauthorised people

3.1.15. Agencies **should** prevent unauthorised people from observing systems, in particular displays and keyboards.

[–,–,TS] Brining non-agency owned devices into secured spaces

3.1.16. Agencies **must not** permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the accreditation authority.

[–,–,TS] Technical surveillance counter-measure testing

3.1.17. Agencies **must** ensure that technical surveillance counter-measure tests are conducted as determined by the outcomes of a security risk assessment and as a part of the physical security certification.

GUIDANCE

[U,IC-HP,R-TS] Preventing observation by unauthorised people

3.1.18. It is **recommended** that agencies position screens and keyboards so that they cannot be seen by unauthorised people, or fix blinds or drapes to the inside of windows.

RATIONALE

Facility physical security

3.1.19. The application of defence-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of physical security. The first layer of security is the use of a secured facility, the second layer is the use of a secured server room (when appropriate) and the final layer is the use of security containers or lockable commercial cabinets. All layers are designed to limit access to those with the appropriate authorisation to access the system and infrastructure.

3.1.20. Deployable platforms need to meet physical security certification requirements as per any other system. Physical security certification authorities dealing with deployable platforms can have specific requirements that supersede the requirements of this manual and as such information security personnel should contact their appropriate physical security certification authority to seek guidance.

3.1.21. In the case of deployable platforms, physical security requirements may also include perimeter controls, building standards and manning levels.

Preventing observation by unauthorised people

3.1.22. Agency facilities without sufficient perimeter security are often exposed to the potential for observation through windows. Ensuring information on workstation screens is not visible will assist in reducing this security risk.

REFERENCES

3.1.23. High-level information relating to physical security is also contained in:

- the PSM, pt E, *Physical Security*, and
- ISO/IEC 27002:2005, 9, *Physical and Environmental Security*.

3.1.24. Part E of the PSM contains additional information and requirements for technical surveillance counter-measure testing.

3.1.25. Further information on endorsed blinds and drapes are available in the *Security Equipment Catalogue* produced by ASIO.

Servers and Network Devices

PRINCIPLE

3.1.26. The physical security for servers and network devices is provided through a combination of physical security of the facility in which they are located and that of the server room, communications room and/or security container in which they are housed.

OBJECTIVE

3.1.27. To ensure that servers and network devices are secured from unauthorised access through the use of layered physical security measures.

CONTEXT

Scope

3.1.28. This section covers the physical security of servers and network devices. Information relating to network infrastructure and hardware products can be found in other sections of this chapter.

Secured server rooms

3.1.29. Agencies may choose to construct a secured server room to provide an additional layer of physical security for servers. In doing so agencies may reduce the storage requirements, as specified in the PSM, for security classified information residing on servers. Agencies choosing not to use a server room, or building a server room that doesn't meet the physical security requirements of the PSM for a secured space, will still need to meet the storage requirements as set out in the PSM for their servers.

Secured communications rooms

3.1.30. The requirements for secured server rooms in this section can be equally applied to secured communications rooms. As such multiple layers of physical security can also be used to reduce the storage requirements, as specified in the PSM, for security classified information residing on network devices. Agencies choosing not to use a communications rooms, or building a communications room that doesn't meet the physical security requirements of the PSM for a secured space, will still need to meet the storage requirements as set out in the PSM for their network devices.

RISKS

3.1.31. An attacker exploits vulnerabilities in the physical security of a facility in order to gain access to information.

3.1.32. An attacker conducts unobserved malicious physical actions to a system to cause an information security incident.

3.1.33. Personnel cause, or fail to notice, an information security incident due to a lack of awareness of the controls and procedures associated with the system.

3.1.34. An attacker exploits vulnerabilities in the physical security of a server room or communications room in order to steal or damage servers and/or network devices to cause a denial of service.

CONTROLS

[U,–,–] Processing and storage requirements for servers

3.1.35. Agencies **should** secure servers in lockable commercial cabinets within locked server rooms.

[–,IC-HP,R-TS] Processing requirements for servers not in secured server rooms

3.1.36. Agencies not using secured server rooms **must** ensure that the area meets the minimum physical security requirements for processing information as specified in the PSM.

[–,IC-HP,R-TS] Storage requirements for servers not in secured server rooms

3.1.37. Agencies not using secured server rooms **must** ensure that servers are stored in security containers that meet the minimum physical security requirements for storing information as specified in the PSM.

[–,IC-HP,R-TS] Processing requirements for servers in secured server rooms

3.1.38. Agencies choosing to use a secured server room within a secured facility **must** ensure the server room, at minimum, meets the physical security requirements for processing information as specified in the PSM, based on the physical security certification of the surrounding facility, as shown in the table below.

FACILITY PHYSICAL SECURITY CERTIFICATION			
	SECURE AREA	PARTIALLY SECURE AREA	INTRUDER RESISTANT AREA
TS	Secure Area	Secure Area	-
S/HP	Intruder Resistant Area	Secure Area	Secure Area
C/P	Intruder Resistant Area	Secure Area	Secure Area
R/IC	Intruder Resistant Area	Intruder Resistant Area	Intruder Resistant Area

[–,IC-HP,R-S] Processing requirements for servers in secured server rooms

3.1.39. Agencies choosing to use a secured server room certified as an Intruder Resistant Area within a facility certified as a Secure Area **must** extend the type one alarm system coverage for the facility into the server room.

[–,IC-HP,R-TS] Storage requirements for servers in secured server rooms

3.1.40. Agencies choosing to use a secured server room within a secured facility **must**, at minimum, meet the physical security requirements for storing information as specified in the PSM, based on the physical security certification of the server room and its surrounding facility, as shown in the table below.

SERVER ROOM PHYSICAL SECURITY CERTIFICATION		
	SECURE AREA	INTRUDER RESISTANT AREA
TS	Class C cabinet	-
S/HP	Lockable commercial cabinet	Lockable commercial cabinet
C/P	Lockable commercial cabinet	Lockable commercial cabinet
R/IC	Lockable commercial cabinet	Lockable commercial cabinet

[U,IC-HP,R-TS] Securing server rooms and security containers containing servers

3.1.41. Agencies **must not** leave server rooms or security containers containing servers in an unsecured state.

[U,IC-HP,R-TS] Shared server rooms

3.1.42. Agencies sharing a common server room with other agencies **should** determine the need-to-know requirements for their information within such an environment and implement appropriate security measures to ensure its confidentiality.

[U,IC-HP,R-TS] No-lone-zones

3.1.43. Agencies operating no-lone-zones **must** suitably signpost the area and have all entry and exit points appropriately secured.

[U,IC-HP,R-TS] Administrative measures

3.1.44. Agencies **must** develop a site security plan for each server room. Information to be covered includes, but is not limited to:

a. a summary of the security risk review for the facility the server room is located within
b. roles and responsibilities of facility or information security personnel
c. the administration, operation and maintenance of the electronic access control system or security alarm system
d. key management, the enrolment and culling of system users and issuing of personal identification number codes
e. personnel security clearances, security awareness training and regular briefings
f. inspection of the generated audit trails and logs
g. end of day checks and lockup
h. reporting of information security incidents and breaches; and
i. what activities to undertake in response to security alarms.

[U,IC-HP,R-TS] Processing and storage requirements for network devices

3.1.45. Agencies **must** ensure that network devices meet the same physical security requirements as specified for servers.

GUIDANCE

[U,IC-HP,R-TS] Administrative measures

3.1.46. It is **recommended** that agencies contact their physical security certification authority for advice on the content of site security plans.

RATIONALE

Storage requirements for servers in secured server rooms

3.1.47. When an agency chooses to implement a security container for a server in an unsecured server room, or outside a secured server room, they need to be compliant with the requirements of the PSM. However, when an agency stores a server within a secured server room the storage requirements for servers are lowered due to the multiple layers of physical security protecting the server. As such, when a secured server room is used the requirements provided in this manual supersede requirement 7.65 of Part E of the PSM.

Securing server rooms and security containers containing servers

3.1.48. If personnel decide to leave server rooms and security containers with keys in locks, unlocked or with security functions disabled it negates the purpose of providing security in the first place. Such activities will compromise the security efforts of the agencies and should not be permitted by the agency.

Shared server rooms

3.1.49. The purpose of controlling access to an agency's own servers within a common server room is to enforce the need-to-know principle. One way of accomplishing this would be to restricted access to keys for security containers to only personnel that belong to the agency the server belongs to or by physically partitioning agency servers from servers belonging to other agencies.

No-lone-zones

3.1.50. Areas containing particularly sensitive materials or 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.

Administrative measures

3.1.51. Site security plans, the physical security equivalent of the SSP and SOPs for systems, are used to document all aspects of physical security for systems. Formally documenting this information ensures that standards, controls and procedures can easily be reviewed by agency information security personnel.

3.1.52. The development of the security risk review is a requirement outlined within Part E of the PSM and is the responsibility of the ASA. The PSM does not require a security risk review for UNCLASSIFIED environments and considers the requirement as discretionary for X-IN-CONFIDENCE and RESTRICTED environments. However, the ISM does require a security risk review for server rooms in these environments due to the higher security risk for servers and the ASA will need to undertake this activity.

Processing and storage requirements for network devices

3.1.53. Network devices are considered to store information when operational and as such need to meet the physical security requirements for storing information as specified in the PSM.

3.1.54. The storage requirements for network devices as specified in the PSM can be reduced if encryption is applied to information communicated over the network (i.e. data in transit encryption).

EXAMPLES

3.1.55. An agency operating a SECRET network within a facility certified as a Secure Area constructs a server room that is certified as an Intruder Resistant Area. Within the server room the agency can use lockable commercial cabinets for the storage of individual servers.

3.1.56. The same agency operating a SECRET network within their facility certified as a Secure Area constructs a communications rooms, on a different floor to the server room, which is certified as an Intruder Resistant Area. Within the communications room the agency can use a lockable commercial cabinet for the storage of switches.

3.1.57. A second agency operating a HIGHLY PROTECTED network within a facility certified as a Partially Secure Area is unable to construct a server room due to insufficient floor space. As such, the agency must use Class B cabinets for the storage of individual servers. However, if the agency had been able to construct a server room that was certified as a Secure Area, they could have used lockable commercial cabinets.

3.1.58. The same agency operating a PROTECTED network within a facility certified as a Partially Secure Area chooses not to construct a communications room within an operations centre. As such, the agency must use a Class C cabinet for the storage of network devices in the open floor space. However, if the agency had been able to construct a communications room that was certified as a Secure Area, they could have used a lockable commercial cabinet for their network devices.

Network Infrastructure

PRINCIPLE

3.1.59. When network infrastructure is located within a secured space security is provided by the physical security of the surrounding facility, however when located in an unsecured space encryption ensures that even if access to the infrastructure is gained the information is protected.

OBJECTIVE

3.1.60. To ensure that network infrastructure is protected in secured and unsecured spaces through the use of physical security and encryption measures.

CONTEXT

Scope

3.1.61. This section covers information relating to the physical security of network infrastructure. Information relating to servers, network devices and hardware products can be found in other sections of this chapter. Additionally, information on using encryption for infrastructure in unsecured spaces can be found in the *Cryptographic Fundamentals* section of this manual.

RISKS

3.1.62. An attacker gains access to network infrastructure and damages cabling to cause a denial of service.

3.1.63. An attacker gains access to network infrastructure and modifies cabling to assist in exfiltrating information.

3.1.64. An attacker gains access to network infrastructure and injects spurious information or alters existing information.

CONTROLS

[–,IC-HP,R-TS] Processing requirements for network infrastructure

3.1.65. Agencies **must** ensure that network infrastructure within facilities meets the minimum physical security requirements for processing information as specified in the PSM.

[U,IC-HP,R-S] Protecting network infrastructure

3.1.66. Agencies **should** locate patch panels, fibre distribution panels and structured wiring enclosures, at minimum, within locked communications rooms or locked commercial cabinets to prevent access by unauthorised personnel.

[–,–,TS] Protecting network infrastructure

3.1.67. Agencies **must** locate patch panels, fibre distribution panels and structured wiring enclosures, at minimum, within locked communications rooms or locked commercial cabinets to prevent access by unauthorised personnel.

3.1.68. ITSMs **must** ensure that the keys or equivalent access mechanisms to locked communications rooms or locked commercial cabinets containing patch panels, fibre distribution panels and structured wiring enclosures are appropriately controlled.

[–,IC-HP,R-TS] Network infrastructure in unsecured spaces

3.1.69. Agencies communicating security classified information over unsecured public network infrastructure or through unsecured spaces **must** use encryption to lower the storage and processing requirements to that for UNCLASSIFIED information.

GUIDANCE

[U,IC-HP,R-S] Protecting network infrastructure

3.1.70. It is **recommended** that ITSMs ensure that the keys or equivalent access mechanisms to locked communications rooms or locked commercial cabinets containing patch panels, fibre distribution panels and structured wiring enclosures are appropriately controlled.

RATIONALE

Processing requirements for network infrastructure

3.1.71. Network infrastructure is considered to only process information being communicated across it and as such needs to meet the minimum physical security requirements for processing information as specified in the PSM.

3.1.72. The processing requirements for network infrastructure can be lowered if encryption is being applied to information communicated over the infrastructure (i.e. data in transit encryption).

Protecting network infrastructure

3.1.73. In most cases patch panels, fibre distribution panels and structured wiring enclosures will be collocated with network devices and will be afforded greater security than specified in this section due to the requirements for the protection of the network devices.

EXAMPLES

3.1.74. To meet processing requirements for network infrastructure carrying unencrypted PROTECTED information, a secured space certified to protect up to PROTECTED information is needed. In most cases the facility housing the network infrastructure will provide the appropriate type of secured space.

3.1.75. In cases where the facility surrounding the network infrastructure does not provide appropriate protection for processing the security classification of information communicated over the infrastructure, encryption will need to be used to lower the requirements to at least that of the facility. For example, an agency requires HIGHLY PROTECTED information to be communicated over network infrastructure from a one secured space certified to process HIGHLY PROTECTED information, through a space that is certified to process PROTECTED information, to another secured space that is certified to process HIGHLY PROTECTED information. As such, the agency uses an appropriate cryptographic product to lower the processing requirements as specified in the PSM from HIGHLY PROTECTED to PROTECTED between the two HIGHLY PROTECTED areas.

3.1.76. To meet storage and processing requirements for network infrastructure carrying PROTECTED information through an unsecured space, encryption of an appropriate assurance level to reduce the requirements to that for UNCLASSIFIED information is needed.

Hardware Products

PRINCIPLE

3.1.77. Physically securing hardware products containing media can prevent theft or disclosure of information.

OBJECTIVE

3.1.78. To ensure that as hardware products containing media take on the security classification of information that they process or store, agencies appropriately protect them in accordance with the physical security requirements of the PSM.

CONTEXT

Scope

3.1.79. This section covers information relating to the physical security of hardware products containing media (excluding network devices). This includes but is not limited to workstations, printers, photocopiers, scanners and multifunction devices (MFDs).

3.1.80. Additional information relating to hardware products and media can be found in the following chapters and sections of this manual:

- *Fax Machines and Multifunction Devices*
- *Product Security*
- *Media Security*, and
- *Multifunction Devices.*

Handling hardware products containing media

3.1.81. During non-operational hours agencies need to store media containing information that resides within hardware products in accordance with the requirements of the PSM. Agencies can comply with this requirement by undertaking one of the following processes:

- ensuring hardware products always reside in an appropriate class of secure room
- storing hardware products during non-operational hours in an appropriate class of security container or lockable commercial cabinet
- using hardware products with removable non-volatile media which is stored during non-operational hours in an appropriate class of security container or lockable commercial cabinet as well as securing its volatile media
- using hardware products without non-volatile media as well as securing its volatile media
- using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media, or
- configuring hardware products to prevent the storage of information on the non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown as well as securing its volatile media.

3.1.82. The intent of using cryptography or preventing the storage of information on non-volatile media in addition to scrubbing temporary data at logoff or shutdown, as well as securing volatile media, is to enable agencies to treat the media within hardware products as per the storage requirements of a lower security classification, as specified in the PSM, during non-operational hours.

3.1.83. As the process of using cryptography and preventing the storage of information on non-volatile media in addition to scrubbing temporary data at logoff or shutdown, for all security classifications, and securing volatile media, for higher security classifications, does not constitute the sanitisation and reclassification of the media, the media retains it security classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal requirements as specified in this manual.

Hardware products using hybrid hard drives or solid state drives

3.1.84. The process of preventing the storage of information on non-volatile media when in use, and enforcing scrubbing of temporary data at logoff or shutdown, is not approved as a method of lowering the storage requirements, as specified in the PSM, when hybrid hard drives or solid state drives are used.

RISKS

3.1.85. An attacker steals a hardware product from a facility, which goes unnoticed, resulting in the disclosure of information and a lack of appropriate response to the incident.

3.1.86. An attacker exploits vulnerabilities in the physical security of a facility in order to gain access to information.

3.1.87. An attacker damages a hardware product causing a denial of service.

3.1.88. An attacker gains access to a hardware product and physically compromises its integrity.

3.1.89. An attacker is able to retrieve information from media as the agency was unaware that an emergency power outage, or system user intervention, had disrupted the processes used to scrub temporary data at logoff or shutdown.

CONTROLS

[–,IC-HP,R-S] Accounting for hardware products containing media

3.1.90. Agencies **should** account for all hardware products containing security classified media.

[–,–,TS] Accounting for hardware products containing media

3.1.91. Agencies **must** account for all hardware products containing security classified media.

[–,IC-HP,R-TS] Processing requirements

3.1.92. Agencies **must** ensure that the area within which hardware products with security classified media are used meets the minimum physical security requirements for processing information as specified in the PSM.

[–,IC-HP,R-TS] Storage requirements

3.1.93. Agencies **must** ensure that during non-operational hours hardware products with security classified media are secured in accordance with the minimum physical security requirements for storing information as specified in the PSM.

[–,IC-HP,R-TS] Securing non-volatile media for storage

3.1.94. Agencies choosing to prevent the storage of security classified information on non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown **should**:

a. assess the security risks associated with such a decision, and
b. specify the processes and conditions for their application within the system's SSP.

[–,IC-HP,R-TS] Securing volatile media for storage

3.1.95. Agencies securing volatile media for hardware products during non-operational hours **should**:

a. remove power from the hardware product the media resides within
b. assess the security risks if not sanitising the media, and
c. specify any additional processes and controls that will be applied within the system's SSP.

RATIONALE

Accounting for hardware products containing media

3.1.96. Ensuring that hardware products containing media are accounted for by using asset registers and regular audits will assist in preventing theft, or in the cases of theft, alerting appropriate authorities to its occurrence.

Processing requirements

3.1.97. As the media within hardware products takes on the security classification of the information it is processing, the area that it is used within needs to be certified a level that is suitable to process the information that is accessible from the product.

Storage requirements

3.1.98. The PSM states in paragraph 7.65 of Part E that either Class C, B or A secure rooms or Class C, B or A security containers or lockable commercial cabinets can be used to meet physical security requirements for the storage of hardware containing security classified media. The class of secure room or security container will depend on the physical security certification of the surrounding area and the security classification of the information.

3.1.99. If agencies need to conduct a security risk assessment as part of the procedure for storing hardware products containing security classified media during non-operation hours, they can consider security risks such as:

- an attacker gaining access to the hardware products immediately after power is removed and accessing the contents of volatile media to recover encryption keys or parts thereof
- extreme environmental conditions causing data to remain in volatile media for extended periods after the removal of power, and
- the physical security of the locations in which the hardware product will reside.

EXAMPLES

3.1.100. An agency has a TOP SECRET workstation. In accordance with the PSM they must have a Secure Area or Partially Secure Area certified to process TOP SECRET information. In addition, due to specific information processed by the agency, they construct a Class B secure room. Workstations within the secure room meet the requirements for storage in the PSM and no further actions are needed by the agency to store the workstations during non-operational periods.

3.1.101. An agency has a small form-factor PROTECTED MFD. In accordance with the PSM they must have a Secure Area, Partially Secure Area or Intruder Resistant Area certified to process PROTECTED information. The agency certifies their facility to a Partially Secure Area. Prior to the beginning of each non-operational period, personnel using the PROTECTED device secure it in a Class C security container.

3.1.102. An agency has a PROTECTED workstation using a diskless architecture. As the workstation contains no non-volatile media the only security classified media within the workstation at the end operational periods is the volatile media. As the agency wishes to treat the volatile media as UNCLASSIFIED they power off the workstation and considered the volatile media to be sanitised after 10 minutes has elapsed.

3.1.103. An agency has a SECRET workstation located in a Partially Secure Area. During non-operational periods, all items of non-volatile media are locked in a Class B security container in accordance with PSM requirements for storing information. In addition, since the workstation is shutdown the agency assesses the security risk of not sanitising the volatile media during non-operational hours and documents extra processes and controls to reduce the security risk in the SSP and SOPs for the system that the workstation belongs to.

3.1.104. An agency has a RESTRICTED workstation making use of an encryption product with a Common Criteria Evaluation Assurance Level (EAL) 2 and a completed DSD cryptographic evaluation (DCE). In accordance with the *Cryptographic Fundamentals* section of this manual, when the data is at rest the non-volatile media can be stored as per the requirements for UNCLASSIFIED information as specified in the PSM. As the agency wishes to also treat the volatile media within the workstation as UNCLASSIFIED they power off the workstation and considered the volatile media to be sanitised after 10 minutes has elapsed.

3.1.105. An agency has an X-IN-CONFIDENCE workstation. As the agency chooses not to use an encryption product or to use removable media, they configure the system to prevent information being stored on the non-volatile media when in use and enforce scrubbing of temporary data at logoff or shutdown. A security risk assessment is conducted on the processes being used in which it is determined that the residual security risks are within an acceptable level for the agency. As the agency wishes to also treat the volatile media within the workstation as UNCLASSIFIED when the system is powered off they power off the workstation and considered the volatile media to be sanitised after 10 minutes has elapsed.

Tamper Evident Seals

PRINCIPLE

3.1.106. Agencies can increase the chances of noticing tampering of assets by using uniquely numbered seals that are registered and regularly inspected for tampering.

OBJECTIVE

3.1.107. To provide information on what type of seals should be used, what information should be recorded for seals and how often they should be inspected to decrease the likelihood of tampering to assets going unnoticed.

CONTEXT

Scope

3.1.108. This section covers information on tamper evident seals that can be applied to assets.

RISKS

3.1.109. An attacker replaces a seal on an asset with another legitimate seal to hide evidence of tampering with the asset.

3.1.110. An attacker modifies an asset leaving tamper evident traces that are not observed by the users of the asset.

CONTROLS

[U,IC-HP,R-S] Recording seal usage

3.1.111. Agencies **should** record the usage of seals in a register that is appropriately secured.

3.1.112. Agencies **should** record in a register information on:

a. issue and usage details of seals and associated tools
b. serial numbers of all seals purchased, and
c. the location or asset on which each seal is used.

[–,–,TS] Recording seal usage

3.1.113. Agencies **must** record the usage of seals in a register that is appropriately secured.

3.1.114. Agencies **must** record in a register, information on:

a. issue and usage details of seals and associated tools
b. serial numbers of all seals purchased, and
c. the location or asset on which each seal is used.

[U,IC-HP,R-TS] Purchasing seals

3.1.115. Agencies **should** consult with the seal manufacturer to ensure that, if available, any purchased seals and sealing tools display a unique identifier or image appropriate to the agency.

3.1.116. Agencies **should not** allow contractors to independently purchase seals and associated tools on behalf of the Australian Government.

[U,IC-HP,R-TS] Reviewing seal usage

3.1.117. Agencies **should** review seals for differences with a register at least annually.

RATIONALE

Tamper evident seals

3.1.118. The use of seals is rarely mandated. However, agencies can choose to use seals as an additional risk reduction method, particularly if other controls defined in this manual cannot be met for a particular environment.

Recording seal usage

3.1.119. Recording information about seals in a register and on which asset they are used assists in reducing the security risk that seals could be replaced without agency information security personnel being aware of the change.

Purchasing seals

3.1.120. Using uniquely numbered seals ensures that a seal can be uniquely mapped to an asset. This assists agency information security personnel in reducing the security risk that seals could be replaced without anyone being aware of the change.

Reviewing seal usage

3.1.121. Users of assets with seals should be encouraged to randomly check the integrity of the seals and to report any concerns to agency information security personnel. In addition, conducting at least annual reviews will allow for detection of any tampering to an asset and ensure that the correct seal is located on the correct asset.

REFERENCES

3.1.122. The SCEC endorses seals to be used for various sealing requirements. Further information on endorsed seals is available in the *Security Equipment Catalogue* produced by ASIO.

EXAMPLES

3.1.123. Examples of when seals can be used include applying a wafer seal over universal serial bus (USB) ports or to hard disk cases to provide a tamper-evident barrier to discourage unauthorised access, or by attaching network connectors to computers using a roto-seal.

Personnel Security

Personnel Security for Information Systems

Information Security Awareness and Training

PRINCIPLE

4.1.1. Information security awareness and training are essential tools that can be fostered through the use of continual security education tailored to a system user's roles and responsibilities.

OBJECTIVE

4.1.2. To ensure that system users are information security trained and aware as it can be a relatively cheap and effective method of preventing, detecting and minimising the impact of information security incidents.

CONTEXT

Scope

4.1.3. This section covers information relating specifically to information security awareness and training. Other ICT awareness training is considered out of scope. Additional information on personnel security can be found in Part D of the PSM.

Information security awareness and training providers

4.1.4. Possible awareness and training providers and resources that can be used to fulfil the requirements of the section include:

- the Attorney-General's Department
- DSD-sponsored seminars for members of the Senior Executive Service
- formal in-house courses
- third-party vendor programs
- self-paced tuition manuals
- system user groups
- customised training programs, and
- external training organisations.

RISKS

4.1.5. Personnel through lack of training or awareness, conduct inappropriate actions on a system, resulting in an information security incident.

4.1.6. An attacker socially engineers personnel into unwittingly assisting to compromise a system.

4.1.7. Personnel through insufficient training, provide inappropriate or insufficient security to a system, resulting in an information security incident.

4.1.8. An attacker attending a training course with government personnel learns of vulnerabilities in a system, subsequently exploiting these vulnerabilities to gain access to the system.

4.1.9. Personnel, due to a lack of awareness of what constitutes appropriate information security within the agency, fail to detect information security incidents or system vulnerabilities.

CONTROLS

[U,IC-HP,R-TS] Information security awareness and training

4.1.10. Agencies **must** provide ongoing information security awareness and training for personnel on topics such as responsibilities, consequences of non-compliance with information security policies and procedures and potential security risks and counter-measures.

[U,IC-HP,R-TS] Information security awareness and training responsibility

4.1.11. Agency management **must** ensure that all personnel who have access to a system have sufficient information security awareness and training.

[U,IC-HP,R-TS] Degree and content of information security awareness and training

4.1.12. Agencies **should** align the exact degree and content of information security awareness and training to system user responsibilities.

4.1.13. Agencies training system users and system administrators **should** include information on:

a. how to recognise an anomaly that could indicate a possible information security incident, and
b. contacts in the event of a real or suspected information security incident.

4.1.14. Agencies **should** ensure that information security training and awareness includes advice to system users not to attempt to:

a. introduce code into any system
b. physically damage the system
c. bypass, strain or test information security mechanisms
d. introduce or use unauthorised software, firmware or hardware on a system
e. assume the roles and privileges of others
f. attempt to gain access to information for which they have no authorisation, or
g. relocate agency ICT equipment without proper authorisation.

[–,–,TS] System familiarisation training

4.1.15. Agencies **must** provide all system users with familiarisation training on the information security policies and procedures and the secure operation of the system before being granted unsupervised access to the system.

[U,IC-HP,R-TS] Disclosure of information while on courses

4.1.16. Agencies **should** advise personnel attending courses along with non-government personnel not to disclose any details that could be used to compromise agency security.

GUIDANCE

[U,IC-HP,R-TS] Degree and content of information security awareness and training

4.1.17. It is **recommended** that agencies ensure that information security training and awareness includes, at a minimum, information on:

a. the purpose of the training or awareness program
b. agency security appointments and contacts
c. the legitimate use of system accounts
d. access and control of media

Continued on next page

e. the security of accounts, including shared passwords
f. authorisation requirements for applications, databases and data
g. the destruction and sanitisation of media and hardcopy output; and
h. the security risks associated with accessing information from non-agency systems, particularly the Internet.

RATIONALE

Information security awareness and training

4.1.18. Information security awareness and training programs are designed to help system users:

- become familiar with their roles and responsibilities
- understand and support security requirements, and
- learn how to fulfil their security responsibilities.

Information security awareness and training responsibility

4.1.19. Agency management is responsible for ensuring that an appropriate information security awareness and training program is provided to personnel. Without management support, agency information security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

4.1.20. Agency personnel will naturally loose awareness or forget training over time. Providing ongoing information security training and awareness will assist in keeping personnel aware of issues and cognisant of their responsibilities.

4.1.21. Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins or memoranda.

Degree and content of information security awareness and training

4.1.22. The exact degree and content of information security awareness and training will depend on the objectives of the organisation. Personnel with responsibilities beyond that of a general user should have tailored training to meet their needs.

4.1.23. As part of the guidance provided to system users, there should be sufficient emphasis placed on the activities that are not allowed on systems. The minimum list of content will also ensure that personnel are sufficiently exposed to issues that if they are ignorant of could cause an information security incident.

System familiarisation training

4.1.24. A TOP SECRET system needs increased awareness by personnel. Ensuring familiarisation with information security policies and procedures, the secure operation of the system and basic information security training, will provide them with specific knowledge relating to these types of systems.

Disclosure of information while on courses

4.1.25. Government personnel attending courses with non-government personnel may not be aware of the consequences of disclosing information relating to the security of their agency's systems. Raising awareness of such consequences in personnel should prevent any disclosure that could lead to a targeted attack being launched against an agency's systems.

Security Clearances and Briefings

PRINCIPLE

4.1.26. Only appropriately cleared and briefed personnel should be authorised to access systems.

OBJECTIVE

4.1.27. To ensure that personnel accessing systems have appropriate security clearances and briefings.

CONTEXT

Scope

4.1.28. This section covers information relating to the security clearances and briefings required by personnel to access systems. Information on the technical implementation of access controls for systems can be found in the *Authorisation and System Access* section of this manual.

Security clearance – Australian and foreign

4.1.29. Where this manual refers to security clearances, the reference applies to Australian security clearances or security clearances from a foreign country which is recognised by Australia under a bi-lateral security instrument.

RISKS

4.1.30. Personnel are granted inappropriate access to a system where they are exposed to information they are not cleared, nor briefed, to access.

4.1.31. Foreign nationals, including seconded foreign nationals, gain access to AUSTEO information resulting in the disclosure of sensitive information.

4.1.32. Foreign nationals, excluding seconded foreign nationals, gain access to AGAO information resulting in the disclosure of sensitive information.

4.1.33. Foreign nationals, including seconded foreign nationals, gain access to information that has nationality releasability markings for which their nation is not included in the list of authorised recipients resulting in the disclosure of sensitive information.

CONTROLS

[U,IC-HP,R-TS] Documenting security clearance and briefing requirements

4.1.34. Agencies **must** specify in the SSP any access requirements, security clearances and briefings necessary for system access.

[U,IC-HP,R-TS] System access briefings

4.1.35. All system users **must** have received any necessary briefings before being granted access to a system.

[–,IC,R] System access

4.1.36. All system users who have not undergone pre-employment security checks **must** undergo a police check to determine their suitability to access security classified information before being granted access to a system.

[–,P-HP,C-TS] System access

4.1.37. All system users **must**:

a. hold a security clearance at least equal to the system security classification
b. hold a security clearance at least equal to the level they are accessing on a multi-level system, or
c. have been granted access in accordance with the requirements in this manual for limited higher access or emergency access.

[U,IC-HP,R-TS] System high mode

4.1.38. All system users accessing a system operating in system high mode **must** have a need-to-know for some of the information processed by the system.

[U,IC-HP,R-TS] Dedicated mode

4.1.39. All system users accessing a system operating in a dedicated mode **must** have a need-to-know all of the information processed by the system.

[U,IC-HP,R-TS] Compartmented mode

4.1.40. All system users accessing a system operating in compartmented mode **must** be formally authorised to access required compartments of information processed by the system.

[U,IC-HP,R-TS] Multi-level mode

4.1.41. All system users accessing a system operating in multi-level mode **must** have a need-to-know for some of the information within that level.

[–,IC-HP,R-TS] Access by foreign nationals to AUSTEO systems

4.1.42. Where systems process, store or communicate unprotected AUSTEO information, agencies **must not** allow foreign nationals, including seconded foreign nationals, to have access to the system.

4.1.43. Where agencies protect AUSTEO information on a system by implementing controls to ensure that AUSTEO information is not passed to, or made accessible to, foreign nationals, agencies **should not** allow foreign nationals, including seconded foreign nationals, to have access to the system.

[–,IC-HP,R-TS] Access by foreign nationals to AGAO systems

4.1.44. Where systems process, store or communicate unprotected AGAO information, agencies **must not** allow foreign nationals, excluding seconded foreign nationals, to have access to the system.

4.1.45. Where agencies protect AGAO information on a system by implementing controls to ensure that AGAO information is not passed to, or made accessible to, foreign nationals, agencies **should not** allow foreign nationals, excluding seconded foreign nationals, to have access to the system.

[–,IC-HP,R-TS] Access by foreign nationals to Australian systems

4.1.46. Where systems process, store or communication information with nationality releasability markings, agencies **must not** allow foreign nationals, including seconded foreign nationals, to have access to information that is not marked as releasable to their nation.

[–,P-HP,C-TS] Granting limited higher access

4.1.47. Agencies granting limited higher access to a system **must** ensure that:

a. the requirement to grant limited higher access is temporary in nature and is an exception rather than the norm
b. an ITSM has approved the limited higher access

Continued on next page

c. a cessation date for limited higher access has been set
d. the access period does not exceed two months
e. the limited higher access is granted on a non-ongoing basis
f. the system user only accesses security classified information at one security clearance level higher than currently held
g. the system user is not granted privileged access to the system
h. the system user's access is formally documented, and
i. the system user's access is reported to the ASA or their delegate.

[–,P-HP,C-TS] Controlling limited higher access

4.1.48. Agencies granting limited higher access to a system **must** ensure that:

a. effective information security controls are in place to restrict access to only security classified information that is necessary to undertake the system user's duties, or
b. the system user is continually supervised by another system user who has the appropriate security clearances to access the system.

[–,P-HP,C-TS] Granting emergency access

4.1.49. Agencies granting emergency access to a system **must** ensure that:

a. the requirements to grant emergency access is due to an immediate and critical need to access security classified information
b. the agency head or their delegate has approved the emergency access
c. the system user's access is formally documented
d. the system user's access is reported to an ITSM and the ASA or their delegate
e. if national security systems are accessed the security clearance process is completed as soon as possible, and
f. if non-national security systems are accessed, or likely to be accessed, for a period greater than two months the security clearance process is completed as soon as possible.

[–,P-HP,C-TS] Accessing systems without necessary security clearances and briefings

4.1.50. Agencies **must not** grant limited higher access or emergency access to systems that process, store or communicate caveated or compartmented information.

RATIONALE

Documenting security clearance and briefing requirements

4.1.51. Ensuring that the requirements for access to a system are documented and agreed upon will assist in determining if system users have appropriate clearances and need-to-know to access the system.

4.1.52. Types of system users for which access requirements will need to be documented include general users, privileged users, contractors and visitors.

REFERENCES

4.1.53. PSM Part D, *Personnel Security*, contains policy on granting and maintaining security clearances.

Escorting Uncleared Personnel

PRINCIPLE

4.1.54. Security classified information can be protected from uncleared personnel by appropriate escorting practices within an agency.

OBJECTIVE

4.1.55. To ensure that personnel do not gain access to secured spaces and that they do not have pre-requisite security clearances and a need-to-know to access.

CONTEXT

Scope

4.1.56. This section covers information relating to the escorting of uncleared personnel without security clearances in secured spaces.

RISKS

4.1.57. An attacker gains unescorted access to an area and accesses information they are not cleared or briefed to access.

CONTROLS

[–,–,TS] Unescorted access

4.1.58. Agencies **must** ensure that all personnel with unescorted access to TOP SECRET areas are cleared to TOP SECRET with appropriate briefings.

[–,–,TS] Unescorted access list

4.1.59. Agencies **must** maintain an up to date list of people entitled to enter a TOP SECRET area without escort.

4.1.60. Agencies **should** display within a TOP SECRET area an up to date list of people entitled to enter the area without escort.

[–,–,TS] Visitor log

4.1.61. Agencies **must not** permit people not on the unescorted access list to enter a TOP SECRET area unless their visit is recorded in a visitor log, and they are escorted by a person on the unescorted access list.

4.1.62. Agencies **must**, at a minimum, record the following information in a visitor log for each entry:

a. name
b. organisation
c. person visiting
d. contact details for person visiting, and
e. date and time in and out.

4.1.63. Agencies with a TOP SECRET area within a larger facility **must** maintain a separate log from any general visitor log.

RATIONALE

Unescorted access

4.1.64. Ensuring that personnel have correct security clearances to access sensitive areas and that access by escorted personnel is recorded for auditing purposes is widely considered a standard security practice.

Using the Internet

PRINCIPLE

4.1.65. Information can be prevented from being accidentally released into the public domain or systems being infected with malicious code if personnel are aware of their responsibilities when using the Internet.

OBJECTIVE

4.1.66. To ensure that personnel are aware of their responsibilities when using the Internet.

CONTEXT

Scope

4.1.67. This section covers information relating to personnel using Internet services such as the Web, Web-based email and peer-to-peer applications. Whilst this section does not address Internet services such as instant messaging, Internet Relay Chat (IRC), Internet Protocol telephony (IPT) and video conferencing, agencies need to remain aware that unless applications using these communications methods are evaluated and approved by DSD they are not approved for communicating security classified information over the Internet.

4.1.68. Additional information on using applications that can be used with the Internet can be found in the *Web Applications* and *Email Applications* sections of this manual.

Exceptions for posting information on the Web

4.1.69. Some government websites are secured to facilitate multi-agency collaborative work and discussions (e.g. OnSecure). Such websites are accredited to process and store information up to a stated security classification. When personnel post information to such sites the information does not need to go through a formal release process.

RISKS

4.1.70. Personnel using applications such as email, instant messaging, IRC and IPT are contacted by unknown people who enquire about work duties, project details or government policies. The personnel willing to assist their clients disclose information in an unauthorised manner.

4.1.71. Personnel post information on websites, especially blogs and forums, resulting in the unauthorised disclosure of the information.

4.1.72. Personnel post personal information on websites resulting in adversaries being able to profile personnel and develop targeted attacks using social engineering.

4.1.73. Personnel use public Web-based email services bypassing the security controls put in the place by the agency allowing malicious code to infect their agency's systems.

4.1.74. Personnel use peer-to-peer file sharing services resulting in information not authorised for public release being shared to the public or disclosed to adversaries from their agency's systems.

4.1.75. Personnel use peer-to-peer file sharing services and accidentally download and execute malicious software which infects their agency's systems.

4.1.76. Personnel using the Internet download and execute malicious software which infects their agency's systems.

4.1.77. Personnel access components of popular social networking websites that an attacker has infected with malicious code resulting in the compromise of their agency's systems.

CONTROLS

[U,IC-HP,R-TS] Using the Internet

4.1.78. Agencies **must** ensure personnel are instructed to report any suspicious contact when using the Internet to an ITSM.

[U,IC-HP,R-TS] Awareness of Web usage policies

4.1.79. Agencies **must** make their system users aware of the agency's Web usage policies.

[U,IC-HP,R-TS] Monitoring Web usage

4.1.80. Agencies **should** implement measures to monitor their personnel's compliance with their Web usage policies.

[U,IC-HP,R-TS] Posting information on the Web

4.1.81. Agencies **must** ensure personnel are instructed not to post information on the Web unless it has been authorised for release into the public domain.

[U,IC-HP,R-TS] Posting personal information on the Web

4.1.82. Agencies **should** ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.

[U,IC-HP,R-TS] Awareness of email usage policies

4.1.83. Agencies **must** make their system users aware of the agency's email usage policies.

[U,IC-HP,R-TS] Monitoring email usage

4.1.84. Agencies **should** implement measures to monitor their personnel's compliance with email usage policies.

[U,IC-HP,R-TS] Public Web-based email services

4.1.85. Agencies **should not** allow personnel to send and receive emails using public Web-based email services.

[U,IC-HP,R-TS] Peer-to-peer applications

4.1.86. Agencies **should not** allow personnel to use peer-to-peer applications over the Internet.

[U,IC-HP,R-TS] Receiving files via the Internet

4.1.87. Agencies **should not** allow personnel to receive files via peer-to-peer, instant messaging or IRC applications.

GUIDANCE

[U,IC-HP,R-TS] Posting personal information on the Web

4.1.88. It is **recommended** that personnel undertake a Web search of themselves to determine what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.

4.1.89. It is **recommended** that personnel restrict the amount of personal information they post on the Web, including:

a. past and present employment details
b. personal details/family structure

Continued on next page

c. schools/institutions
d. clubs/hobbies
e. educational qualifications
f. current work duties, and
g. work contact details.

[U,IC-HP,R-TS] Accessing social networking websites

4.1.90. It is **recommended** that agencies prevent personnel from accessing social networking websites that pose a higher than normal security risk relating to the unauthorised release of government information or disclosure of personal information.

RATIONALE

Using the Internet

4.1.91. Agencies will need to determine what constitutes suspicious contact in relation to their own work environment. Suspicious contact may relate to the work duties of personnel or the specifics of projects being undertaken by personnel within the agency.

Monitoring Web usage

4.1.92. Agencies may choose to monitor compliance with aspects of Web usage policies such as access attempts to blocked websites, such as pornographic and gambling websites, as well as compiling a list of system users that excessively download and/or upload data without a legitimate business requirement.

Posting information on the Web

4.1.93. Personnel posting information on the Web, especially in forums and blogs, need to remain cognisant of whether the information has been authorised for release into the public domain. Information that appears to be benign in isolation could, in aggregate, along with other information, have a considerable security impact on the Australian Government.

Posting personal information on the Web

4.1.94. Personnel need to be aware that any personal information they post on websites could be used to develop a detailed profile of their lifestyle and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit government information from them or implant malicious software on systems by inducing them to, for instance, open emails or visit websites with malicious content.

Monitoring email usage

4.1.95. Agencies may choose to monitor compliance with aspects of email usage policies such as attempts to send prohibited file types or executables, attempts to send excessive sized attachments or attempts to send security classified information without appropriate protective markings.

Public Web-based email services

4.1.96. Using public Web-based email services allows personnel to bypass security measures that agencies will have put in place to protect against malicious code or phishing attempts distributed via email.

Peer-to-peer applications

4.1.97. Personnel using peer-to-peer file sharing applications are often unaware of the extent of files that are being shared from their workstation. In most cases peer-to-peer file sharing applications will scan workstations for common file types and share them automatically for public consumption. Examples of peer-to-peer file sharing applications include Shareaza, KaZaA, Limewire, eMule and µTorrent.

4.1.98. Some peer-to-peer IPT applications, such as Skype, use proprietary protocols and make heavy use of encrypted tunnels to bypass firewalls. Because of this their use can not be regulated or monitored by agencies. It is important that agencies implementing an IPT solution over the Internet choose applications that use protocols that are open to inspection by gateway/CDS and intrusions detection solutions.

Receiving files via the Internet

4.1.99. When personnel receive files via peer-to-peer, instant messaging or IRC applications they are often bypassing security mechanisms put in place by the agency to detect and quarantine malicious code. Personnel should be encouraged to send files via established methods such as email to ensure they are appropriately scanned for malicious code.

Accessing social networking websites

4.1.100. Websites that may pose a higher than normal security risk relating to the unauthorised release of government information or disclosure of personal information can include, but are not limited to, websites such as Facebook, Myspace and Twitter.

Communications Security

Communications System Infrastructure

Cabling

PRINCIPLE

5.1.1. Secure cabling is implemented through the use of inspection, configuration and installation security enforcing procedures.

OBJECTIVE

5.1.2. To ensure that agencies install cabling in an appropriate manner to minimise potential emanation security and physical security weaknesses.

CONTEXT

Scope

5.1.3. This section covers information relating specifically to the inspection, configuration and installation of cabling associated with network infrastructure for Australian systems.

RISKS

5.1.4. An agency's poor cable installation practices allow unauthorised access, resulting in a compromise of information.

5.1.5. An agency's poor installation practices result in electromagnetic emanations being detected by an attacker beyond a secure perimeter resulting in a compromise of a system and the information it processes.

5.1.6. An agency allows the installation of a foreign system into an Australian facility using cable colours that if used for an Australian system would indicate a lower security classification than that of the system resulting in the agency inappropriately protecting the foreign system.

5.1.7. An agency allows the installation of a foreign system into an Australian facility using cable colours for an equivalent Australian system that processes AUSTEO or AGAO information resulting in the agency providing inadequate protection for the Australian system.

CONTROLS

[U,IC-HP,R-TS] Cabling standards

5.1.8. Agencies **must** install all cabling in accordance with the relevant Australian standards as directed by the Australian Communications and Media Authority.

[–,–,TS] Use of fibre optic cabling

5.1.9. Agencies **must** use fibre optic cabling for TOP SECRET systems.

5.1.10. When agencies cannot use fibre optic cabling for TOP SECRET systems they **must** seek advice from DSD.

[–,–,TS] Cabling inspectability

5.1.11. TOP SECRET cabling **must** be fully inspectable for its entire length.

5.1.12. The three-dimensional space around TOP SECRET cabling **must** be fully inspectable to confirm compliance with ACSI 61(C) cable separation requirements.

[U,IC-HP,R-S] Cable colours for foreign systems in Australian facilities

5.1.13. Agencies **should not** allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

5.1.14. The cable colour to be used for foreign systems **should** be agreed between the host agency, the foreign system owner and the accreditation authority.

[–,–,TS] Cable colours for foreign systems in Australian facilities

5.1.15. Agencies **must not** allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

5.1.16. The cable colour to be used for foreign systems **must** be agreed between the host agency, the foreign system owner and the accreditation authority.

[–,–,TS] Cable colours

5.1.17. Agencies **must** comply with the cable colours specified in the following table for TOP SECRET areas.

SECURITY CLASSIFICATION	CABLE COLOUR
TOP SECRET	Red
SECRET	Pink
CONFIDENTIAL	Green
RESTRICTED	Blue
HIGHLY PROTECTED	Blue
PROTECTED	Blue
X-IN-CONFIDENCE	Blue
UNCLASSIFIED	Black or grey

[U,IC-HP,R-S] Cabling diagrams

5.1.18. Agencies **should** develop a site/floor cabling diagram or equivalent document.

5.1.19. The site/floor cabling diagram **should**:

a. be updated on a regular basis as cabling/conduit configuration changes are made and approved, and
b. contain a 'current as at [date]' statement on each page to indicate the status of the document.

[–,–,TS] Cabling diagrams

5.1.20. Agencies **must** develop a site/floor cabling diagram or equivalent document.

5.1.21. The site/floor cabling diagram **should**:

a. be updated on a regular basis as cabling/conduit configuration changes are made and approved
b. contain a 'current as at [date]' statement on each page to indicate the status of the document
c. show the physical location of all TOP SECRET cable runs, associated wall outlets, and equipment located within the site, and
d. show the cable runs and equipment of security classifications other than TOP SECRET where the separation distances do not meet ACSI 61(C) requirements.

GUIDANCE

[U,IC-HP,R-S] Cable colours

5.1.22. It is **recommended** that agencies comply with the cable colours specified in the following table.

SECURITY CLASSIFICATION	CABLE COLOUR
SECRET	Pink
CONFIDENTIAL	Green
RESTRICTED	Blue
HIGHLY PROTECTED	Blue
PROTECTED	Blue
X-IN-CONFIDENCE	Blue
UNCLASSIFIED	Black or grey

RATIONALE

Cabling standards

5.1.23. Unauthorised personnel could inadvertently or deliberately access system cabling. This could result in loss or compromise of information. Covert tampering or access to system cabling may not be readily detected, resulting in long term unauthorised access to the information by a hostile entity.

Use of fibre optic cabling

5.1.24. An attacker could intercept electromagnetic signals from the security classified network that have radiated or been conducted beyond the secured space. This results in compromise of the information. Fibre optic cabling does not produce and is not influenced by electromagnetic emanations. It offers the highest degree of protection from electromagnetic emanation effects.

Cabling inspectability

5.1.25. Regular inspections of cabling are essential to ensure that the cabling has not been damaged, tampered with or suffered deterioration. Accordingly, both the cable and the surrounding three-dimensional space must be inspectable.

REFERENCES

5.1.26. Australian Standards for cabling can be obtained from the Australian Communications and Media Authority at http://www.acma.gov.au/WEB/STANDARD/pc=PC_2459.

5.1.27. ACSI 61(C), *Guidelines for the Installation of Communication and Information Processing Equipment and Systems* can be consulted for additional information.

EXAMPLES

5.1.28. An agency allowing the installation of a foreign system into an Australian facility requests that the cabling for the foreign system be coloured white so that it can be easily differentiated from cabling for Australian systems.

Cable Distribution Systems

PRINCIPLE

5.1.29. Approved combinations of cables can be run together in common conduits when installed in a controlled and inspectable manner.

OBJECTIVE

5.1.30. To ensure that only appropriate cabling shares a common conduit to assist in reducing emanation security risks.

CONTEXT

Scope

5.1.31. This section covers information relating to cable distribution systems used in secured spaces.

TOP SECRET cabling

5.1.32. For TOP SECRET cabling the cable's protective sheath is not considered to be a conduit

RISKS

5.1.33. An attacker sufficiently damages cabling via tampering or sabotage to disable the interconnection of equipment or distribution of information.

5.1.34. An attacker connects additional equipment to mount an attack against the system such that the system becomes ineffective, disabled or unusable.

5.1.35. Poor cabling installation causes emanations security issues between systems.

5.1.36. Personnel inappropriately access cabling systems such that information is collected and released outside of secured channels or for malicious purposes.

5.1.37. An attacker tampers with cabling systems such that access is gained to information which is subsequently amended to change the content/intent of that information.

CONTROLS

[U,IC-HP,R-S] Cables sharing a common conduit

5.1.38. Agencies **must not** deviate from the approved combinations for cable security classifications sharing a common conduit as indicated below.

GROUP	APPROVED COMBINATION
1	Any combination of: • UNCLASSIFIED • X-IN-CONFIDENCE • RESTRICTED • PROTECTED • HIGHLY PROTECTED
2	• CONFIDENTIAL • SECRET

[–,–,TS] Cables sharing a common conduit

5.1.39. Agencies **must not** run TOP SECRET cables along with cables of other security classifications in a common conduit.

[U,IC-HP,R-TS] Fibre optic cables sharing a common conduit

5.1.40. With optical fibre cables, the cable's protective sheath can be considered to be a conduit and therefore the fibres within the sheath **must** only carry a single group.

5.1.41. If a cable contains subunits, as shown below, then each subunit **must** only carry a single group, however each subunit within the cable can carry a different group.

[–,–,TS] Type of conduit

5.1.42. Conduits and the front covers of associated fittings that contain TOP SECRET cabling **must** be clear plastic.

[–,–,TS] Suspended conduit

5.1.43. To satisfy TOP SECRET cable separation and inspection requirements conduit runs **should** be suspended a minimum distance of 50mm from the ceiling to ensure that separation is maintained from unknown cables within the ceiling cavity.

5.1.44. If fibre optic cabling is the sole cabling within the conduit agencies **should** consider the impact of copper cabling being installed at a later date.

[–,–,TS] Sealing conduits

5.1.45. Agencies **must** use a visible smear of conduit glue to seal:

a. all clear plastic conduit joints, and
b. conduit runs connected by threaded lock nuts.

5.1.46. Agencies **must** use SCEC endorsed tamper evident seals to seal all removable covers on:

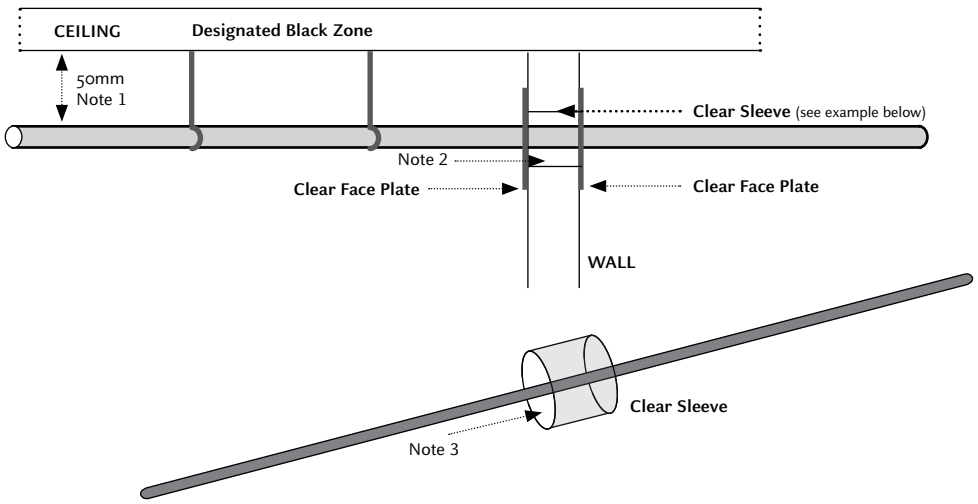
a. conduit inspection boxes
b. outlet and junction boxes, and
c. T-pieces.

5.1.47. Tamper evident seals **must** be uniquely identifiable.

[–,–,TS] Wall penetrations

5.1.48. Agencies **must** ensure that the following conditions are met for wall penetrations:

a. if conduit penetrates a wall, the penetrating section is encased in a second plastic conduit
b. the outer conduit is at least 10mm from the inner conduit
c. the outer conduit is large enough to ensure visibility of the cable for the entire length of the wall penetration
d. each end of the wall penetration is sealed with a clear face plate secured to the wall as shown in the diagram below, and
e. the inner conduit run is clearly visible from both sides of the wall.



Note 1 Minimum clearance between the ceiling and conduit is 50mm. This allows the installation of security classified copper cable in accordance with ACSI 61(C).

Note 2 Surrounding can be filled with fire retardant material only if required to meet building regulations.

Note 3 Minimum clearance between inner and outer conduit is 10mm.

5.1.49. When penetrations of audio secured spaces are desired, agencies **must** consult ASIO.

[–,HP,C-S] Connecting conduit to equipment cabinets

5.1.50. Conduit leading into equipment cabinets **should** be fastened so that it is both tamper-resistant and tamper-evident.

[–,–,TS] Connecting conduit to equipment cabinets

5.1.51. Conduit leading into equipment cabinets **must** be fastened so that it is both tamper-resistant and tamper-evident.

RATIONALE

Cable distribution systems

5.1.52. Systems are vulnerable to Denial-of-Service (DoS) attacks, data interception and data corruption, both deliberately and inadvertently. These vulnerabilities are exposed through uncontrolled and unfettered access to the ICT cabling infrastructure.

5.1.53. The controls in this section ensure that cabling is installed in a structured manner such that access to the cabling is tightly controlled, cabling can be readily and easily monitored and any anomalies can be quickly identified and dealt with.

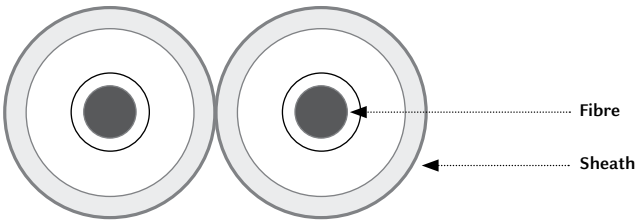
Suspended conduit

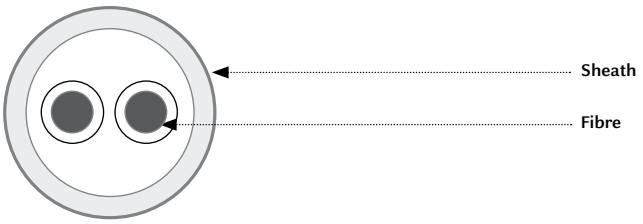
5.1.54. To achieve necessary separation distance, where the empty space above the cables within the conduit is sufficiently great, agencies may use conduit of diameter 50mm or larger attached to the ceiling.

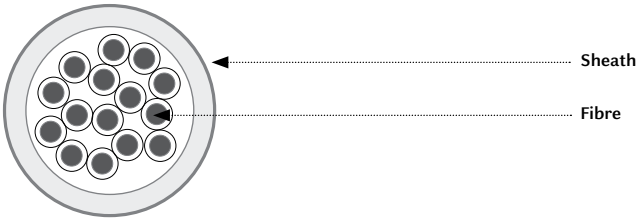
EXAMPLES

5.1.55. The cable shown below could carry UNCLASSIFIED and HIGHLY PROTECTED in one subunit and CONFIDENTIAL and SECRET in another subunit.

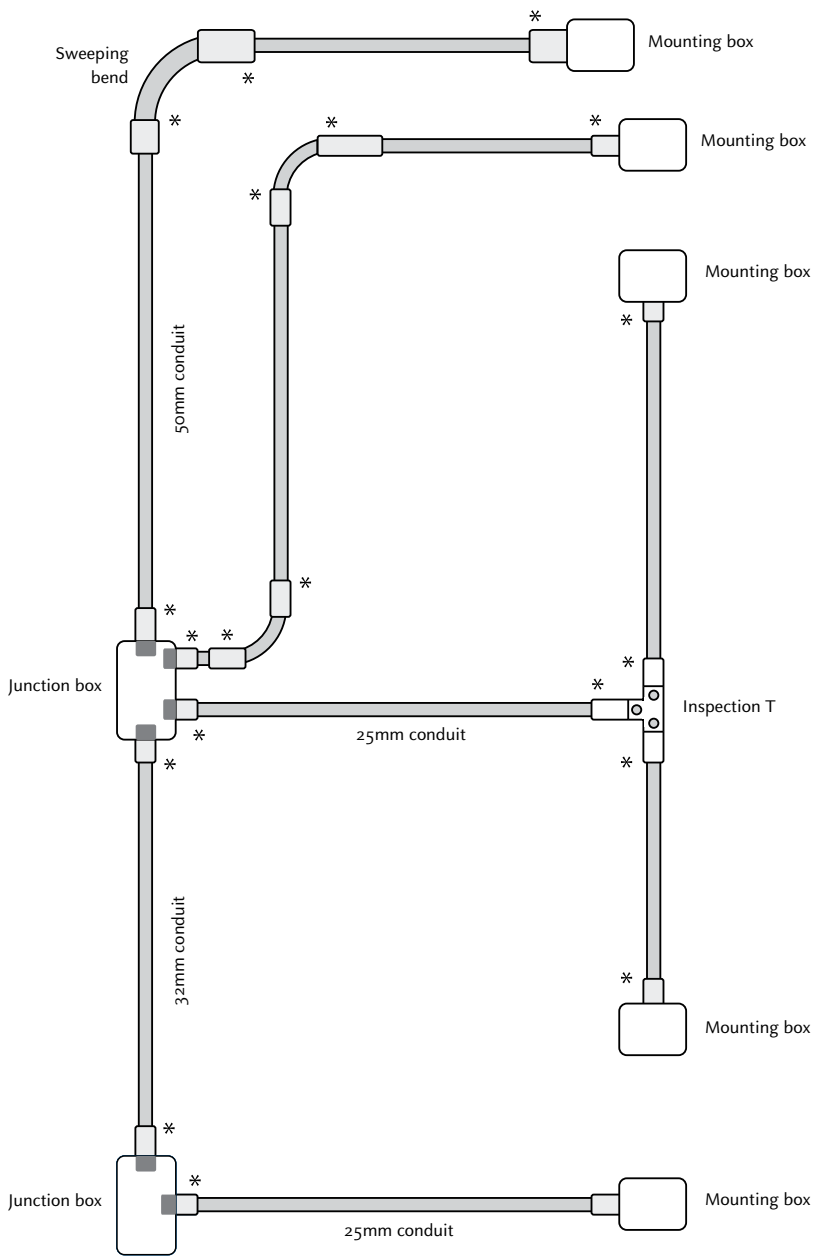
5.1.56. Examples of other typical fibre cross-sections are shown below.







5.1.57. The diagram below shows an example conduit plan.



* Glued Joint

Labelling and Registration

PRINCIPLE

5.1.58. Cable labelling and cable registers ensure good management of cabling systems and allow for easy auditing processes.

OBJECTIVE

5.1.59. To ensure that conduit labelling and cable registers is used to track cable runs within a facility.

CONTEXT

Scope

5.1.60. This section covers information relating to the labelling of cabling infrastructure installed in secured spaces.

RISKS

5.1.61. An agency having incorrect or no cable infrastructure labelling can lead to accidental or malicious rerouting of secure cabling to a lesser security classified cable system.

5.1.62. An agency unable to accurately identify secure cable/outlets through labelling and a cable register prevents security personnel or accreditation personnel from determining if any accidental or malicious cabling modifications have occurred.

5.1.63. Personnel make modifications to secure cabling using poorly maintained or non-existent cable registers, leading to compromise or denial of service through accidental or malicious cable routing practices.

5.1.64. An attacker gains unauthorised or uncontrolled access to network infrastructure, resulting in labelling changes to security classified labelling infrastructure to deliberately hide unauthorised cabling.

CONTROLS

[–,–,TS] Conduit label specifications

5.1.65. Labels for TOP SECRET conduits **must** be:

a. a minimum size of 2.5cm x 1cm
b. attached at 1m intervals, and
c. marked as 'TS RUN'.

5.1.66. Areas where uncleared personnel could frequently visit **must** have red text on a clear background.

5.1.67. Areas that are not clearly observable **must** have red text on a white background.

[U,IC-HP,R-TS] Installing conduit labelling

5.1.68. Conduits installed in public or visitor areas **should** be labelled in a manner that does not attract undue attention by people who do not have the appropriate security clearances or a need-to-know of the existence of such cabling.

[–,–,TS] Labelling wall outlet boxes

5.1.69. Wall outlet boxes for TOP SECRET cables **must** be labelled according to the conduit label specifications and with the addition of the system name(s).

[U,IC-HP,R-TS] Standard operating procedures

5.1.70. Site conventions for labelling and registration **should** be recorded in SOPs.

[–,–,TS] Labelling cables

5.1.71. TOP SECRET cables **must** be labelled at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable along its entire path.

[U,IC-HP,R-S] Cable register

5.1.72. Agencies **should** maintain a register of cables.

5.1.73. A cable register **should** record at least the following information:

a. cable identification number,
b. security classification
c. source
d. destination, and
e. floor plan diagram.

[–,–,TS] Cable register

5.1.74. Agencies **must** keep a cable register for TOP SECRET cables.

[U,IC-HP,R-TS] Cable inspections

5.1.75. Agencies **should** inspect cables for inconsistencies with the cable register on a regular basis.

5.1.76. The frequency of cable inspections **should** be defined in the SSP.

RATIONALE

Cable register

5.1.77. Cabling systems installed in security classified areas should be readily identifiable and details listed in a cable register. This allows for:

- tight control of cabling as cabling systems are easily identifiable and documented
- good management of the cabling systems, and
- easy audit to ensure that the system has not been compromised.

Patch Panels, Patch Cables and Fly Leads

PRINCIPLE

5.1.78. Patch panel security can be achieved through the configuration control of separations, terminations, fly lead connectors and cable lengths.

OBJECTIVE

5.1.79. To ensure that systems are not accidentally or maliciously patched to other systems of a lesser security classification on a patch panel.

CONTEXT

Scope

5.1.80. This section covers information relating specifically to the configuration and installation of patch panels, patch cables and fly leads associated with security classified processing equipment.

Exception for patch cable and fly lead connectors

5.1.81. For patch cables, the same connectors can be used for different security classifications if the length of the TOP SECRET patch cables is less than the distance between the patch panel and any patch panel of a lower security classification.

RISKS

5.1.82. Uncleared or hostile personnel can inadvertently or maliciously connect a system of a higher security classification to a system of a lower security classification, resulting in a data spill from the higher to the lower system.

5.1.83. Uncleared or hostile personnel can gain access to security classified patching systems that do not have appropriate physical security protection. This increases the potential for inadvertent or deliberate cross-connection, resulting in a data spill from the higher to the lower system. In addition, an information security breach would be created by allowing unauthorised personnel access to the information.

5.1.84. Electromagnetic coupling of signals from a higher to a lower security classified network could allow detection of these signals outside the secured space by an attacker.

CONTROLS

[–,–,TS] Terminations to patch panels

5.1.85. Agencies **must** ensure that only TOP SECRET cabling is terminated on a TOP SECRET patch panel.

[–,–,TS] Patch cable and fly lead connectors

5.1.86. In rooms containing cabling for both TOP SECRET systems and systems of other security classifications, agencies **must** ensure that the connectors for the TOP SECRET systems are different to those of the other systems.

5.1.87. In rooms containing cabling for both TOP SECRET systems and systems of other security classifications, agencies **must** document the selection of connector types.

[–,–,TS] Physical separation of patch panels

5.1.88. Agencies **should** physically separate TOP SECRET and non-TOP SECRET patch panels by installing them in separate equipment cabinets.

5.1.89. Where spatial constraints demand patch panels of a lower security classification than TOP SECRET to be located in the same equipment cabinet, agencies **must**:

a. provide adequate separation within the cabinet as specified by ACSI 61(C)
b. ensure that only people cleared to TOP SECRET have access to the cabinet, and
c. obtain approval from the relevant accreditation authority prior to installation.

[–,–,TS] Fly lead installation

5.1.90. Agencies **must** ensure that the fibre optic fly leads used to connect conduit outlets to equipment either:

a. do not exceed 5m in length; or
b. if they exceed 5m in length:
   1) are run in a protective and easily inspected pathway where practicable
   2) are clearly labelled at the terminal end with the wall outlet designator, and
   3) are approved by the accreditation authority.

[–,–,TS] Length of transceiver unshielded twisted pair cables

5.1.91. In situations where a length of unshielded twisted pair cable is needed to patch between a fibre optic modem and equipment such as a workstation, the length of the cable **should not** exceed 0.5m.

5.1.92. Agencies **must not** use cables that exceed 0.5m without approval from their accreditation authority.

RATIONALE

Terminations to patch panels

5.1.93. Connecting a TOP SECRET system to a system of a lesser security classification will result in a data spill. A data spill could result in the following issues:

- inadvertent or deliberate access by non-TOP SECRET cleared personnel or personnel, and
- the lesser system not meeting the appropriate requirements to secure the TOP SECRET information from unauthorised access or tampering.

Patch cable and fly lead connectors

5.1.94. Ensuring that TOP SECRET cables are equipped with connectors of a different configuration to all other cables will prevent inadvertent connection to systems of lesser security classifications.

Physical separation of patch panels

5.1.95. Appropriate physical separation between a TOP SECRET system and a system of a lesser security classification will:

- reduce or eliminate the chances of cross patching between the systems
- reduce or eliminate the effects of electromagnetic coupling from one system to another, and
- reduce or eliminate the possibility of unauthorised personnel or personnel gaining access to TOP SECRET system elements.

Fly lead installation

5.1.96. Fibre optic fly leads greater than 5m in length should be made part of the facility's fixed infrastructure for cable configuration and physical protection purposes.

5.1.97. TOP SECRET systems are mandated to use fibre optic cabling to eliminate electromagnetic radiation from cabling. Where the use of metallic cable is unavoidable, the metallic cable length must be kept as short as possible, to minimise potential electromagnetic radiation from the cable.

REFERENCES

5.1.98. The following references can be consulted for additional information: ACSI 61(C), *Guidelines for the Installation of Communication and Information Processing Equipment and Systems*.

Communications Systems and Devices

Radio Frequency and Infrared Devices

PRINCIPLE

5.2.1. Radio frequency (RF) and infrared devices can be controlled by restricting their use to appropriately secured spaces and restricting their transmission power.

OBJECTIVE

5.2.2. To ensure that RF and infrared devices are appropriately controlled to prevent security classified communications from being compromised from outside an agency's area of physical control.

CONTEXT

Scope

5.2.3. This section covers information relating to the use of RF and infrared devices in secured spaces. Information on the use of RF devices outside secured spaces can be found in the *Working Off-Site Security* chapter of this manual.

Exemptions for the use of infrared devices

5.2.4. An infrared device can be used in a secured space provided it does not communicate information.

Exemptions for the use of RF devices

5.2.5. The following devices, at the discretion of the accreditation authority, can be exempted from the controls associated with RF transmitters:

- pagers that can only receive messages
- garage door openers, and
- car lock/alarm keypads.

5.2.6. Medical equipment that uses RF to communicate between sub-components is exempted from the controls associated with RF transmitters.

RISKS

5.2.7. An attacker compromises a wireless device and subsequently uses it for clandestine information collection.

5.2.8. An attacker intercepts unsecured wireless communications in order to capture information.

5.2.9. An agency's use of RF devices poses an emanation security risk.

5.2.10. An attacker jams wireless devices to prevent availability of resources.

5.2.11. An attacker intercepts and changes or corrupts the information to prevent data integrity.

CONTROLS

[–,–,TS] Pointing devices

5.2.12. Wireless RF pointing devices **must not** be used in TOP SECRET areas unless used within a RF screened building.

[U,IC-P,R] Infrared keyboards

5.2.13. Agencies using infrared keyboards **should** ensure that infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.

[–,HP,C-S] Infrared keyboards

5.2.14. Agencies using infrared keyboards **must not** allow:

a. line of sight and reflected communications travelling into an unsecured space
b. multiple infrared keyboards at different security classifications in the same area
c. other infrared devices to be brought into line of sight of the keyboard or its receiving device/port, and
d. infrared keyboards to be operated in areas with unprotected windows.

[–,–,TS] Infrared keyboards

5.2.15. Agencies using infrared keyboards **must not** allow:

a. line of sight and reflected communications travelling into an unsecured space
b. multiple infrared keyboards at different security classifications in the same area
c. other infrared devices within the same area, and
d. infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

[–,–,TS] RF devices in secured spaces

5.2.16. Agencies **must** prevent RF devices from being brought into TOP SECRET areas unless authorised by the accreditation authority.

5.2.17. Agencies **should** deploy measures to detect and respond to active RF devices within TOP SECRET areas.

[–,HP,C-S] RF devices in secured spaces

5.2.18. Agencies **should** prevent RF devices from being brought into secured spaces unless authorised by the accreditation authority.

GUIDANCE

[–,P,–] RF devices in secured spaces

5.2.19. It is **recommended** that agencies prevent RF devices from being brought into secured spaces unless authorised by the accreditation authority.

[–,HP,C-S] RF devices in secured spaces

5.2.20. It is **recommended** that agencies deploy measures to detect and respond to active RF devices within secured spaces.

[U,IC-HP,R-TS] RF controls

5.2.21. It is **recommended** that agencies limit the effective range of communications outside the agency's area of control by:

a. minimising the output power level of wireless devices, or
b. RF shielding.

RATIONALE

Infrared keyboards

5.2.22. When using infrared keyboards with a HIGHLY PROTECTED, CONFIDENTIAL or SECRET system, drawn opaque curtains are an acceptable method of protecting windows.

5.2.23. When using infrared keyboards with a TOP SECRET system, windows with curtains that can be opened are not acceptable as a method of permanently blocking infrared transmissions.

Fax Machines and Multifunction Devices

PRINCIPLE

5.2.24. The development of installation and configuration guidelines can be used to prevent inappropriate configuration and usage by personnel of modern fax machines and MFDs.

OBJECTIVE

5.2.25. To ensure that appropriate procedures for sending and receiving information over a fax machine or MFD are implemented and followed.

CONTEXT

Scope

5.2.26. This section covers information relating to fax machines and MFDs connected to either the public switched telephone network (PSTN) or to HGCE. Other transmission and reception techniques are considered out of scope.

RISKS

5.2.27. An attacker exploits incorrect authentication procedures leading to a fax message being received by uncleared personnel and resulting in a compromise.

5.2.28. An operator fails to clear from memory a secure fax communication that has failed before switching back to an unsecured line, resulting in the secure fax being resent over an unsecured phone line.

5.2.29. An operator fails to establish a secure transmission before sending a fax, resulting in the secure fax being communicated in the clear and the information being compromised.

5.2.30. An agency's poor memory clearing procedures can lead to a security classified fax being retained in memory and printed by someone that does not have the need-to-know.

5.2.31. An operator accidentally sends a security classified fax stored in memory from a dedicated secure fax machine that has been connected directly to an unsecured phone line.

5.2.32. An attacker uses a telephone network connected to a MFD to compromise a computer network to which the device is also connected.

CONTROLS

[–,IC-HP,R-TS] Communicating information

5.2.33. Agencies intending to use fax functionality to send security classified information **must** ensure that:

a. all requirements for the use of telephone systems are met at both ends for the security classification to be sent; and
b. the sender makes arrangements for the receiver to:
   1) collect the information from the receiving machine as soon as possible after it is received, and
   2) notify the sender if the fax does not arrive within an agreed amount of time.

[–,–,C-TS] Communicating information

5.2.34. Agencies intending to use fax machines to send security classified information are **required** to comply with additional requirements in ACSI 129 and ACSI 131.

[–,IC,R] Connecting MFDs to telephone networks

5.2.35. Agencies **should not** enable a direct connection from a MFD to a telephone network of a lower security classification unless the device:

a. has been evaluated to at least Common Criteria EAL2 and the scope of the evaluation includes:
   1) information flow control functions to prevent unintended and unauthorised data flows
   2) data export controls capable of blocking information based on protective markings
   3) authentication, and
   4) audit data generation and protection; and
b. is configured to use the evaluated functionality in accordance with the relevant policies.

[–,P,–] Connecting MFDs to telephone networks

5.2.36. Agencies **should not** enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same security classification as the computer network to which the device is connected.

[–,HP,C-TS] Connecting MFDs to telephone networks

5.2.37. Agencies **must not** enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same security classification as the computer network to which the device is connected.

RATIONALE

Communicating information

5.2.38. Using the correct procedure for sending a security classified fax will ensure that it is sent securely to the correct recipient.

5.2.39. Using the correct memory erase procedure will prevent a secure fax being communicated in the clear.

5.2.40. Implementing the correct procedure for establishing a secure call will prevent sending a secure fax in the clear.

5.2.41. Witnessing the receiving of a fax and powering down the receiving machine or clearing the memory after transmission will prevent someone without a need-to-know accessing the fax.

5.2.42. Ensuring secure fax machines and MFDs are not connected to unsecured phone lines will prevent accidentally sending security classified messages stored in memory.

REFERENCES

5.2.43. Specific information regarding the procedures for fax machines and MFDs attached to HGCE can be found in ACSI 129, *Operational Systems Security Doctrine for the Sectera Wireline Terminal* and ACSI 131, *Operational Systems Security Doctrine for the OMNI Terminal*.

Telephones and Telephone Systems

PRINCIPLE

5.2.44. Telephone systems can be protected through personnel awareness, visual indicators and off-hook audio protection mechanisms.

OBJECTIVE

5.2.45. To ensure that security classified background conversations are not accidentally communicated across an unsecured communications medium or to personnel without a need-to-know.

CONTEXT

Scope

5.2.46. This section covers information relating to the secure use of fixed, cordless and mobile telephones, as well as the systems used to communicate the information. Information regarding Voice over Internet Protocol and encryption of data in transit is covered in the *Internet Protocol Telephony* and *Cryptographic Fundamentals* sections of this manual.

Exception for speakerphones

5.2.47. A speakerphone can be used on a TOP SECRET telephone within a TOP SECRET area as long as:

- it is located in a room rated as audio secure
- the room is audio secure during any conversations, and
- only personnel involved in discussions are present in the room.

RISKS

5.2.48. A person discusses security classified material over an unsecured telephone network, resulting in a compromise.

5.2.49. Personnel conducting an unsecured telephone call are within earshot of a background conversation, resulting in the background conversation being communicated over the unsecured telephone.

5.2.50. Personnel are not instructed in the appropriate use of telephone protocols and information is released into an unsecured environment resulting in a compromise.

5.2.51. A person using a secure telephone to communicate information is not aware of surrounding environmental conditions, including the proximity of any uncleared or unauthorised individuals.

5.2.52. An attacker exploits the fact that having an active speakerphone in a security classified environment is more likely to pick up unintentional conversations, resulting in a compromise.

5.2.53. An attacker intercepts background conversations due to an agency failing to implement off-hook audio protection, resulting in the disclosure of information.

CONTROLS

[U,IC-HP,R-TS] Personnel awareness

5.2.54. Agencies **must** advise personnel of the maximum permitted security classifications for conversations using both internal and external telephone connections, as determined by the accreditation of the internal telephone system and the degree of encryption, if any, on external connections.

5.2.55. Agencies **should** advise personnel of the audio security risk posed by using telephones in areas where security classified conversations can occur.

[U,IC-HP,R-TS] Visual indication

5.2.56. Agencies permitting different levels of conversation for different kinds of connections **should** use telephones that give a visual indication of what kind of connection has been made.

[–,IC-HP,R-TS] Use of telephone systems

5.2.57. Agencies intending to use telephone systems for the transmission of security classified information **must** ensure that:

a. the system has been accredited for the purpose, including the completion of a security risk assessment and formal acceptance of the residual security risks, and
b. all security classified traffic that passes over external systems is encrypted in accordance with the encryption specified for the security classification of the information being communicated.

[–,IC-HP,R-TS] Cordless and mobile telephones

5.2.58. Agencies **must not** use cordless or mobile telephones for the transmission of security classified information unless the security they use has been approved by DSD for that security classification.

[U,IC-HP,R-TS] Cordless telephones with secure telephony devices

5.2.59. Agencies **must not** use cordless telephones in conjunction with secure telephony devices.

[–,–,TS] Speakerphones

5.2.60. Agencies **must not** use speakerphones on telephones within TOP SECRET areas.

[–,–,S] Off-hook audio protection

5.2.61. Agencies **should** ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of security classified information in areas where such information could be discussed.

[–,–,TS] Off-hook audio protection

5.2.62. Agencies **must** ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of security classified information in areas where such information could be discussed.

5.2.63. Agencies **should** use push-to-talk handsets to meet the requirement for off-hook audio protection.

5.2.64. Where agencies vary from the requirement to use push-to-talk handsets, agencies **must** ensure that personnel are made aware of the requirement to use the protection feature appropriately.

[–,IC-HP,R-TS] Paging services

5.2.65. Agencies **must not** use paging, multimedia or short message services to communicate security classified information.

GUIDANCE

[–,P-HP,C] Off-hook audio protection

5.2.66. It is **recommended** that agencies ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of security classified information in areas where such information could be discussed.

[–,–,S] Off-hook audio protection

5.2.67. It is **recommended** that agencies use push-to-talk handsets in open areas, and where phones are shared.

RATIONALE

Telephones and telephone systems

5.2.68. All non-secure telephone networks are subject to interception. The level of expertise needed to do this varies greatly. Accidentally or maliciously revealing information over a public telephone networks can lead to interception.

Cordless and mobile telephones

5.2.69. Cordless telephones have minimal transmission security, therefore should not be used for security classified communications.

Off-hook audio protection

5.2.70. Providing off-hook security minimises the chance of accidental security classified conversation being coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat.

5.2.71. Simply providing an off-hook audio protection feature to personnel is not sufficient to meet the requirement for its use. To ensure that the protection feature is used appropriately personnel will need to be made aware of the protection feature and trained in its proper use.

EXAMPLES

5.2.72. If an agency has accredited their internal system to carry PROTECTED conversations but external calls are only permitted up to X-IN-CONFIDENCE, then they can use telephones with displays that show an extension number for internal calls, and the full number for external calls. Personnel would then be advised to double check this display before undertaking a security classified conversation.

5.2.73. If an agency has chosen to implement encryption on some calls, then they can use phones that display an icon to indicate when a call is encrypted.

Emanation Security

Emanation Security Threat Assessments

PRINCIPLE

5.3.1. Emanation security threat assessments are used to identify specific counter-measures to minimise the threat of interception of compromising emanations that disclose information from electronic processing equipment.

OBJECTIVE

5.3.2. To ensure that the threat of interception of compromising emanations is considered and appropriately risk managed.

CONTEXT

Scope

5.3.3. This section covers information relating to emanation security controls that could be mandated when identified in an emanation security threat assessment.

RISKS

5.3.4. An agency underestimates an attacker of a secure system in a high-threat environment, resulting in a compromise of information.

5.3.5. An agency does not implement recommended installation counter-measures for a secure system, resulting in a compromise by the interception of radiated information.

5.3.6. An attacker compromises tactical mobile platform transmissions due to poor procedures or installation standards.

CONTROLS

[–,–,C-TS] Early identification of emanation security issues

5.3.7. Agencies **should** seek an emanation security threat assessment as early as possible in project lifecycles as emanation security controls can have significant cost implications.

[–,–,C-S] Emanation security threat assessments within Australia

5.3.8. Agencies designing and installing systems within Australia **should**:

a. contact DSD for an emanation security threat assessment in accordance with ACSI 71(C), and
b. install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment, as defined in ACSI 61(C).

[–,–,TS] Emanation security threat assessments within Australia

5.3.9. Agencies designing and installing systems within Australia **must**:

a. contact DSD for an emanation security threat assessment in accordance with ACSI 71(C), and
b. install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment, as defined in ACSI 61(C).

[–,–,C-TS] Emanation security threat assessments outside Australia

5.3.10. Agencies deploying systems overseas in military and high security risk locations **must**:

a. contact DSD for an emanation security threat assessment in accordance with ACSI 71(C), and
b. install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment, as defined in ACSI 61(C).

[–,–,TS] TEMPEST rated equipment

5.3.11. Equipment within a TOP SECRET area within Australia does not usually need certification to TEMPEST standards. However, agencies **must** ensure that equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

GUIDANCE

[–,P-HP,R] Emanation security threat assessments outside Australia

5.3.12. It is **recommended** that agencies deploying systems overseas:

a. contact DSD for emanation security threat advice, and
b. install cabling and equipment in accordance with this document plus any specific installation criteria derived from the emanation security threat assessment, as defined in ACSI 61(C).

[U,IC-P,R] Emanation security

5.3.13. It is **recommended** that agencies implement the requirements from this section if they have specific concerns about compromise through emanation security attacks.

5.3.14. It is **recommended** that emanation security controls implemented include:

a. using TEMPEST rated equipment
b. using fibre optic cables
c. installing and using filters on communications and power lines
d. using TEMPEST screened buildings or rooms, and
e. appropriately positioning sensitive equipment in relation to other equipment.

RATIONALE

Emanation security threat assessments

5.3.15. Obtaining the current threat advice from DSD on potential adversaries and applying the appropriate counter-measures is vital in maintaining the confidentiality of systems both domestically and overseas from an emanation security attack.

5.3.16. This is a cost effective way of only implementing counter-measures that will reduce the threat and provide some future proof if threats increase.

Emanation security threat assessment outside Australia

5.3.17. Deployed military platforms are more vulnerable to emanation security attack, requiring a current threat assessment and counter-measure implementation. Failing to implement recommended counter-measures and standard operation procedures to reduce threats could result in the platform emanating compromising signals which, if intercepted and analysed, could lead to platform compromise with serious consequences.

Emanation security

5.3.18. Failing to implement recommended counter-measures against an emanation security attack in high threat locations can lead to compromise. Having a good cable infrastructure and installation methodology will provide a strong backbone that will not need updating if the threat increases. Infrastructure costs are very expensive and time consuming to retro-fit.

REFERENCES

5.3.19. Additional information on cabling and separation standards, as well as the potential dangers of operating RF transmitters in the vicinity of systems can be found in ACSI 61(C), *Guidelines for the Installation of Communication and Information Processing Equipment and Systems*.

5.3.20. Additional information on conducting an emanation security threat assessment can be found in ACSI 71(C), *A Guide to the Assessment of Electromagnetic Security in Military and High-risk Locations*.

Information Technology Security

Product Security

Product Selection and Acquisition

PRINCIPLE

6.1.1. Evaluated products form the basis of an agency's information security posture.

OBJECTIVE

6.1.2. To ensure that through proper product selection and acquisition processes agencies can gain independent assurance that technical security risks are reduced.

CONTEXT

Scope

6.1.3. This section covers information on the selection and acquisition of products that provide security functionality for the protection of information. It does not provide information on the selection or acquisition of products that do not provide security functionality or physical security products.

Selecting products without information security functions

6.1.4. Agencies selecting products that do not provide an information security function or selecting products that will not use their security functions are free to follow their own agency or departmental acquisition guidelines.

Convergence

6.1.5. Convergence is the integration of a number of discrete technologies into one product. Converged solutions can include the advantages and disadvantages of each discrete technology.

6.1.6. Most products will exhibit some element of convergence. When products have converged elements, agencies will need to comply with the relevant areas of this manual for the discrete technologies when deploying the converged product.

6.1.7. As an example, when agencies choose to use evaluated media devices, such as encrypted flash memory media, the requirements for evaluated products, media devices and cryptographic security apply.

Evaluated Products List

6.1.8. The Evaluated Products List (EPL) consists of products that have been, or are in the process of being, evaluated through one or more of the following schemes:

- Common Criteria
- high grade evaluation, or
- another DSD approved evaluation.

6.1.9. The EPL is maintained by DSD and provides a listing of approved products for the protection of information.

Evaluation level mapping

6.1.10. The Information Technology Security Evaluation Criteria (ITSEC) and Common Criteria assurance levels used in the EPL are similar, but not identical, in their relationship. The table below shows the relationship between the two evaluation criteria.

6.1.11. This manual refers only to Common Criteria EALs. The table maps ITSEC assurance levels to Common Criteria assurance levels.

CRITERIA	ASSURANCE LEVEL							
Common Criteria	N/A	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	E0	N/A	E1	E2	E3	E4	E5	E6

6.1.12. For guidance on the level of assurance provided by products approved under another recognised evaluation standard, please refer to the corresponding consumer guide.

Recognition arrangements

6.1.13. DSD has a number of recognition arrangements regarding evaluated products. Before choosing a product that has not been evaluated by the AISEP or DSD, agencies are encouraged to investigate whether the product will be recognised for Australian use once it has complete evaluation in a foreign scheme.

6.1.14. Two such recognition arrangements are for the Common Criteria Recognition Arrangement up to the assurance level of EAL4 with the lifecycle flaw remediation augmentation and for degausser products listed on the National Security Agency/Central Security Service's *Evaluated Products List - Degausser* (EPLD).

Australasian Information Security Evaluation Program

6.1.15. The AISEP exists to ensure that a range of evaluated products are available to meet the needs of Australian and New Zealand Government agencies.

6.1.16. The AISEP performs the following functions:

- evaluation and certification of products using the Common Criteria
- continued maintenance of the assurance of evaluated products, and
- recognition of products evaluated by a foreign scheme with which the AISEP has a mutual recognition agreement.

RISKS

6.1.17. Agencies rely upon the security functionality of a product that does not meet the vendors' claims, resulting in a loss of confidentiality, integrity or availability of information.

6.1.18. A failure in a security feature of a product results in a loss of confidentiality, integrity or availability of information.

6.1.19. Agencies rely upon the security functionality of a product that does not have sufficient assurance to protect against external threats.

6.1.20. A product is accidentally or maliciously replaced or altered during the purchase and delivery process, resulting in vulnerabilities in the agency's system.

6.1.21. An agency enters into a contractual agreement that stipulates conditions that are contrary to an agency's security requirements, resulting in a loss of confidentiality of information.

6.1.22. An agency installs a non-evaluated software product onto a system without confirming the integrity of the software, resulting in malicious code being introduced to the system.

6.1.23. An agency deploys a converged product without considering the security risks associated with the convergence of technologies, resulting in a converged vulnerability in the product going unnoticed.

CONTROLS

[U,IC-HP,R-TS] Evaluated product selection

6.1.24. When relying on a product's security functionality for the protection of information and systems, agencies **should** select products that have been evaluated against the desired information security function.

[U,IC-HP,R-TS] Evaluated product selection preference order

6.1.25. Agencies **should** select products in the following order of preference:

a. products having completed a Common Criteria evaluation through the AISEP, a Common Criteria evaluation covered under the Common Criteria Recognition Arrangement, a high grade evaluation or other DSD approved evaluation
b. products in evaluation in the AISEP or DSD
c. products in evaluation in a scheme or program that DSD has a recognition agreement with, and will be recognised under the agreement when evaluation is completed, and
d. products that have had no formally recognised evaluation.

[U,IC-HP,R-TS] Assessing the suitability of evaluated products

6.1.26. In assessing a product for its suitability to meet security objectives, an agency **should** review all available documentation for the following:

a. its applicability to the intended environment
b. that the version and configuration of the product matches that of the evaluated product
c. that the desired functionality was evaluated and certified
d. that the level of assurance is adequate for their needs, and
e. for any constraints or caveats DSD have placed on the product's implementation and use.

[U,IC-HP,R-TS] Documenting product choice

6.1.27. When choosing a product, agencies **must** document:

a. the desired degree of assurance in the product's key functions
b. the actual degree of assurance provided by the chosen product, based on the level of evaluation it has received for its key functions
c. justification for any decisions to drop to the next level in the defined selection order of preference, and
d. acknowledgement and acceptance of any security risk introduced by the use of a product of lower assurance than desired, particularly if using a product that has not, and might never, complete all relevant evaluation processes.

[U,IC-HP,R-TS] Assessing the suitability of evaluated high grade products

6.1.28. Agencies selecting high grade products **must** contact DSD through their accreditation authority for product specific guidance.

[–,HP,C-TS] Sourcing non-evaluated software products

6.1.29. Agencies **should**:

a. obtain software from verifiable sources and verify its integrity using vendor supplied checksums, and
b. validate the software's interaction with the operating systems and network within a test environment prior to use on operational systems.

[U,IC-HP,R-TS] Delivery of evaluated products

6.1.30. Agencies **should** ensure that products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

[U,IC-HP,R-TS] Delivery of evaluated high grade products

6.1.31. Agencies procuring high grade products **must** contact DSD through their accreditation authority for any product specific delivery procedures.

[U,IC-HP,R-TS] Leasing arrangements

6.1.32. Agencies **should** ensure that leasing agreements for hardware products take into account the:

a. difficulties that could be encountered when the hardware product needs maintenance
b. if the hardware product can be easily sanitised prior to its return, and
c. the possible requirement for destruction if sanitisation cannot be performed.

[U,IC-HP,R-TS] Converged products

6.1.33. Agencies deploying converged products **should** take into account security risks identified for each discrete technology and how these security risks could affect the converged product as a whole.

GUIDANCE

[U,IC-HP,R-TS] Evaluated product selection preference order

6.1.34. It is **recommended** that agencies choosing a product that has no formally recognised evaluation conduct an evaluation of the product or choose a product that has been evaluated by a vendor independent third party.

[U,IC-HP,R-TS] Ongoing maintenance of assurance

6.1.35. It is **recommended** that agencies choose products from developers that have made a commitment to the ongoing maintenance of the assurance of their product.

[U,IC-P,R] Sourcing non-evaluated software products

6.1.36. It is **recommended** that agencies:

a. obtain software from verifiable sources and verify its integrity using vendor supplied checksums, and
b. validate the software's interaction with the operating systems and network within a test environment prior to use on operational systems.

[U,IC-HP,R-TS] Delivery of non-evaluated products

6.1.37. It is **recommended** that agencies ensure that products purchased without the delivery assurances provided through the use of formally evaluated procedures are delivered in a manner that provides confidence that they receive the product that they expect to receive.

RATIONALE

Evaluated product selection

6.1.38. All products that are listed on the EPL have gained a degree of independent assurance testing by an approved DSD evaluation. Further investigation is needed to ensure that the evaluation examined the desired security requirements of the purchasing agency.

Evaluated product selection preference order

6.1.39. In selecting products for use, agencies should note that completed evaluations provide greater assurance than those products that are still undergoing evaluation or have not completed any formal evaluation activity. This assurance gradation is reflected in the preference order for selecting security products. If an agency selects a product that is ranked lower in the preference order, the reason for this decision must be recorded.

6.1.40. For products that are currently in evaluation, agencies should select those that are undergoing evaluation through AISEP in preference to those being conducted in a recognised foreign scheme. If a major vulnerability is found during the course of an AISEP evaluation, DSD might be able to advise agencies on appropriate risk reduction strategies.

6.1.41. For products that have not completed a formally recognised evaluation the agency will still need to ensure that the product's security functionality has been evaluated. Agencies are recommended to either organise for an evaluation by a vendor independent third-party or they could choose to evaluate the product internally to the agency.

6.1.42. Agencies should be aware that while this section provides a product selection preference order, policy stated elsewhere in this manual, or product specific advice from DSD, could override this standard by specifying more rigorous requirements for particular functions and device use. Additionally, where an EAL is mandated for a product to perform a cryptographic function for the protection of data at rest or in transit, as specified within the *Cryptographic Security* chapter, products that have not completed a DCE evaluation do not satisfy the requirement.

6.1.43. Where an agency needs a product that either does not provide an information security function, or relies upon an inherent security function, then the policy regarding the selection of products from the EPL does not apply.

Assessing the suitability of evaluated products

6.1.44. A product listed on the EPL might not meet the security requirements of an agency. This could occur for a number of reasons, including that the scope of the evaluation is inappropriate for the intended use or the operational environment differs from that assumed in the evaluation.

6.1.45. As such, an agency should ensure that a product is suitable by reviewing all available documentation. In the case of Common Criteria certified products, this documentation includes the security target, certification report, consumer guide and any caveats contained in the entry on the EPL.

6.1.46. Products that are in evaluation will not have a certification report and may not have a published security target. A draft security target can be obtained from DSD for products that are in evaluation through AISEP. For products that are in evaluation through a foreign scheme, the vendor can be contacted directly for further information.

Documenting product choice

6.1.47. Agencies must document their decision for choosing a particular product. This provides a detailed rationale for the decision made, and enables this information to be used in an overall risk management process.

Sourcing non-evaluated software products

6.1.48. Software products downloaded from websites on the Internet could contain malicious code or malicious content that is installed along with the legitimate software. Agencies need to confirm the integrity of the software they are installing before deploying it on a system to ensure that no unintended software is installed at the same time.

Delivery of evaluated products

6.1.49. It is important that agencies ensure that the product that is intended for use is the actual product that is received. If the product differs from the evaluated version, then no assurance can be gained from an evaluation being previously performed.

6.1.50. For products evaluated under the ITSEC or the Common Criteria scheme at EAL2 or higher, delivery information is available from the developer in the delivery procedures document.

6.1.51. For products that do not have evaluated delivery procedures, it is recommended that agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

6.1.52. Other factors that the assessment of the delivery procedures for products might need to consider include:

- the intended environment of the product
- the types of attackers that the product will defend against
- the resources of any potential attackers
- the likelihood of an attack
- the level of importance of maintaining confidentiality of the product purchase, and
- the level of importance of ensuring adherence to delivery timeframes.

6.1.53. Delivery procedures can vary greatly from product to product. For most products the standard commercial practice for packaging and delivery could be sufficient for agencies requirements. More secure delivery procedures can include measures to detect tampering or masquerading. Some examples of specific security measures include tamper evident seals, cryptographic checksums and signatures, and secure transportation.

Leasing arrangements

6.1.54. Agencies should consider security and policy requirements when entering into a leasing agreement for equipment in order to avoid potential information security breaches during maintenance, repairs or disposal processes.

Converged products

6.1.55. When different technologies are integrated into a product the security risks, including threats and vulnerabilities, associated with each of the discrete technologies could be transferred to the converged product as a direct result of convergence.

Ongoing maintenance of assurance

6.1.56. Developers that have demonstrated a commitment to ongoing maintenance or evaluation are more likely to be responsive to ensuring that security patches are independently assessed.

6.1.57. A vendor's commitment to assurance continuity can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

REFERENCES

6.1.58. Additional information on the EPL, AISEP and the Common Criteria can be found at:

- http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html
- http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html
- http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep_faqs.html
- http://www.commoncriteriaportal.org, and
- http://www.commoncriteriaportal.org/schemes.html.

Product Installation and Configuration

PRINCIPLE

6.1.59. An evaluated product used in its evaluated configurations will result in gaining the most benefit and assurance from its evaluation.

OBJECTIVE

6.1.60. To ensure that if a product is used outside of its recommended configuration, then the security risk is managed accordingly.

CONTEXT

Scope

6.1.61. This section covers information on installing and configuring products providing information security functionality. It does not provide information on the installation and configuration of general products or physical security products.

Evaluated configuration

6.1.62. A product is considered to be operating in its evaluated configuration if:

- functionality is used that was within the scope of the evaluation and implemented in the specified manner
- only patches that have been assessed through a formal assurance continuity process have been applied, and
- the environment complies with assumptions or organisational security policies stated in the product's security target or similar document.

Unevaluated configuration

6.1.63. A product is considered to be operating in an unevaluated configuration when it does not meet the requirements of an evaluated configuration.

RISKS

6.1.64. Agencies use an evaluated product in a manner that is outside of the scope of the original evaluation, which introduces vulnerabilities that when exploited, result in a loss of confidentiality, integrity or availability of information.

CONTROLS

[U,IC-HP,R-TS] Installation and configuration of evaluated products

6.1.65. Agencies **should** install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

[U,IC-HP,R-TS] Installation and configuration of evaluated high grade products

6.1.66. Agencies **must** ensure that high grade products are installed, configured, operated and administered in accordance with all product specific ACSIs produced by DSD.

[U,IC-HP,R-TS] Use of evaluated products in unevaluated configurations

6.1.67. Agencies wishing to use a product in an unevaluated configuration **must** undertake a security risk assessment including:

a. the necessity of the unevaluated configuration
b. testing of the unevaluated configuration, and
c. the environment in which the unevaluated product is to be used.

[U,IC-HP,R-TS] Use of evaluated high grade products in unevaluated configurations

6.1.68. Products that have a high grade level of assurance **must not** be used in unevaluated configurations.

RATIONALE

Installation and configuration of evaluated products

6.1.69. Evaluation of products provides assurance that the product will work as expected in a clearly defined set of constraints. These constraints, defined by the scope of the evaluation, generally consist of what security functionality can be used, and how the products are configured and operated.

6.1.70. Using an evaluated product in manner which it was not intended could result in the introduction of new threats and vulnerabilities that were not considered by the initial evaluation.

6.1.71. For products evaluated under the Common Criteria and ITSEC, information is available from the developer in the product's installation, generation and startup documentation. Further information is also available in the security target and certification report.

Use of evaluated products in unevaluated configurations

6.1.72. To ensure that a product will still provide the assurance desired by the agency when used in a manner for which it was not intended, a security risk assessment must be conducted upon the altered configuration. The further that a product deviates from its evaluated configuration, the less assurance can be gained from the evaluation.

6.1.73. Given the potential threat vectors and the value of the information being protected, high grade products must be configured in accordance with DSD's guidelines.

Product Classifying and Labelling

PRINCIPLE

6.1.74. Classifying and labelling hardware products can assist in ensuring that system users are aware of procedures that need to be followed when using the hardware.

OBJECTIVE

6.1.75. To ensure that agencies appropriately notify system users of the processing and storage potential of the system they are using.

CONTEXT

Scope

6.1.76. This section covers information relating to the security classification and labelling of both evaluated and non-evaluated hardware products.

Non-essential labels

6.1.77. Non-essential labels are labels other than security classification and asset labels.

RISKS

6.1.78. An agency treats hardware products containing security classified media at a lower security classification than that of the media, resulting in insufficient protection mechanisms being applied to the hardware.

6.1.79. An agency treats hardware products containing security classified media at a lower security classification than that of the media, resulting in insufficient sanitisation and disposal procedures being followed when the hardware is decommissioned.

6.1.80. Personnel cause an information security breach by inputting information into a system that is not accredited to handle information of that security classification.

6.1.81. An attacker is able to make unnoticed modifications to high grade equipment due to unnecessary labels reducing the effectiveness of tamper-evident seals.

CONTROLS

[–,IC-HP,R-TS] Classifying hardware products

6.1.82. Agencies **must** classify hardware products based on the highest security classification of information the hardware and any associated media within the hardware, are approved for processing, storing or communicating.

[–,IC-HP,R-TS] Labelling hardware products

6.1.83. Agencies **must** clearly label all hardware products capable of storing security classified information, with the exception of HGCE, with the appropriate security classification.

[U,IC-HP,R-TS] Labelling of high grade products

6.1.84. Agencies **must not** have any non-essential labels applied to external surfaces of high grade products capable of storing information.

[U,IC-HP,R-TS] Labelling of high grade cryptographic equipment

6.1.85. Agencies are **required** to seek DSD authorisation before applying labels to external surfaces of HGCE.

RATIONALE

Classifying hardware products

6.1.86. When media is used in hardware products there is no guarantee that the hardware has not automatically accessed information from the media and stored it locally to the device, without the knowledge of the system user. As such, the hardware needs to be afforded the same degree of protection as that of the associated media.

Labelling hardware products

6.1.87. The purpose of applying security classification labels to all assets in an area is to reduce the likelihood that a system user will accidentally input information into another system residing in the same area that is of a lower security classification than the information.

6.1.88. Applying security classification labels to assets also assists in determining the appropriate sanitisation, disposal or destruction requirements of the asset based on its security classification.

Labelling of high grade cryptographic equipment

6.1.89. High grade hardware and HGCE often have tamper-evident seals placed on their external surfaces. To assist system users in noticing changes to the seals, and to prevent functionality being degraded, agencies must only place seals on devices when approved by DSD to do so.

EXAMPLES

6.1.90. If a RESTRICTED flash memory device is connected to a standalone UNCLASSIFIED computer the computer must subsequently be afforded the protection of a RESTRICTED asset. However, if the computer happened to be connected to an UNCLASSIFIED system the action would have resulted in an information security incident and would need to be handled appropriately.

Product Patching and Updating

PRINCIPLE

6.1.91. Agencies can patch and upgrade products as long as security risks are considered and reporting processes are followed.

OBJECTIVE

6.1.92. To ensure that attackers are prevented from exploiting known vulnerabilities in products by implementing proper patch management processes.

CONTEXT

Scope

6.1.93. This section covers information on patching both evaluated and non-evaluated software and hardware products.

Patched configuration

6.1.94. A product is considered to be operating in a patched configuration if it had originally been operating in an evaluated configuration but has subsequently had software or firmware patches applied to address security vulnerabilities, without the introduction of new functionality.

RISKS

6.1.95. An attacker exploits a publicly known vulnerability in a product, for which the agency has not applied the available security patch, resulting in the disclosure of information.

6.1.96. An attacker exploits a publicly known vulnerability in a product, for which there is no available security patch, resulting in the disclosure of information.

6.1.97. An agency updates the firmware of a hardware product without checking the integrity of the firmware or the updating process, resulting in compromised firmware being loaded into the product.

CONTROLS

[U,IC-HP,R-TS] Vulnerability and patch availability awareness

6.1.98. Agencies **should**:

a. monitor relevant sources for information about new vulnerabilities and patches for software and hardware used by the agency
b. take corrective action, including a security risk assessment as necessary, when vulnerabilities that could affect systems are discovered
c. follow their change management procedures when applying patches, including the testing of patches prior to their application to production systems, and
d. replace obsolete software and hardware with products for which ongoing support is available.

[U,IC-HP,R-TS] Patching security vulnerabilities in products

6.1.99. Agencies **should**, when possible, ensure that known security vulnerabilities in products are corrected through a vendor recommended patch or upgrade process.

[U,IC-HP,R-TS] Patching security vulnerabilities in evaluated products

6.1.100. Where a vendor patch for security vulnerabilities introduces new functionality in addition to resolving vulnerabilities, agencies **must** treat the resulting configuration as an unevaluated configuration and comply with the requirements for unevaluated configurations.

[U,IC-HP,R-TS] Patching security vulnerabilities in evaluated high grade products

6.1.101. Agencies **must not** operate a high grade product in a patched configuration without approval from DSD.

[U,IC-HP,R-TS] Patching evaluated products with cryptographic functionality

6.1.102. Agencies **must** contact DSD if a patch or service pack addresses a known cryptographic vulnerability.

[U,IC-HP,R-TS] When security patches are not available

6.1.103. Where known vulnerabilities cannot be patched, agencies **should** use other protective measures as determined by a security risk assessment.

[U,IC-HP,R-TS] Firmware updates

6.1.104. Agencies **must** ensure that any firmware updates are performed in accordance with their change management procedures and in a manner that verifies the integrity and authenticity of the updating process.

[U,IC-HP,R-TS] Unsupported software

6.1.105. Agencies **should** assess the security risk of using software or hardware when a cessation date for support is announced or when the product is no longer supported by the developer.

GUIDANCE

[U,IC-HP,R-TS] Patching vulnerabilities in evaluated products

6.1.106. It is **recommended** that agencies ensure that prior to patching evaluated products they conduct a security risk assessment based on:

a. the necessity of the patch
b. the testing of the patch
c. the environment in which the product is used, and
d. any new functionality the patch includes.

[U,IC-HP,R-TS] Patching vulnerabilities in non-evaluated products

6.1.107. It is **recommended** that agencies test and apply all relevant security patches as soon as possible.

[U,IC-HP,R-TS] When security patches are not available

6.1.108. It is **recommended** that protective measures applied to a product to address vulnerabilities when security patches are not available include:

a. controls to resolve the vulnerability:
    1) disable the functionality associated with the vulnerability though product configuration
    2) ask the vendor for an alternative method of managing the vulnerability
    3) move to a different product with a more responsive vendor, or
    4) engage a software developer to correct the software
b. controls to prevent exploitation of the vulnerability:
    1) apply external input sanitisation (if an input triggers the exploit)
    2) apply filtering or verification on the software output (if the exploit relates to an information disclosure)
    3) apply additional access controls that prevent access to the vulnerability, or
    4) configure firewall rules to limit access to the vulnerable software

Continued on next page

c. controls to contain the exploit:
   1) apply firewall rules limiting outward traffic that is likely in the event of an exploitation
   2) apply mandatory access control preventing the execution of exploitation code, or
   3) set filesystem permissions preventing exploitation code from being written to disk; and
d. controls to detect attacks:
   1) deploy an IDS
   2) monitor logging alerts, or
   3) use other mechanisms as appropriate for the detection of exploits using the known vulnerability.

RATIONALE

Patching security vulnerabilities in products

6.1.109. The assurance provided by an evaluation is related to the date at which the results were issued. Over the course of a normal product lifecycle, patches could be released to address known security vulnerabilities. Applying these patches should be considered as part of an agency's overall risk management strategy.

Patching security vulnerabilities in evaluated high grade products

6.1.110. Given the potential threat vectors and the value of the information being protected, high grade products must not be patched by an agency without specific direction from DSD. If a patch is released for a high grade product, DSD will conduct an assessment of the patch and might revise the product's usage guidance. Likewise, for patches released for products containing cryptographic functionality, DSD will subsequently conduct an assessment of the cryptographic vulnerability and might revise usage guidance in the consumer guide for the product.

EXAMPLES

6.1.111. A vulnerability exists in the remote management interface for an agency server. No patch is available. As the remote management functionality is rarely used it is disabled to reduce the vulnerability.

6.1.112. A Web browser is susceptible to an ActiveX exploit. This functionality is not needed by the agency for Web browsing and is therefore disabled in the configuration of the browser.

6.1.113. A Web content management vendor has not released a patch for a product which is being used by an agency. Indications are that the vendor will not release a patch as they have other projects. A decision is made to move to another well-maintained Web content management product as patching support is desired by the agency.

6.1.114. An exploit in a Web form is found for a custom Web application developed in-house by an agency. The agency fixes the vulnerability by using a software developer that is familiar with the Web scripting language used by the application.

6.1.115. An agency's word processing software has a vulnerability where a malicious document can cause remote code execution. The vendor is unable to release a patch for at least another month. The risk exposure to the agency in the mean time is excessive and they deploy email filter software to convert documents to portable document format at the gateway/CDS preventing exploitation from outside the agency.

6.1.116. A common gateway/CDS interface application is susceptible to a buffer overflow when passed large arguments in the uniform resource locator for a webpage. The Web server software and reverse proxy are able to filter large uniform resource locators before they reach the application.

Product Maintenance and Repairs

PRINCIPLE

6.1.117. Maintenance of hardware can be undertaken by cleared and briefed maintenance personnel or by uncleared maintenance personnel with appropriate escorting.

OBJECTIVE

6.1.118. To ensure that uncleared personnel are not exposed to information they do not have a need-to-know when maintaining or repairing hardware products.

CONTEXT

Scope

6.1.119. This section covers information on maintaining and repairing both evaluated and non-evaluated hardware products.

Maintaining and repairing UNCLASSIFIED hardware

6.1.120. Agencies can choose the most appropriate method to repair and maintain UNCLASSIFIED hardware products as long as due care is taken to protect the information on the hardware.

RISKS

6.1.121. An uncleared technician undertaking maintenance or repairs on a hardware product is exposed to information they do not need-to-know.

6.1.122. An uncleared technician while undertaking maintenance or repairs on a hardware products, gains an understanding of the capability or purpose of the product.

6.1.123. An uncleared technician undertaking maintenance or repair to a hardware product is not properly supervised, allowing unmonitored access to information they do not have a need-to-know.

6.1.124. A cleared technician conducting off-site maintenance or repairs on a hardware product is not able to provide sufficient protection and storage for the product out of business hours, resulting in exposure or unrestricted access by uncleared personnel.

6.1.125. A technician repairing ICT hardware notices it is used in a secure environment and while undertaking off-site repairs modifies the hardware for malicious purposes.

CONTROLS

[–,IC-HP,R-TS] Maintenance and repairs

6.1.126. Maintenance and repairs for hardware products containing security classified media **should** be carried out on-site by an appropriately cleared technician.

[–,IC-HP,R-TS] Maintenance and repairs by an uncleared technician

6.1.127. If an uncleared technician is used to undertake maintenance or repairs of a hardware product, on-site or off-site, the technician **must** be escorted by someone who:

a. is appropriately cleared and briefed
b. takes due care to ensure that security classified information is not disclosed
c. takes all responsible measures to ensure the integrity of the product
d. has the authority to direct the technician, and
e. is familiar with the security requirements relating to the repair of security classified products.

6.1.128. Agencies **should** sanitise and reclassify or declassify hardware products and associated media before maintenance or repair work is undertaken by an uncleared technician.

6.1.129. Agencies **should** ensure that the ratio of escorts to uncleared technicians allows for an appropriate oversight of all activities.

[–,HP,C-TS] Maintenance and repairs by an uncleared technician

6.1.130. If an uncleared technician is used to undertake maintenance or repairs of a hardware product, on-site or off-site, the technician **should** be escorted by someone who is sufficiently familiar with the product to understand the work being performed.

[–,IC-HP,R-TS] Off-site maintenance and repairs

6.1.131. Agencies having hardware products maintained or repaired off-site **must** ensure that the physical transfer, processing and storage requirements are appropriate for the security classification of the product, as defined by the PSM, and are maintained at all times.

GUIDANCE

[–,IC-HP,R-TS] Maintenance and repairs by an uncleared technician

6.1.132. It is **recommended** that agencies conceal the origin and nature of hardware products when maintenance or repairs are undertaken.

[–,IC-P,R] Maintenance and repairs by an uncleared technician

6.1.133. It is **recommended** that if an uncleared technician is used to undertake maintenance or repairs of a hardware product, on-site or off-site, the technician is escorted by someone who is sufficiently familiar with the product to understand the work being performed.

[–,HP,C-TS] Maintenance and repair of hardware from secured spaces

6.1.134. It is **recommended** that agencies having hardware maintained or repaired off-site treat the hardware as per the requirements for the highest security classification processed, stored or communicated in the area that the hardware being maintained or repaired will be returned to.

RATIONALE

Maintenance and repairs

6.1.135. Using cleared technicians on-site at an agency's facilities is considered the most desired approach to maintaining and repairing hardware products. This ensures that if information is disclosed during the course of maintenance or repairs the technicians are aware of the protection requirements for the information.

Maintenance and repairs by an uncleared technician

6.1.136. Agencies choosing to use uncleared technicians to maintain or repair hardware products on-site at an agency's facilities, or off-site at a company's facilities, need to be aware of the requirement for cleared personnel to escort the uncleared technicians during maintenance or repair activities.

Off-site maintenance and repairs

6.1.137. Agencies choosing to have hardware products maintained or repaired off-site need to be aware of additional requirements for the company's off-site facilities to be approved to process and store the products at the appropriate security classification as specified by PSM requirements.

6.1.138. Agencies choosing to have hardware products maintained or repaired off-site can sanitise, declassify or lower the security classification of the product prior to transport and subsequent maintenance or repair activities, to lower the physical transfer, processing and storage requirements as specified by the PSM.

Product Sanitisation and Disposal

PRINCIPLE

6.1.139. Product sanitisation and disposal is to be undertaken in an approved manner.

OBJECTIVE

6.1.140. To ensure that hardware products are not disposed of in a manner that compromises information or capabilities.

CONTEXT

Scope

6.1.141. This section covers information on sanitising and disposing of both evaluated and non-evaluated hardware products. Additional information on the sanitisation, destruction and disposal of media can be found in the *Media Security* chapter of this manual.

6.1.142. Security classified media typically found within hardware products are electrostatic memory devices such as laser printer cartridges and photocopier drums, non-volatile magnetic memory such as hard disks, non-volatile semi-conductor memory such as flash cards and volatile memory such as random access memory (RAM) cards.

RISKS

6.1.143. An agency fails to sanitise and declassify media contained in a hardware product before disposal, resulting in the unexpected disclosure of information to the subsequent owner of the product.

6.1.144. An agency fails to sanitise and declassify printer cartridges or copier drums contained in a hardware product before disposal, resulting in the unexpected disclosure of information to the subsequent owner of the product.

6.1.145. The improper disposal of a high grade product or HGCE results in a attacker gaining detailed insight into how to successfully exploit the product.

6.1.146. The improper disposal of TEMPEST rated equipment results in a breach of product licensing requirements and intellectual property of the vendor.

6.1.147. The improper disposal of TEMPEST rated equipment results in the product not being properly sanitised.

CONTROLS

[–,IC-HP,R-TS] Sanitisation or destruction of hardware products

6.1.148. Agencies **must** sanitise or destroy and declassify hardware products containing security classified media to UNCLASSIFIED before disposal.

6.1.149. Agencies **should** return hardware products and associated media that have processed or stored AUSTEO or AGAO information to Australia for sanitisation or destruction, declassification and disposal.

[U,IC-HP,R-TS] Disposal of hardware products

6.1.150. Agencies **must** have a documented process for the disposal of hardware products.

6.1.151. Agencies **must** contact DSD for advice on the disposal of high grade products.

6.1.152. Agencies are **required** to contact DSD for advice on the disposal of HGCE.

6.1.153. Agencies **must** formally authorise the disposal of hardware products, or waste, into the public domain.

[U,IC-HP,R-TS] Sanitising printer cartridges and copier drums

6.1.154. Agencies **must** print at least three pages of random text with no blank areas on each colour printer cartridge or copier drum.

[U,IC-HP,R-TS] Destroying printer cartridges and copier drums

6.1.155. Agencies unable to sanitise printer cartridges or copier drums **must** destroy the cartridge or drum in accordance with the requirements for electrostatic memory devices.

[U,IC-HP,R-TS] Sanitising video screens

6.1.156. Agencies **must** visually inspect video screens by turning up the brightness to the maximum level to determine if any information has been burnt into the screen. If the functionality exists, alter the intensity on a colour-by-colour basis.

[U,IC-HP,R-TS] TEMPEST rated equipment

6.1.157. Agencies **should** reuse TEMPEST rated equipment within the agency, or offer the equipment to another agency for reuse when it is no longer needed.

6.1.158. Agencies **must** contact DSD for advice regarding the disposal of TEMPEST rated equipment or if the equipment is non-functional.

RATIONALE

Disposal of hardware products

6.1.159. When disposing of hardware products, agencies need to sanitise or destroy and subsequently declassify any media within the product that are capable of storing information. Once the media have been removed from the product it can be considered sanitised. Following subsequent approval for declassification from the owner of the information previously processed by the product, it can be disposed of by the agency.

6.1.160. DSD provides specific advice on how to securely dispose of high grade products and HGCE. There are a number of security risks that can occur due to improper disposal including providing an attacker with an opportunity to gain insight into Australian Government capabilities.

TEMPEST rated equipment

6.1.161. There are two main considerations for the disposal of TEMPEST rated equipment—cost and abiding by any licensing agreement entered into with the vendor.

6.1.162. TEMPEST rated equipment is expensive to purchase and when it is no longer needed it should be reused within the agency, or by another agency. If the equipment cannot be redeployed, or is not functioning correctly, DSD will provide advice on the requirements for its repair or sanitisation and disposal.

Media Security

Media Handling

PRINCIPLE

6.2.1. Classifying, labelling and registering media assists in properly identifying and accounting for media.

OBJECTIVE

6.2.2. To ensure that system users are aware of the appropriate procedures for using media.

CONTEXT

Scope

6.2.3. This section covers information relating to classifying, labelling and registering media. Information relating to classifying and labelling hardware can be found in the *Product Classifying and Labelling* section of this manual.

Media reclassification and declassification process

6.2.4. When reclassifying or declassifying media the process is based on an assessment of relevant issues, including:

- the consequences of damage from unauthorised disclosure or misuse
- the effectiveness of any sanitisation or destruction procedure used, and
- the intended destination of the media.

Exceptions for labelling and registering media

6.2.5. Labels are not needed for internally mounted fixed media if the hardware containing the media is labelled. Likewise fixed media does not need to be registered if the hardware containing the media is registered.

RISKS

6.2.6. An attacker gains access to media that is unlabelled, where the media actually contains information, resulting in the disclosure of such information.

6.2.7. An attacker gains access to media that is labelled and protected at a lower security classification than that of the information it contains, resulting in the disclosure of such information.

6.2.8. An attacker gains access to media that has not been correctly sanitised and subsequently recovers and accesses its contents, resulting in the disclosure of information.

6.2.9. An attacker takes possession of removable media containing information without an agency's knowledge, resulting in the agency being unaware that such information has been disclosed.

6.2.10. An agency excessively classifies media without considering the security classification of information stored on the media, resulting in unnecessary controls being enforced on the usage, distribution and storage of the media.

CONTROLS

[U,IC-HP,R-TS] Reclassification and declassification procedures

6.2.11. Agencies **must** document procedures for the reclassification and declassification of media.

[U,IC-HP,R-TS] Classifying media storing information

6.2.12. Agencies **must** classify media, including both non-volatile and volatile media, to the highest security classification stored on the media since any previous reclassification.

[U,IC-P,R] Classifying media connected to systems of higher security classifications

6.2.13. Agencies **should** classify any media connected to, or inserted into, a system of a higher security classification as the system security classification, including any caveats, until confirmed not to be the case.

[–,HP,C-TS] Classifying media connected to systems of higher security classifications

6.2.14. Agencies **must** classify any media connected to, or inserted into, a system of a higher security classification as the system security classification, including any caveats, until confirmed not to be the case.

[–,IC-P,R] Classifying media below that of the system

6.2.15. Agencies intending to classify media below the security classification of the system to which it is connected or inserted into **should** ensure that:

a. the media is read-only
b. the media is inserted into a read-only device
c. the system has a mechanism through which read-only access can be assured, or
d. an accredited process is used to determine the security classification.

[–,HP,C-TS] Classifying media below that of the system

6.2.16. Agencies intending to classify media below the security classification of the system to which it is connected or inserted into **must** ensure that:

a. the media is read-only
b. the media is inserted into a read-only device,
c. the system has a mechanism through which read-only access can be assured, or
d. an accredited process is used to determine the security classification.

[U,IC-HP,R-TS] Lowering security classifications for media connecting to systems

6.2.17. Any process used to confirm the lower security classification of media connected to, or inserted into a system **must** be reviewed during the system's accreditation.

[–,IC-HP,R-TS] Declassifying media

6.2.18. Agencies wishing to declassify security classified media **must** ensure that:

a. the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed to UNCLASSIFIED, and
b. a formal administrative decision is made to release the media into the public domain.

[–,IC-HP,R-TS] Reclassifying media to a lower security classification

6.2.19. Agencies wishing to reclassify security classified media to a lower security classification **must** ensure that:

a. the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed, and
b. a formal administrative decision is made to reclassify the media.

[U,IC-HP,R-TS] Reclassifying media to a higher security classification

6.2.20. Agencies **must** reclassify media if:

a. information copied onto the media is of a higher security classification, or
b. information contained on the media is subjected to a security classification upgrade.

[U,IC-HP,R-TS] Labelling media

6.2.21. Agencies **should** label media with a marking that indicates the maximum security classification and set of caveats applicable to the information it stores.

[U,IC-HP,R-TS] Identifying labelled media

6.2.22. Agencies **must** ensure that the security classification of all media is easily visually identifiable.

6.2.23. When using non-textual protective markings due to operational security reasons, agencies **must** document the labelling scheme and train personnel appropriately.

[–,–,S-TS] Labelling sanitised media

6.2.24. Agencies **must** label non-volatile media that has been sanitised and reclassified with a notice similar to:

> 'Warning: media has been sanitised and reclassified from
> [security classification] to [security classification].
> Further lowering of security classification only via destruction.'

[–,HP,C-TS] Registering media

6.2.25. Agencies **should** register all media with a unique identifier in an appropriate register.

GUIDANCE

[U,IC-HP,R-TS] Labelling media

6.2.26. It is **recommended** that agencies, where possible, label media so that the security classification is visible when the media is mounted in the hardware in which it is used and when it has been removed.

[U,IC-P,R] Registering media

6.2.27. It is **recommended** that agencies register all media with a unique identifier in an appropriate register.

RATIONALE

Classifying media storing information

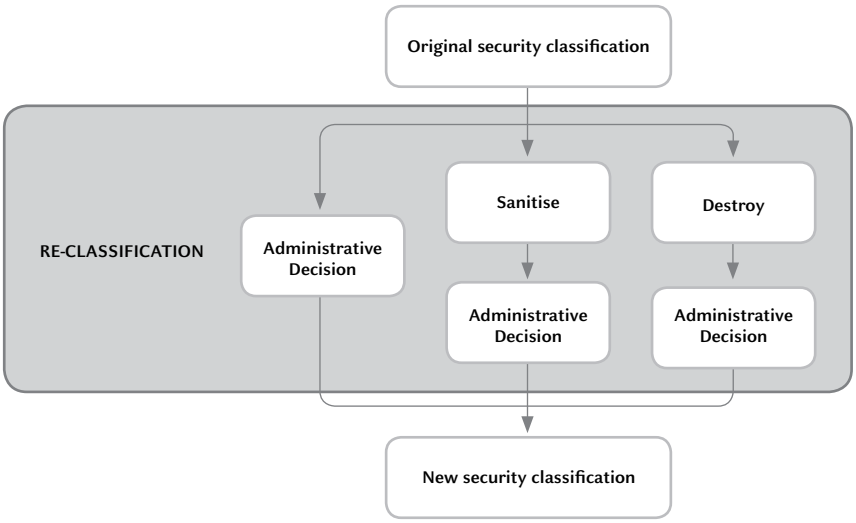
6.2.28. Media that is not correctly classified can be stored, identified and handled inappropriately or accessed by a person who does not have the appropriate security clearance.

Classifying media connecting to systems

6.2.29. Unless confirmed, there is no guarantee that information was not copied to the media while it was connected to a system.

Reclassifying media

6.2.30. The following diagram shows an overview of the mandated reclassification process.



Labelling media

6.2.31. Labelling helps all personnel to identify the security classification of media and ensure that they afford the media the correct protection measures.

Labelling sanitised media

6.2.32. It is not possible to sanitise and subsequently reclassify TOP SECRET non-volatile media.

REFERENCES

6.2.33. Additional information relating to media handling is contained in AS/NZS ISO/IEC 17799:2001, 10.7, *Media Handling*.

EXAMPLES

6.2.34. The security classification of a flash memory device is upgraded when:

- information of a higher security classification is transferred to the device
- the device is connected to a system that processes information at a higher security classification than that of the device, or
- the information on the device is subject to a security classification upgrade.

6.2.35. Personnel use a SECRET flash memory device to store information during military exercises. Following the completion of the exercises the information owner notifies personnel using the device that the information can be treated as RESTRICTED. A formal administrative decision is made to reclassify the media to a lower security classification and as a result the media is relabelled, with all registers containing the media appropriately updated.

Media Usage

PRINCIPLE

6.2.36. The likelihood of unauthorised exfiltration of data from a system is reduced by storing, registering and controlling connections to the system.

OBJECTIVE

6.2.37. To ensure that media is handled in an appropriate manner and agencies are aware of requirements for connecting peripherals to systems.

CONTEXT

Scope

6.2.38. This section covers information on using removable media. Agencies will also need to meet the requirements for automated data import and data export in addition to those outlined in this section when conducting manual data transfers.

RISKS

6.2.39. Personnel are exposed to information or equipment for which they do not have a need-to-know.

6.2.40. An attacker connects flash memory media, a FireWire capable device or inserts optical media into a system that contains a program designed to execute under the automatic execution feature of an operation system, which subsequently compromises the system by executing malicious code or undertaking malicious actions.

6.2.41. An attacker connects flash memory media or a FireWire capable device to a system in order to copy information from the system to their device.

6.2.42. An attacker connects a FireWire capable device to a system in order to use direct memory access and gain access to the system.

6.2.43. Security classified information on removable media is transferred unencrypted through an area not certified to process the information (e.g. public facility), the media is accidentally misplaced and the information is subsequently disclosed into the public domain.

6.2.44. Personnel conduct a manual data transfer using removable media of a higher security classification than either of the systems involved is accredited to process, causing a data spill.

CONTROLS

[U,IC-HP,R-TS] Using removable media with systems

6.2.45. Agencies **must not** use removable media containing security classified information with a system that has a lower security classification than the media.

[–,IC-HP,R-TS] Storage of removable media

6.2.46. Agencies **must** ensure that removable media containing security classified information meets the minimum physical security storage requirements as specified in the PSM.

[–,IC-HP,R-TS] Removable media storage devices

6.2.47. Storage devices holding removable media **must** meet the minimum physical security storage requirements as specified in the PSM.

[U,IC-HP,R-TS] Connecting removable media to systems

6.2.48. Agencies **must** disable any automatic execution features within operating systems for connectable devices and removable media.

6.2.49. Agencies **must** prevent unauthorised removable media from connecting to a system via the use of device access control software, seals, physical means or other methods approved by the accreditation authority.

6.2.50. When writable removable media is connected to, or inserted into, a writable communications port or device, agencies **should** implement controls to prevent the unintended writing of data to the media.

[U,IC-P,R] IEEE 1394 interface connections

6.2.51. Agencies **should** disable IEEE 1394 interfaces (e.g. FireWire ports) using device access control software, seals or physical mechanisms.

[–,HP,C-TS] IEEE 1394 interface connections

6.2.52. Agencies **must** disable IEEE 1394 interfaces (e.g. FireWire ports) using device access control software, seals or physical mechanisms.

[–,IC-HP,R-TS] Transferring removable media

6.2.53. Agencies **must** ensure that removable media containing security classified information meets the minimum physical transfer requirements as specified in the PSM.

6.2.54. Agencies **should** encrypt any removable media with at least a DSD approved cryptographic algorithm (DACA) if it is to be transferred through an area not certified to process information of a security classification contained on the media.

[–,–,TS] Removable media

6.2.55. Agencies **must not** permit any removable media that uses external interface connections within a TOP SECRET area without prior written approval from the accreditation authority.

[U,IC-HP,R-TS] Air gapped transfers

6.2.56. Agencies transferring data manually between two systems **should**:

a. use previously unused removable media or removable media items used only for data transfer between the two relevant systems, and
b. ensure that the removable media is sufficiently sanitised to permit its reuse on the less security classified of the two systems.

RATIONALE

Storage of removable media

6.2.57. The security requirements for storage and physical transfer of information and equipment are specified in the PSM.

Connecting removable media to systems

6.2.58. Some operating systems provide the functionality to automatically execute certain types of programs that reside on optical media and devices such as flash memory media. While this functionality was designed with a legitimate purpose in mind, such as automatically loading a graphical user interface for the system user to browse the contents of the media, or to install software residing on the media, it can also be used for malicious purposes.

6.2.59. An attacker can create a file on optical media or a connectable device that the operating system believes it should automatically execute. However, when the operating system executes the file, it can have the same effect as when a system user explicitly executes malicious code. However, in this case the system user is taken out of the equation as the operating system executes the file without explicitly asking the system user for permission.

6.2.60. Some operating systems will cache information on media to improve performance. As such, inserting media of a higher security classification into a system of a lower security classification or no security classification could cause data to be read from the device without user intervention.

6.2.61. Using device access control software will prevent unauthorised removable media from being attached to a system. Using a whitelisting approach allows agency information security personnel greater control over what can, and what cannot, be connected to the system.

IEEE 1394 interface connections

6.2.62. Known vulnerabilities have been demonstrated where attackers can connect a FireWire capable device to a locked workstation and modify information in RAM to gain access to encryption keys. Furthermore, as FireWire provides direct memory access to the system memory an attacker can read or write any content to memory that they desire. The best defence against this vulnerability is to disable access to FireWire ports using either software controls or physically damaging the FireWire ports so that devices cannot be connected.

Transferring removable media

6.2.63. As removable media is often transferred through areas not certified to process the security classified information on the media, protection mechanisms need to be put in place to protect the information. As the PSM requirements for the physical transfer of security classified information are based on paper-based material and not electronic-based material the security risk is vastly different.

6.2.64. When agencies apply encryption to removable media devices it may reduce the requirements for storage and physical transfer as outlined in the PSM. The application of encryption does not automatically render the device UNCLASSIFIED. The reduction of any requirements is based on the original security classification of information residing on the removable media and the level of assurance in the cryptographic product being used to encrypt the media.

6.2.65. Further information on reducing storage and physical transfer requirements can be found in the *Cryptographic Fundamentals* section within this manual.

Removable media

6.2.66. Ensuring certain types of removable media including USB, FireWire and eSATA capable devices must be explicitly approved in a TOP SECRET environment. This provides an additional level of system user awareness and security. This practice should be used in addition to device access control software on workstations in case system users are unaware of, or choose to ignore, security requirements for removable media.

Air gapped transfers

6.2.67. Using removable media that is previously unused or completely sanitised prevents information from being accidentally disclosed, especially between systems of differing security classifications, as well as protecting against malicious code execution.

Media Sanitisation

PRINCIPLE

6.2.68. Sanitising media reduces the security risk of unauthorised access to security classified information.

OBJECTIVE

6.2.69. To ensure that media is sanitised in accordance with approved methods prior to reuse or disposal.

CONTEXT

Scope

6.2.70. This section covers information relating to sanitising media. Information relating to sanitising hardware can be found in the *Product Sanitisation and Disposal* section of this manual.

Sanitising media

6.2.71. The process of sanitisation does not automatically change the security classification of the media, nor does sanitisation involve the destruction of media.

Factors to be considered when sanitising media

6.2.72. When agencies choose to sanitise media a number of factors can be considered, including the following.

- Does an approved sanitisation procedure exist for the specific media involved?
- What are the relative costs of sanitising versus destroying (and replacing where necessary) the media?
- What is the security classification and sensitivity of the data?
- What is the acceptable level of security risk associated with the recovery of data from the media following declassification?
- Is the media defective and sanitisation prohibited?

Hybrid hard drives

6.2.73. When agencies use hybrid hard drives the sanitisation and post sanitisation treatment requirements for flash memory devices of the same capacity apply.

Solid state drives

6.2.74. When agencies use solid state drives the sanitisation and post sanitisation treatment requirements for flash memory devices of the same capacity apply.

RISKS

6.2.75. An attacker gains access to media that has previously stored information and that has failed to undergo appropriate sanitisation, enabling the recovery of information.

6.2.76. An attacker gains access to media where an agency had not verified the overwrite during the sanitisation process and the overwrite has failed to remove information, resulting in the disclosure of information.

6.2.77. An attacker gains access to volatile media within a specified timeframe following removal of power, allowing them to recover information prior to complete information decay.

6.2.78. An attacker gains access to media where an agency had used an approved method to sanitise magnetic media containing information, however some information remained in bad sectors not accessible during the sanitisation process, resulting in the disclosure of the information.

6.2.79. An attacker uses specialised recovery techniques on an agency sanitised erasable programmable read-only memory (EPROM) that has been exposed to ultraviolet light but was not overwritten with a pseudo random pattern, resulting in the recovery of information.

6.2.80. An attacker uses specialised recovery techniques where an agency has sanitised the electrically erasable programmable read-only memory (EEPROM) by erasing the media rather than overwriting the media with a pseudo random pattern, resulting in the disclosure of information.

6.2.81. An attacker gains access to unsanitised volatile media, which has been used to store static information for an extended period of time, and analyses the characteristics of the memory to retrieve information.

6.2.82. An attacker gains access to flash memory media where an agency has used an approved method to sanitise the media, however some information remained in free blocks (as a result of wear levelling) and was not accessed during the sanitisation process, resulting in the disclosure of the information.

CONTROLS

[U,IC-HP,R-TS] Sanitisation procedures

6.2.83. Agencies **must** document procedures for the sanitisation of media.

[–,–,TS] Sanitisation procedures

6.2.84. As part of the media sanitisation process agencies **must** conduct a security risk assessment to determine the security risks associated with reclassifying TOP SECRET media.

[U,–,–] Media that cannot be sanitised

6.2.85. Agencies **should** destroy the following media types prior to disposal, as they cannot be sanitised:

a. microfiche
b. microfilm
c. optical discs
d. printer ribbons and the impact surface facing the platen
e. programmable read-only memory
f. read-only memory, and
g. faulty media that cannot be successfully sanitised.

[–,IC-HP,R-TS] Media that cannot be sanitised

6.2.86. Agencies **must** destroy the following media types prior to disposal, as they cannot be sanitised:

a. microfiche
b. microfilm
c. optical discs
d. printer ribbons and the impact surface facing the platen
e. programmable read-only memory
f. read-only memory, and
g. faulty media that cannot be successfully sanitised.

[U,IC-HP,R-TS] Product selection

6.2.87. Agencies are permitted to use non-evaluated products to sanitise media, however, the product **must** conform with the requirements for sanitising media as outlined in this section.

[U,IC-P,R] Volatile media sanitisation

6.2.88. Agencies **must** sanitise volatile media by:

a. removing power from the media for at least 10 minutes, or
b. overwriting all locations of the media with an arbitrary pattern followed by a read back for verification.

[–,HP,C-TS] Volatile media sanitisation

6.2.89. Agencies **must** sanitise volatile media by overwriting the media at least once in its entirety with an arbitrary pattern, followed by a read back for verification, followed by removing power from the media for at least 10 minutes.

[U,IC-HP,R-TS] Treatment of volatile media following sanitisation

6.2.90. Following sanitisation, volatile media **must** be treated as indicated in the table below.

PRE-SANITISATION SECURITY CLASSIFICATION	POST-SANITISATION SECURITY CLASSIFICATION
• TOP SECRET	• UNCLASSIFIED (under certain circumstances)
• SECRET • CONFIDENTIAL • HIGHLY PROTECTED • PROTECTED • RESTRICTED • X-IN-CONFIDENCE • UNCLASSIFIED	• UNCLASSIFIED

[–,–,TS] Circumstances preventing reclassification of TOP SECRET volatile media

6.2.91. Volatile media **must not** be reclassified below TOP SECRET if the volatile media:

a. stored sensitive, static, data for an extended period of time, and
b. sensitive data was repeatedly stored or written to the same location on the volatile media for an extended period of time.

[U,IC-HP,R-TS] Non-volatile magnetic media sanitisation

6.2.92. Agencies **must** sanitise non-volatile magnetic media by:

a. overwriting the media, if pre-2001 or under 15GB, at least three times in its entirety, with an arbitrary pattern followed by a read back for verification
b. overwriting the media, if post-2001 or over 15GB, at least once in its entirety, with an arbitrary pattern followed by a read back for verification, or
c. using an approved degausser.

[–,HP,C-TS] Non-volatile magnetic media sanitisation

6.2.93. When sanitising non-volatile magnetic media agencies **must** determine if the media contains bad sectors and if present, perform a security risk assessment which determines the security risk of residual data remaining on the media prior to reuse or disposal.

[U,IC-HP,R-TS] Treatment of non-volatile magnetic media following sanitisation

6.2.94. Following sanitisation, non-volatile magnetic media **must** be treated as indicated in the table below.

PRE-SANITISATION SECURITY CLASSIFICATION	POST-SANITISATION SECURITY CLASSIFICATION
• TOP SECRET	• TOP SECRET
• SECRET	• CONFIDENTIAL
• CONFIDENTIAL • HIGHLY PROTECTED • PROTECTED • RESTRICTED • UNCLASSIFIED	• UNCLASSIFIED

[U,IC-HP,R-TS] Non-volatile EPROM media sanitisation

6.2.95. Agencies **must** sanitise non-volatile EPROM media by erasing as per the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

[U,IC-HP,R-TS] Non-volatile EEPROM media sanitisation

6.2.96. Agencies **must** sanitise non-volatile EEPROM media by overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

[U,IC-HP,R-TS] Treatment of non-volatile EPROM and EEPROM media following sanitisation

6.2.97. Following sanitisation, non-volatile EPROM and EEPROM media **must** be treated as indicated in the table below.

PRE-SANITISATION SECURITY CLASSIFICATION	POST-SANITISATION SECURITY CLASSIFICATION
• TOP SECRET	• TOP SECRET
• SECRET	• CONFIDENTIAL
• CONFIDENTIAL • HIGHLY PROTECTED • PROTECTED • RESTRICTED • X-IN-CONFIDENCE • UNCLASSIFIED	• UNCLASSIFIED

[U,IC-HP,R-TS] Non-volatile flash memory media sanitisation

6.2.98. Agencies **must** sanitise non-volatile flash memory media by overwriting the media at least twice in its entirety with a pseudo random pattern, followed by a read back for verification.

[U,IC-HP,R-TS] Treatment of non-volatile flash memory media following sanitisation

6.2.99. Following sanitisation, non-volatile flash memory media **must** be treated as indicated in the table below.

PRE-SANITISATION SECURITY CLASSIFICATION	POST-SANITISATION SECURITY CLASSIFICATION
• TOP SECRET	• TOP SECRET
• SECRET	• SECRET
• CONFIDENTIAL	• CONFIDENTIAL
• HIGHLY PROTECTED	• HIGHLY PROTECTED
• PROTECTED • RESTRICTED • X-IN-CONFIDENCE • UNCLASSIFIED	• UNCLASSIFIED

[U,IC-HP,R-TS] Degaussers

6.2.100. Agencies **should** use a degausser approved by DSD and comply with any directions for its use.

6.2.101. Agencies **must** use a degausser of sufficient field strength for the coercivity of the media during sanitisation as outlined in the National Security Agency/Central Security Service's EPLD.

6.2.102. Agencies **must** use a degausser which has been evaluated as capable for the magnetic orientation (longitudinal or perpendicular) of the media being sanitised.

6.2.103. Agencies **must** comply with the directions provided in the National Security Agency/Central Security Service's EPLD when using a degausser from the list.

GUIDANCE

[U,IC-HP,R-TS] Sanitising media prior to reuse

6.2.104. It is **recommended** that agencies sanitise all media prior to reuse at the same or higher security classification.

[U,IC-HP,R-TS] Degaussers

6.2.105. It is **recommended** that agencies consult DSD where directions provided in the EPLD appear to conflict with this manual.

[U,IC-HP,R-TS] Verifying sanitised media

6.2.106. It is **recommended** that agencies verify the sanitisation of media using a different product from the one used to perform the initial sanitisation.

RATIONALE

Sanitisation procedures

6.2.107. Sanitising media prior to reuse in a different environment ensures that information is not inadvertently accessed by an unauthorised individual or protected by insufficient security measures.

6.2.108. Using approved sanitisation methods provides a high level of assurance that no remnant data is on the media.

6.2.109. The procedures used in this manual are designed not only to prevent common attacks that are currently feasible but also to protect from threats that could emerge in the future.

6.2.110. When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process completed successfully.

Media that cannot be sanitised

6.2.111. Some types of media cannot be sanitised and therefore must be destroyed. It is not possible to use these types of media while maintaining a high level of assurance that no previous data can be recovered.

Volatile media sanitisation

6.2.112. When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to research on recovering the contents of volatile media.

Treatment of volatile media following sanitisation

6.2.113. There is published literature that supports short-term remanence effects in volatile media. Data retention time is reported to be in the magnitude of minutes (at normal room temperatures) to hours (in extreme cold), depending on the temperature of the volatile media. Further, published literature has shown that some volatile media can suffer from long-term remanence effects resulting from physical changes to the media due to continuous storage of static data for an extended period of time. It is for these reasons that under certain circumstances TOP SECRET volatile media must always remain at this security classification, even after sanitisation.

6.2.114. For example, in the following scenarios TOP SECRET volatile media must not be reclassified.

a. A static cryptographic key is stored in the same memory location in volatile media during every boot of a device.
b. A static image is displayed on a device and stored in volatile media for a period of months.

Treatment of non-volatile magnetic media following sanitisation

6.2.115. Modern magnetic media automatically reallocates space for bad sectors. These bad sectors are maintained in what is known as a 'G-list'. If information was stored in a sector that is subsequently added to the G-list, sanitising the media will not overwrite these non-addressable bad sectors. Information will therefore remain on the media. It is for these reasons that TOP SECRET and SECRET magnetic media cannot be sanitised below TOP SECRET and CONFIDENTIAL respectively.

Non-volatile flash memory media sanitisation

6.2.116. Wear levelling ensures that writes are distributed evenly across each memory block in flash memory. This feature of the algorithm therefore necessitates the need for flash memory to be overwritten with a pseudo random pattern twice, rather than once, as this helps to ensure that all memory blocks are overwritten during sanitisation.

Treatment of non-volatile flash memory media following sanitisation

6.2.117. Due to the use of wear levelling in flash memory, it is possible that not all physical memory locations are written to when attempting to overwrite the media. Information can therefore remain on the media. It is for these reasons that TOP SECRET, SECRET, CONFIDENTIAL and HIGHLY PROTECTED flash memory media must always remain at their respective security classification, even after sanitisation.

Degaussers

6.2.118. DSD has approved the use of degausser products listed within the National Security Agency/Central Security Service's EPLD.

6.2.119. Coercivity varies between media types and between brands and models of the same type. Care is needed when determining the desired coercivity as a degausser of insufficient strength will not be effective.

6.2.120. Since 2006 perpendicular magnetic media have been available. Some degaussers are only capable of sanitising longitudinal magnetic media. As such care needs to be taken to ensure that a suitable degausser is used when sanitising perpendicular magnetic media.

REFERENCES

6.2.121. Additional information on the National Security Agency/Central Security Service's EPLD can be found at: http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

6.2.122. Further information on recoverability of information from volatile media can be found in the paper *Data Remanence in Semiconductor Devices* at: http://www.cypherpunks.to/~peter/usenix01.pdf.

6.2.123. The RAM testing tool memtest86+ can be obtained from: http://memtest.org.

6.2.124. The graphics processing unit (GPU) RAM testing tool Memtest80 can be obtained from: https://simtk.org/hom/memtest.

EXAMPLES

6.2.125. To reclassify PROTECTED volatile RAM to UNCLASSIFIED using sanitisation, simply remove the power for at least 10 minutes from the system in which the RAM resides. Once a formal administrative decision is made to reclassify the RAM it can be treated as UNCLASSIFIED.

6.2.126. To reclassify HIGHLY PROTECTED volatile RAM to UNCLASSIFIED using open source tools:

- remove all media except the RAM from the system
- configure the system to boot into memtest86+ from an optical disc
- run memtest86+, allowing it to complete and ensuring no errors are found
- shutdown the system and remove power for at least 10 minutes, then
- formally reclassify the media.

6.2.127. Note: memtest86+ is publicly available software designed to stress test a computer's RAM. It is available under the GNU General Public License.

6.2.128. Warning: The following examples should not be copied verbatim, as the destination drive (e.g. /dev/sda, /dev/sdd, etc) may be different depending on your system's configuration. Please note that writing to raw devices incorrectly will cause irrecoverable data loss, so please ensure that the correct device name is used.

6.2.129. To reclassify a SECRET non-volatile magnetic media hard drive to CONFIDENTIAL using a Linux operating system, or bootable Linux distribution such as Knoppix and open source tools:

- determine the destination drive (e.g. /dev/sda)
- run 'sudo bash'
- run 'dd if=/dev/zero of=/dev/sda bs=64k'
- check if any errors are reported, if so the drive could be defective and cannot be adequately reclassified
- run 'hd /dev/sda' and ensure that the entire device contains zeros, and
- determine if the media contains any bad sectors and if so conduct a security risk assessment before formally reclassifying the media, otherwise formally reclassify the media.

6.2.130. Hexdump (hd) will actually eliminate duplicate output lines and represent this duplication with a '*'. This makes manual, or scripted, inspection of a disk during verification easier.

6.2.131. To reclassify a RESTRICTED non-volatile flash memory device to UNCLASSIFIED using a Linux operating system, or bootable Linux distribution such as Knoppix and open source tools:

- determine the destination drive (e.g. /dev/sdd)
- run 'sudo bash'
- run 'fdisk -l /dev/sdd' which will show the size of the disk in bytes (the top line commencing with the word 'disk')
- run 'dd if=/dev/urandom bs=512 count=<size of device in bytes / 512> | tee /dev/sdd | md5sum' which will print a number of lines containing the amount of data read (this should match the size of the device), and finally a 32-character long string, which is the md5sum of the pseudo random stream
- run 'md5sum /dev/sdd'
- check this md5sum matches the 32-character string previously returned
- repeat all again for second pass, then
- formally reclassify the media.

6.2.132. To check for the existence of bad sectors (i.e. potentially security classified remnant data) on a non-volatile magnetic media hard drive using a bootable Linux distribution such as Knoppix:

- connect the hard drive to the system
- configure the system to boot into a bootable distribution such as Knoppix
- run 'sudo bash'
- determine the destination disk (e.g. /dev/sda)
- run 'smartctl –s on /dev/sda' to turn self-monitoring, analysis and report technology access on
- run 'smartctl –a /dev/sda –d ata | less'
- review the raw value for the attribute Reallocated_Sector_Ct, and
- check if the value is zero to ensure that there are no bad sectors on the hard drive.

6.2.133. To reclassify a TOP SECRET GPU to UNCLASSIFIED using open source tools:

- determine if the GPU was used under certain circumstances that prohibits reclassification to UNCLASSIFIED
- conduct a security risk assessment based on the previous function of the GPU
- remove all media except the RAM and the GPU from the system
- configure the system to boot into a utility such as MemtestG80 from an optical disc
- run Memtest80, allowing it to complete and ensure that no errors are found
- shutdown the system and remove power for at least 10 minutes, then
- formally reclassify the GPU.

6.2.134. If the GPU had been used under certain circumstances that prohibit its reclassification to UNCLASSIFIED, the GPU must be treated as TOP SECRET after sanitisation.

Media Destruction

PRINCIPLE

6.2.135. Media can be destroyed to the extent that the cost of analysis on the individual particles to obtain information far exceeds the potential value of the information.

OBJECTIVE

6.2.136. To ensure that prior to disposal if media is to be destroyed it is done using an approved method.

CONTEXT

Scope

6.2.137. This section covers information relating to the destruction of media. Information relating to the destruction of hardware can be found in the *Product Sanitisation and Disposal* section of this manual.

RISKS

6.2.138. An attacker or uncleared individual gains access to media that has been inadequately destroyed and recovers information.

6.2.139. An attacker or uncleared individual gains access to media containing information during the process of media destruction itself, resulting in the disclosure of the information.

CONTROLS

[U,IC-HP,R-TS] Destruction procedures

6.2.140. Agencies **must** document procedures for the destruction of media.

[U,IC-HP,R-TS] Media destruction

6.2.141. To destroy media, agencies **must**:

a. break up the media, or
b. heat the media until it has either burnt to ash or melted.

6.2.142. Agencies **must** employ equipment approved by the SCEC for the purpose of media destruction.

6.2.143. Agencies **must** use one of the methods shown in the table below.

ITEM	METHODS				
	FURNACE/ INCINERATOR	HAMMER MILL	DISINTEGRATOR	GRINDER/ SANDER	CUT
Electrostatic memory device	Yes	Yes	Yes	Yes	No
Floppy disk	Yes	Yes	Yes	No	Yes
Hard disk	Yes	Yes	Yes	Yes	No
Optical disk	Yes	Yes	Yes	Yes	Yes
Semi-conductor memory	Yes	Yes	Yes	No	No
Tape	Yes	Yes	Yes	No	Yes

[U,IC-P,R] Storage and handling of media waste particles

6.2.144. Agencies **must**, at a minimum, store and handle the resulting media waste for all methods, except for furnace/incinerator, as for the security classification given in the table below.

INITIAL MEDIA SECURITY CLASSIFICATION	SCREEN APERTURE SIZE PARTICLES CAN PASS THROUGH	
	≤ 9MM	≤ 12MM
UNCLASSIFIED	U	U
X-IN-CONFIDENCE	U	U
RESTRICTED	U	U
PROTECTED	U	IC

[–,HP,C-TS] Storage and handling of media waste particles

6.2.145. Agencies **must**, at a minimum, store and handle the resulting media waste for all methods, except for furnace/incinerator, as for the security classification given in the table below.

INITIAL MEDIA SECURITY CLASSIFICATION	SCREEN APERTURE SIZE PARTICLES CAN PASS THROUGH			
	≤ 3MM	≤ 6MM	≤ 9MM	≤ 12MM
HIGHLY PROTECTED	U	U	IC	P
CONFIDENTIAL	U	U	U	R
SECRET	U	U	R	C
TOP SECRET	U	R	C	S

[U,IC-HP,R-TS] Supervision of destruction

6.2.146. Agencies **must** perform the destruction of media under the supervision of personnel cleared to the highest security classification of the media being destroyed.

6.2.147. Personnel supervising the destruction of media **must**:

a. supervise the handling of the media to the point of destruction, and
b. ensure that the destruction is completed successfully.

[U,IC-HP,R-TS] Supervision of accountable material destruction

6.2.148. Agencies **must** perform the destruction of accountable material under the supervision of two personnel cleared to the highest level of the media being destroyed.

6.2.149. Personnel supervising the destruction of accountable media **must**:

a. supervise the handling of the material to the point of destruction
b. ensure that the destruction is completed successfully, and
c. sign a destruction certificate.

[U,IC-HP,R-TS] Outsourcing media destruction

6.2.150. Agencies **should not** outsource the destruction of TOP SECRET media or accountable material.

6.2.151. Agencies outsourcing the destruction of media to a commercial facility **must** use a facility that has been approved by ASIO T4 Protective Security.

GUIDANCE

[U,IC-HP,R-TS] Media destruction equipment

6.2.152. It is **recommended** that agencies contact ASIO for further information on the selection of protective security equipment used to destroy media.

RATIONALE

Media destruction

6.2.153. The destruction methods given are designed to ensure that recovery of data is impossible or impractical. ASIO T4 Protective Security maintains a list of businesses that are accredited to destroy media in an approved manner.

Storage and handling of media waste particles

6.2.154. Following destruction, normal accounting and auditing procedures do not apply for media items. As such, it is essential that when an item is recorded as being destroyed, destruction is assured.

Outsourcing media destruction

6.2.155. The requirements for outsourcing media destruction are a reflection of those from Part C of the PSM. Further requirements on the physical transfer of media between agencies and commercial facilities can be found in the PSM.

EXAMPLES

6.2.156. An agency determines that a PROTECTED hard disk drive is no longer needed. As part of the declassification process it is decided that the security risk associated with sanitising the drive and disposing of it in the public domain is not acceptable. As such, the decision is made to destroy the drive. A hammer mill is selected as the destruction method to shred the platter of the drive resulting in media waste particles that fit through a screen of less than or equal to 9mm. As such, an administrative decision is made to reclassify the media waste. The media waste can now be handled and treated as per the requirements for UNCLASSIFIED information. A formal administrative decision is then made to release the media waste into the public domain. The resultant media waste is disposed of in a way that does not attract undue attention and all applicable registers are updated.

6.2.157. An agency determines that a PROTECTED hard disk drive is no longer needed. As part of the declassification process it is decided that the security risk associated with sanitising the drive and disposing of it in the public domain is not acceptable. As such, the decision is made to destroy the drive. A hammer mill is selected as the destruction method to shred the platter of the hard disk drive resulting in media waste particles that fit through a screen of less than or equal to 12mm. As such, the media waste must be handled as stored as per the requirements of X-IN-CONFIDENCE information and is reclassified accordingly. At this stage the media waste is not suitable for public release as it is still security classified, as such the resulting media waste is then burnt until melted. At this stage, a decision is made to reclassify the media waste to UNCLASSIFIED. Following this reclassification to UNCLASSIFIED a decision is made to release the media waste into the public domain. The resultant media waste is then disposed of in a way that does not attract undue attention and all applicable registers are updated.

Media Disposal

PRINCIPLE

6.2.158. Disposing of media in accordance with approved processes reduces the risk of unauthorised access to information.

OBJECTIVE

6.2.159. To ensure that agencies follow a proper process for the disposal of media.

CONTEXT

Scope

6.2.160. This section covers information relating to the disposal of media. Information relating to the disposal of hardware can be found in the *Product Sanitisation and Disposal* section of this manual.

RISKS

6.2.161. An attacker or uncleared individual gains access to media that was disposed of while still containing information, resulting in the disclosure of the information.

6.2.162. An attacker or uncleared individual gains access to a faulty device that was disposed of without sanitisation and manages to repair the device, or directly recover data from it, resulting in the disclosure of information.

6.2.163. An attacker or uncleared individual gains access to media containing information that has not been approved for public release, resulting in the public disclosure of the information.

CONTROLS

[U,IC-HP,R-TS] Disposal procedures

6.2.164. Agencies **must** document procedures for the disposal of media.

[–,IC-HP,R-TS] Reclassifying prior to disposal

6.2.165. Agencies **must** reclassify all security classified media, including faulty media, to UNCLASSIFIED prior to making an administrative decision to formally authorise the disposal the media into the public domain.

[U,–,–] Sanitisation prior to disposal

6.2.166. Agencies **should** sanitise or destroy media that was not previously sanitised or destroyed as part of a reclassification process for security classified media.

[U,–,–] Disposal of media

6.2.167. Agencies **must** formally authorise the disposal of media and media waste into the public domain.

[U,–,–] Manner of disposal

6.2.168. Agencies **should** dispose of media and media waste in a manner that does not attract undue attention.

RATIONALE

Reclassifying prior to disposal

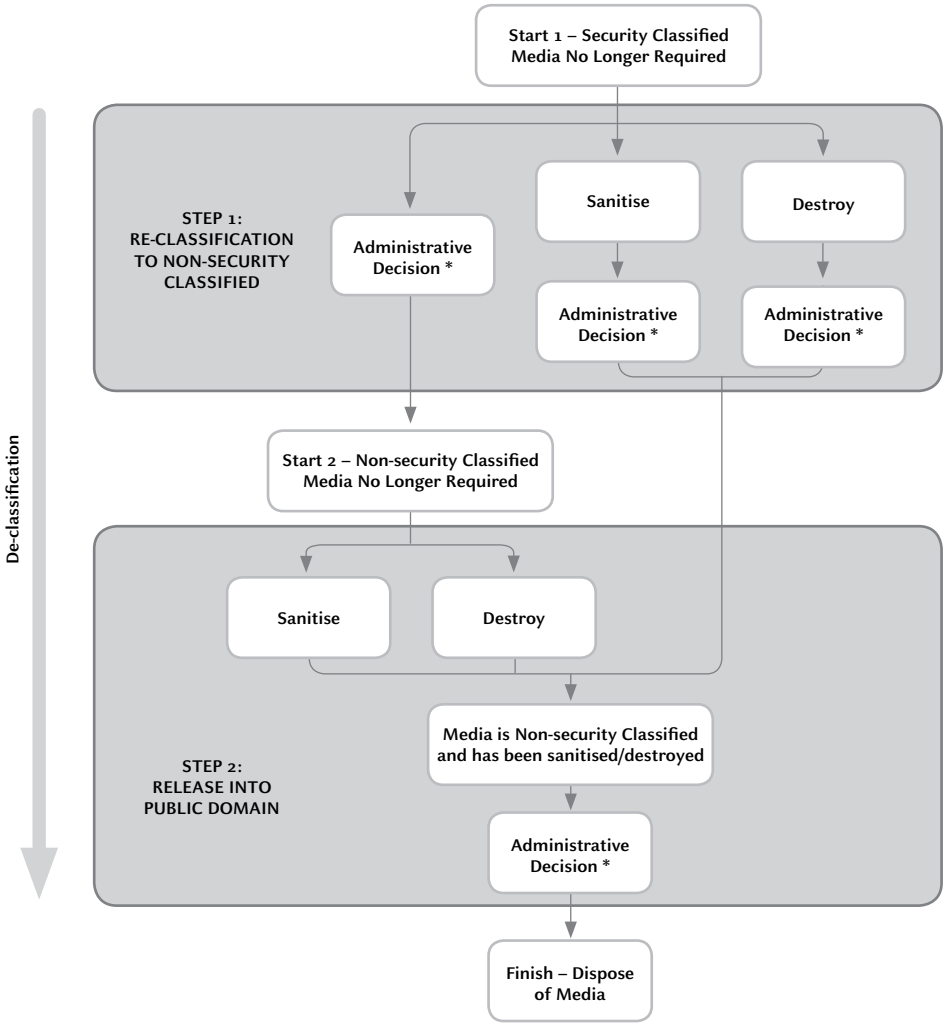
6.2.169. Prior to disposal security classified media needs to be reclassified to UNCLASSIFIED using sanitisation or destruction, as part of the declassification process, to ensure that security classified information is not accidentally released to the public.

Sanitisation prior to disposal

6.2.170. Media containing UNCLASSIFIED information is not automatically approved for public release. As such, sanitisation can be used to ensure that UNCLASSIFIED information is not released to the public without proper authorisation.

Disposal of media

6.2.171. The following diagram shows an overview of the mandated disposal process. In the diagram there are two starting points—one for security classified media and one for non-security classified media. Also note declassification is the entire process, including any reclassifications and administrative decisions, before media and media waste can be released into the public domain.



*See examples at the end of this section for explanation.

Manner of disposal

6.2.172. Disposing of media waste in a manner that does not attract attention ensures that destroyed media that was previously security classified is not subjected to additional scrutiny over that of regular waste.

EXAMPLES

6.2.173. An agency wishes to declassify an X-IN-CONFIDENCE flash memory device that is no longer needed. The declassification process, which includes the sanitisation and reclassification of the flash memory device, is undertaken. Once the flash memory device has been reclassified it can be handled and stored as per the requirements for UNCLASSIFIED devices. A formal administrative decision is then made to release the device into the public domain in a way that will not attract undue attention, and all applicable registers are updated.

6.2.174. An agency wishes to declassify an UNCLASSIFIED hard disk that is no longer needed. Reclassification of the media is not needed as it is not security classified. Since no previous sanitisation has occurred as a result of reclassification, the agency sanitises the hard disk. A formal administrative decision is then made to release the hard disk into the public domain in a way that will not attract attention, and all applicable registers are updated.

Software Security

Standard Operating Environments

PRINCIPLE

6.3.1. Unsecured and uncontrolled Standard Operating Environments (SOEs) are commonly exploited by attackers to gain unauthorised access to systems.

OBJECTIVE

6.3.2. To ensure that agency software fundamentals are based on hardening systems during installation, developing SOEs and establishing configuration baselines.

CONTEXT

Scope

6.3.3. This section covers information on the hardening of software used on workstations and servers.

Characterisation

6.3.4. Characterisation is a technique used to analyse and record a system's configuration. It is important as it can be used to verify the system's integrity at a later date.

6.3.5. Methods of characterising files and directories include:

- performing a cryptographic checksum on the files/directories when they are known to be virus/contaminant free
- documenting the name, type, size and attributes of legitimate files and directories, along with any changes to this information expected under normal operating conditions, or
- for a Windows system, taking a system difference snapshot.

RISKS

6.3.6. Personnel not adhering to, or not being aware of relevant information security policies and plans relating to their SOE, inadvertently allow or facilitate unauthorised access to a system.

6.3.7. An attacker exploits vulnerabilities relating to unused, unpatched, unnecessary or out-of-date information, accounts or software, to gain unauthorised access to a system.

6.3.8. Software running on a security classified network automatically connects to its vendor and downloads an unauthorised update, resulting in a weakening of the agency's information security posture.

6.3.9. An attacker exploits an agency's poor management of passwords to gain access to a system.

CONTROLS

[U,IC-HP,R-TS] Documentation

6.3.10. All server and workstation security objectives and mechanisms **should** be documented in the relevant SSP.

[U,IC-HP,R-TS] Workstation environments

6.3.11. Agencies **should** develop a hardened SOE for workstations, covering:

a. removal of unneeded software
b. disabling of unused or undesired functionality in installed software and operating systems
c. implementation of access controls on relevant objects to limit system users and programs to the minimum access needed to perform their duties
d. installation of software-based firewalls limiting inbound and outbound network connections, and
e. configuration of either remote logging or the transfer of local event logs to a central server.

[–,HP,C-TS] Server environments

6.3.12. Agencies **should**:

a. limit information that could be disclosed outside the agency about what software is installed on servers, and
b. implement access controls on relevant objects to limit system users and programs to the minimum access needed to perform their duties.

[U,IC-HP,R-TS] Hardening during installation

6.3.13. Agencies **should** reduce potential vulnerabilities in their systems by:

a. removing unnecessary file shares
b. ensuring patching is up to date, and
c. disabling access to all unnecessary input/output functionality.

[U,IC-HP,R-S] Default passwords and accounts

6.3.14. Agencies **should** reduce potential vulnerabilities in their SOEs by:

a. removing unused accounts
b. renaming default accounts, and
c. replacing default passwords.

[–,–,TS] Default passwords and accounts

6.3.15. Agencies **must** reduce potential vulnerabilities in their SOEs by:

a. removing unused accounts
b. renaming or deleting default accounts, and
c. replacing default passwords.

[U,IC-HP,R-TS] Server separation

6.3.16. Where servers with a high security risk have connectivity to unsecured public networks, agencies **should**:

a. maintain effective functional separation between servers allowing them to operate independently
b. minimise communications between servers at both the network and filesystem level, as appropriate, and
c. limit system users and programs to the minimum access needed to perform their duties.

[U,IC-HP,R-TS] Functional separation between servers

6.3.17. Virtualisation technology **should not** be used for functional separation between servers in different security domains at the same security classification.

6.3.18. Virtualisation technology **must not** be used for functional separation between servers of different security classifications.

[U,IC-HP,R-TS] Characterisation

6.3.19. Agencies **should**:

a. characterise all servers whose functions are critical to the agency, and those identified as being at a high security risk of compromise
b. store the characterisation information securely off the server in a manner that maintains integrity
c. update the characterisation information after every legitimate change to a system
d. as part of the agency's ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred
e. perform the characterisation from a trusted environment rather than the standard operating system wherever possible, and
f. resolve any detected changes in accordance with the agency's information security incident management procedures.

[U,IC-HP,R-TS] Automated outbound connections by software

6.3.20. Agencies **should** review all software applications to determine whether they attempt to establish any external connections.

6.3.21. If automated outbound connection functionality is included, agencies **should** make a business decision to determine whether to permit or deny these connections, including an assessment of the security risks involved in doing so.

GUIDANCE

[U,IC-HP,R-TS] Workstation environments

6.3.22. It is **recommended** that agencies investigate additional information on hardening techniques relevant to their specific systems.

[U,IC-P,R] Server environments

6.3.23. It is **recommended** that agencies:

a. limit information that could be disclosed outside the agency about what software is installed, and
b. implement access controls on relevant objects to limit system users and programs to the minimum access needed to perform their duties.

[U,IC-HP,R-TS] Functional separation between servers

6.3.24. It is **recommended** that agencies ensure that functional separation between servers be achieved either:

a. physically, using single dedicated machines for each function, or
b. using virtualisation technology to create separate virtual machines for each function within the same security domain.

[U,IC-HP,R-TS] Characterisation

6.3.25. It is **recommended** that agencies meet the requirement for characterisation using a DACA to perform cryptographic checksums.

RATIONALE

Server environments

6.3.26. Information about installed software, that could be disclosed outside the agency, can include:

- user agent on Web requests disclosing the Web browser type
- network and email client information in email headers, and
- email server software headers.

6.3.27. This information could provide a malicious entity with knowledge of how to tailor attacks to exploit vulnerabilities in the agency's systems.

6.3.28. Objects where access controls can be implemented to limit system users and programs to the minimum access needed to perform their duties can include directories, files, programs, databases and communications ports.

Server separation

6.3.29. Servers with a high security risk can include Web, email, file and IPT servers.

Functional separation between servers

6.3.30. Agencies may implement separation through the use of techniques to restrict a process to a limited portion of the file system, but this is less effective.

Characterisation

6.3.31. Unfortunately, there are known techniques for defeating basic characterisations, therefore other methods of intrusion detection are also needed, particularly in situations where it is impractical to use a trusted environment for the generation of the characterisation data. However, it is very useful in post-intrusion forensic investigations where an infected disk can be compared to stored characterisation data in order to determine what files have been changed or introduced.

Automated outbound connections by software

6.3.32. Applications that include beaconing functionality include those that initiate a connection to the vendor site over the Internet and inbound remote management.

REFERENCES

6.3.33. Additional information relating to software fundamentals is contained in:

- AS/NZS ISO/IEC 27001:2006, A.12.4.1, *Control of Operational Software*, and
- AS/NZS ISO/IEC 27001:2006, A.12.6.1, *Control of Technical Vulnerabilities*.

Application Whitelisting

PRINCIPLE

6.3.34. The likelihood of malicious code being executed on a system can be reduced by the implementation and proper configuration of application whitelisting.

OBJECTIVE

6.3.35. To ensure that application whitelisting is implemented securely and effectively.

CONTEXT

Scope

6.3.36. This section covers information on the use of technical controls to restrict the specific applications that can be accessed by a user or group of users.

RISKS

6.3.37. An attacker exploits vulnerabilities in a legitimate application and executes arbitrary malicious code.

6.3.38. An attacker, having gained access to a workstation, uses in-built system functionality to spread further within the system.

6.3.39. Personnel install undesirable applications such as peer-to-peer and instant messaging applications which adversely affects system reliability and support overhead.

6.3.40. Personnel inadvertently run a system application, changing the configuration of the system and making it less secure.

6.3.41. Personnel disable the application whitelisting mechanism, allowing them to run any executable of their choosing causing harm to the agency's system.

6.3.42. An agency implements application whitelisting without adequate planning and testing leading to an implementation that is not as effective or secure as it could be.

6.3.43. An agency creates an application whitelisting policy which is too permissive by default and allows for the execution of arbitrary code causing harm to the agency's system.

6.3.44. An agency does not implement sufficient logging of application whitelisting events and crucial information regarding its use and effectiveness is not recorded.

6.3.45. An agency implements application whitelisting without adequately controlled update and patching mechanisms leading to an implementation that gradually reduces its security status over time.

6.3.46. Removable media containing a malicious executable is inserted into an agency's system resulting in the system being compromised.

6.3.47. Personnel open malicious files that were downloaded over the Internet, or attached to an email that were not detected by antivirus software, resulting in the system being compromised.

CONTROLS

[U,IC-HP,R-TS] Application whitelisting

6.3.48. Agencies **should** implement application whitelisting as part of the SOE for both workstations and servers.

[U,IC-HP,R-TS] System user permissions

6.3.49. Agencies **should** prevent a system user from running arbitrary executables.

6.3.50. Agencies **should** restrict a system user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.

6.3.51. Agencies **should** ensure that a system user cannot disable the application whitelisting mechanism.

6.3.52. Agencies **should** ensure that application whitelisting does not replace the antivirus software already in place within a system.

[U,IC-HP,R-TS] System administrator permissions

6.3.53. Agencies **should** ensure that system administrators are not automatically exempt from application whitelisting policy.

[U,IC-HP,R-TS] Application whitelisting configuration

6.3.54. Agencies **should** ensure that the default policy is to deny the execution of software.

6.3.55. Agencies **should** ensure that application whitelisting is used in addition to a strong access control list model and the use of limited privilege accounts.

6.3.56. Agencies **should** plan and test application whitelisting thoroughly prior to implementation.

GUIDANCE

[U,IC-HP,R-TS] Application whitelisting configuration

6.3.57. It is **recommended** that agencies restrict the decision whether to run an executable based on the following, in the order of preference shown:

a. cryptographic hash
b. executable absolute path
c. digital signature, and
d. parent folder.

6.3.58. It is **recommended** that agencies, where possible, restrict the process creation permissions of any executables which are permitted to run by the application whitelisting controls.

6.3.59. It is **recommended** that logs from the application whitelisting implementation include all relevant information.

RATIONALE

Application whitelisting

6.3.60. Application whitelisting can be an effective mechanism to prevent the successful compromise of an agency system resulting from the exploitation of a vulnerability in an application or the execution of malicious code.

6.3.61. Defining a list of trusted executables, a whitelist, is a more practical and secure method of securing a system than relying on a list of bad executables to be prevented from running.

6.3.62. Application whitelisting is considered only one part of a defence-in-depth strategy in order to prevent a successful attack, or to help mitigate consequences arising from an attack.

System user permissions

6.3.63. An average system user requires access to only a few applications, or groups of applications, in order to conduct their work. Restricting the system user's permissions to execute code to this limited set of applications reduces the attack surface of the system.

6.3.64. Since the consequences of running malicious code as a privileged user are much more severe than an unprivileged user, an application whitelisting implementation should also be enforced for system administrators.

Application whitelisting configuration

6.3.65. A decision to execute should be made based on cryptographic hash as it is more secure than a decision based on the executable's signature, path or parent folder.

6.3.66. In order for application whitelisting to be effective an agency must initially gather information on necessary executables and applications in order to ensure that the implementation is fully effective.

6.3.67. Different application whitelisting controls, such as restricting execution based on cryptographic hash or folder, have various advantages and disadvantages. Agencies need to be aware of this when implementing application whitelisting.

6.3.68. Application whitelisting based on parent folder or executable path is futile if access control list permissions allow a system user to write to the folders or overwrite permitted executables.

6.3.69. Adequate logging information can allow system administrators to further refine the application whitelisting implementation and detect a pattern of deny decisions for a system user.

6.3.70. An example of relevant information that could be included in logs for application whitelisting implementations would be decisions to deny execution incorporating information that would present a reviewer with evidence of misuse.

REFERENCES

6.3.71. Further information on application whitelisting as implemented by Microsoft can be found at: http://technet.microsoft.com/en-us/library/bb457006.aspx.

Web Applications

PRINCIPLE

6.3.72. The likelihood of malicious code being transferred to a system user's workstation from the Web can be reduced by blocking the download of software programs, active-content and websites not needed for business purposes.

OBJECTIVE

6.3.73. To ensure that personnel only have access to websites and resources that they need for business purposes.

CONTEXT

Scope

6.3.74. This section covers information on Web browsers, plug-ins and active content including the development and implementation of appropriate use policies. The requirements in this section apply equally to the Web accessed via the Internet as well as websites accessed on an agency intranet.

RISKS

6.3.75. A system user accesses a malicious website resulting in the introduction of malicious code to their workstation—such as a virus, key-logger or Trojan—which views, deletes, corrupts, uses or gains access to their workstation's resources.

CONTROLS

[U,IC-HP,R-TS] Web usage policies

6.3.76. Agencies **must** have a policy governing appropriate Web usage.

[U,IC-HP,R-TS] Web proxy

6.3.77. Agencies **should** use a Web proxy for all Web browsing activities.

6.3.78. An agency's Web proxy **should** authenticate system users and provide logging that includes the following details about websites accessed:

a. uniform resource locator
b. time/date
c. system user
d. internal Internet Protocol address, and
e. external Internet Protocol address.

[U,IC-HP,R-TS] Applications and plug-ins

6.3.79. Agencies **should** block the automatic launching of files downloaded from external websites.

[U,IC-HP,R-TS] SSL/TLS filtering

6.3.80. Agencies permitting Secure Sockets Layer/Transport Layer Security (SSL/TLS) through their gateway/CDS **should** implement:

a. a solution that decrypts and inspects the SSL/TLS traffic as per the Web content filtering requirements, or
b. a whitelist specifying the external uniform resource locators to which encrypted connections are permitted, with all other addresses blocked.

GUIDANCE

[U,IC-HP,R-TS] Whitelisting websites

6.3.81. It is **recommended** that agencies implement whitelisting for all Hypertext Transfer Protocol traffic being communicated through their gateway/CDS.

6.3.82. It is **recommended** that if agencies do not whitelist websites they blacklist websites to prevent access to known malicious websites.

6.3.83. It is **recommended** that agencies blacklisting websites update the blacklist on a frequent basis to ensure that it remains effective.

[U,IC-HP,R-TS] Client-side active content

6.3.84. It is **recommended** that agencies block client-side active content, such as Java and ActiveX, which might not have a large business impact.

6.3.85. It is **recommended** that agencies:

a. use client-side controls that allow JavaScript on a per website basis, and
b. add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS.

[U,IC-HP,R-TS] Web content filter

6.3.86. It is **recommended** that agencies use the Web proxy to filter content that is potentially harmful to system users and their workstations.

RATIONALE

Web proxy

6.3.87. Web proxies provide valuable information in determining if malicious code is performing regular interactions over Web traffic. Web proxies also provide usable information if system users are violating agency Web usage policies.

Applications and plug-ins

6.3.88. Web browsers can be configured to allow the automatic launching of downloaded files. This can occur with or without the system user's knowledge thus making the workstation vulnerable to attack.

SSL/TLS filtering

6.3.89. As SSL/TLS Web traffic travelling over Hypertext Transfer Protocol Secure (HTTPS) connections can deliver content without any filtering agencies can reduce this security risk by using SSL/TLS inspection so that the Web traffic can be filtered.

6.3.90. An alternate of using a whitelist for HTTPS websites can allow websites that have a low security risk of delivering malicious code and have a high privacy requirement like Web banking, to continue to have end-to-end encryption.

Whitelisting websites

6.3.91. Defining a whitelist of permitted websites and blocking all unlisted websites effectively removes one of the most common data delivery and exfiltration techniques used by malicious code. However, if agency personnel have a legitimate requirement to access a numerous and rapidly changing list of websites, agencies will need to consider the costs of such an implementation.

Client-side active content

6.3.92. Software that runs in an agency should be controlled by the agency. Active content delivered though websites should be constrained so that it cannot arbitrarily access system users' files or deliver malicious code. Unfortunately the implementations of Web browsers regularly contain flaws that permit such activity.

REFERENCES

6.3.93. A Web whitelisting software application that allows for the management of whitelists can be obtained from http://whitetrash.sf.net.

6.3.94. Examples of client-side JavaScript controls are available at http://noscript.net.

6.3.95. A list of JavaScript functions that are typically used for malicious purposes is listed on the OnSecure website at https://members.onsecure.gov.au.

EXAMPLES

6.3.96. Web content filtering could perform the following functions to reduce the vulnerabilities in the client browser:

- pass only a whitelist of legitimate JavaScript functions
- block or strip Java 'APPLET' tags
- block or strip ActiveX control tags
- pass only a whitelist of allowed file types determined by content checking, and
- block inline frames as particularly small sized inline frames are often used to deliver malicious code.

6.3.97. The above functions are not possible with HTTPS websites unless SSL/TLS inspection is used.

Email Applications

PRINCIPLE

6.3.98. Email marking practices convey the security classification of information in emails.

OBJECTIVE

6.3.99. To ensure that system users know how to appropriately handle and protect the information contained in emails.

CONTEXT

Scope

6.3.100. This section covers information on email usage as it applies to content and protective markings. Information on email infrastructure is located in the *Email Infrastructure* section of the *Network Security* chapter of this manual.

Automatically generated emails

6.3.101. The requirements for emails within this section equally apply to automatically generated emails.

Exceptions for receiving unmarked email messages

6.3.102. Where an agency receives unmarked non-government emails as part of its business practice the application of protective markings can be automated by a system.

RISKS

6.3.103. An attacker forges an email and socially engineers personnel into divulging information, installing malicious code or corrupting information stores.

6.3.104. An attacker sends a malicious email to personnel, which once opened results in workstation infection.

6.3.105. An attacker sends a malicious email to personnel. These personnel use a public Web-based email client to download and execute an attachment, effectively bypassing agency email gateway/CDS malicious code checks.

6.3.106. Personnel automatically forward a security classified email for which the receiver does not have a need-to-know, resulting in an information security breach.

6.3.107. Personnel send an email containing AUSTEO, AGAO or other nationality releasability marked information to a distribution list. Unbeknownst to the sender, personnel not authorised to receive such information are included on the distribution list.

6.3.108. An agency fails to put in place a set of email policies, plans and procedures, resulting in system users being unaware of required email security practices.

6.3.109. Personnel send security classified emails with protective markings that accurately reflect the security classification of the email body, but with an attachment of a higher security classification and the receiving email system accepts the email due to its protective marking resulting in a data spill.

6.3.110. A security classified email without a protective marking, or a protective marking that is a lower security classification than the true content of the email, is received by an agency email server. The agency, having no indication that the email has a security classification higher than their internal systems, delivers the email to a number of other internal systems that need to be sanitised to remove traces of the email.

6.3.111. An agency system automatically generates a security classified email but does not apply the protective markings. The recipient of the email, unaware of the correct security classification, handles the email in a manner that is not approved for that security classification.

6.3.112. Personnel send security classified emails with incorrect protective markings. The recipient of the email, unaware of the correct security classification, handles the email in a manner not approved for that security classification.

6.3.113. Personnel send emails without protective markings, leaving the recipient of the email unsure of how to properly handle the email.

6.3.114. An agency uses a non-standard protective marking for emails, resulting in recipients being unsure of appropriate handling procedures for the email.

6.3.115. A system user sends an email with a protective marking automatically generated by an agency tool without checking the protective marking resulting in a data spill.

CONTROLS

[U,IC-HP,R-TS] Email usage policies

6.3.116. Agencies **must** have a policy governing the use of email.

[U,IC-HP,R-TS] Automatic forwarding of emails

6.3.117. Agencies **should** warn personnel that the automatic forwarding of email to other personnel could result in the recipient seeing information for which they do not have a need-to-know.

[–,IC-HP,R-TS] Email distribution

6.3.118. Agencies **should** ensure that emails containing AUSTEO, AGAO or other nationality releasability marked information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

[U,IC-HP,R-TS] Protective marking standard

6.3.119. Agencies **should** comply with the standard for the application of protective markings to emails, as promulgated by AGIMO.

[U,IC-HP,R-TS] Marking tools

6.3.120. Agencies **should not** allow a protective marking to be inserted into system user generated emails without their intervention.

6.3.121. Agencies providing a marking tool **should not** allow system users to select protective markings that the system has not been accredited to process, store or communicate.

[–,IC-HP,R-TS] Marking security classified emails

6.3.122. All security classified emails **must** have a protective marking.

6.3.123. Email labelling **must** accurately reflect the security classification of each element of an email, including attachments.

[–,IC-P,R] Marking non-security classified emails on security classified systems

6.3.124. All emails that originate from a security classified system but do not contain any security classified information **should** have a protective marking.

[–,HP,C-TS] Marking non-security classified emails on security classified systems

6.3.125. All emails that originate from a security classified system but do not contain any security classified information **must** have a protective marking.

[U,IC-HP,R-TS] Emails from outside the Australian Government

6.3.126. Where an unmarked email has originated outside the Australian Government, the agency **must** assess the information and determine how it is to be handled.

[U,IC-HP,R-TS] Marking personal emails

6.3.127. Where an email is of a personal nature and does not contain government information, protective markings for non-security classified or security classified information **should not** be used.

GUIDANCE

[U,–,–] Marking non-security classified emails

6.3.128. It is **recommended** that all emails have a protective marking.

[U,IC-HP,R-TS] Receiving unmarked emails

6.3.129. It is **recommended** that where an unmarked email has originated from an Australian or overseas government agency, personnel contact the originator to determine how it is to be handled.

[U,IC-HP,R-TS] Receiving emails with unknown protective markings

6.3.130. It is **recommended** that where an email is received with an unknown protective marking from an Australian or overseas government agency, personnel contact the originator to determine appropriate protection measures.

[U,IC-HP,R-TS] Emails from outside the Australian Government

6.3.131. It is **recommended** that agencies encourage external organisations that send email to the agency to adopt the AGIMO protective marking standard.

[U,IC-HP,R-TS] Printing

6.3.132. It is **recommended** that agencies configure systems so that the protective markings appear at the top and bottom of every page when the email is printed.

[U,IC-HP,R-TS] Marking personal emails

6.3.133. It is **recommended** that where an email is of a personal nature and does not contain government information, the protective marking of UNOFFICIAL is used.

RATIONALE

Email usage policies

6.3.134. There are many security risks associated with the non-secure nature of email that are often overlooked. Documenting them will inform information owners about these security risks and how they might affect business operations.

Protective marking standard

6.3.135. Applying markings that reflect the protective requirements of an email informs the recipient on how to appropriately handle the email as a whole.

6.3.136. The application of protective markings as per the AGIMO standard facilitates interoperability between agencies.

Marking tools

6.3.137. Requiring system user intervention in the marking of system user-generated emails assures a conscious decision by the system user, lessening the chance of incorrectly marked emails.

6.3.138. Limiting the protective markings from which a tool allows a system user to choose, to those for which the system is accredited lessens the chance that a system user inadvertently over-classifies an email and reminds them of the maximum security classification of information that is permitted on the system.

6.3.139. Using a marking tool that facilitates a correctly formatted protective marking will assist in the automated blocking of emails being sent to systems that are not accredited to process them.

6.3.140. Requiring a system user to apply a protective marking before forwarding a received, unmarked email, halts further spread of the unmarked email and informs the recipient of the correct handling procedures for the email.

Marking security classified emails

6.3.141. Applying protective markings to an email that is above the security classification of that email can hinder the release of information to personnel with a valid need-to-know.

Marking personal emails

6.3.142. Applying incorrect protective markings to emails that do not contain government information places an extra burden on agencies to protect emails that do not need protection. The use of UNOFFICIAL as a protective marking, whilst not currently listed in the PSM, has become the de facto standard within government for protectively marking emails that do not contain government information.

REFERENCES

6.3.143. The AGIMO email protective markings standard and its associated implementation guide is available from http://www.finance.gov.au/e-government/security-and-authentication/ict-security/index.html.

Software Application Development

PRINCIPLE

6.3.144. Secure software development relies on the implementation of secure programming methods and appropriate levels of testing to lessen the potential for information security vulnerabilities in the production environment.

OBJECTIVE

6.3.145. To ensure that secure software testing and development procedures are undertaken.

CONTEXT

Scope

6.3.146. This section covers information relating to the development, upgrade and maintenance of application software used on systems.

RISKS

6.3.147. Personnel release un-tested software that introduces new vulnerabilities to the product environment.

6.3.148. Agency personnel undertaking software testing have insufficient expertise to conduct appropriate testing, resulting in a vulnerable application being released to the production environment.

6.3.149. An agency developer reviews their own software, missing vulnerabilities due to over familiarisation, allowing a vulnerable application to be released into the production environment.

6.3.150. Personnel fail to turn off debug mode in production software, providing an attacker with access to the source code and insight into further vulnerabilities.

6.3.151. Personnel insert compromised media into the development environment which copies source code to the device and provides an easy way for it to be stolen.

6.3.152. An attacker plants malicious code in the testing environment which is subsequently copied to the production environment.

CONTROLS

[U,IC-HP,R-TS] Software development environments

6.3.153. Agencies **should** ensure that software development environments are configured such that:

a. there are at least three environments covering:
   1) development
   2) testing, and
   3) production
b. information flow between the environments is strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement
c. new development and modifications only take place in the development environment; and
d. write access to the authoritative source for the software is disabled.

[U,IC-HP,R-TS] Secure programming

6.3.154. Agencies **should** ensure that software developers use secure programming practices when writing code, including:

a. designing software to use the lowest privilege level needed to achieve its task
b. denying access by default
c. checking return values of all system calls, and
d. validating all inputs.

[U,IC-HP,R-TS] Software testing

6.3.155. Software **should** be reviewed or tested for vulnerabilities before it is used in a production environment.

6.3.156. Software **should** be reviewed or tested by an independent party as well as the developer.

GUIDANCE

[U,IC-HP,R-TS] Software development outsourcing

6.3.157. It is **recommended** that agencies determine the security risks associated with the outsourcing of software development.

RATIONALE

Software development environments

6.3.158. Segregating development, testing and production environments limits the spread of malicious code and minimises the likelihood of faulty code being put into production.

6.3.159. Limiting access to development and testing environments will reduce the information that can be gained by an internal attacker.

Secure programming

6.3.160. Designing software to use the lowest privilege level needed to achieve its task will limit the privileges an attacker could gain should they subvert the software security.

6.3.161. Validating all inputs will ensure that the input is within expected ranges, reducing the chance that malicious or erroneous input causes unexpected results.

Software testing

6.3.162. Software reviewing and testing will lessen the possibility of security vulnerabilities being introduced into a production environment.

6.3.163. Using an independent party for software testing will remove any bias that can occur when a developer tests their own software.

Software development outsourcing

6.3.164. When an agency chooses to outsource software development they loose control of the development lifecycle for the software application being developed. Agencies are recommended to consider the implications this could have on their information security posture.

REFERENCES

6.3.165. Additional information relating to software development is contained in AS/NZS ISO/IEC 27001:2006, A.12.5, *Security in Development and Support Processes*.

Web Application Development

PRINCIPLE

6.3.166. Web applications need to protect the availability, access control and integrity of the information that they use.

OBJECTIVE

6.3.167. To ensure that deployed Web applications have sufficient security mechanisms to assist in protecting against the most common classes of exploits.

SCOPE

Scope

6.3.168. This section covers the deployment of agency Web applications and websites.

Protecting Web servers

6.3.169. Even though Web servers may only contain information authorised for release into the public domain there still remains a need to protect the integrity of the information. As such, Web servers are at a minimum to be treated as per the requirements for UNCLASSIFIED systems. If Web servers internal to an agency contain information they are to be treated as per the requirement for the security classification of the information.

Web application components

6.3.170. Web application components at a high level consist of a Web server for presentation, a Web application for processing and a database for content storage. There can be more or less components, however in general there is a presentation layer, application layer and database layer.

RISKS

6.3.171. A Web application leaks information to an unauthorised recipient resulting in the disclosure of information.

6.3.172. An attacker gains access to information they are not authorised to access by exploiting vulnerabilities in forms used by Web applications.

6.3.173. A Web application accidentally spills information into a system of a lesser security classification resulting in an information security incident.

6.3.174. An attacker modifies information through a Web application without authorisation resulting in the loss of information integrity.

6.3.175. An attacker or software consumes resources, resulting in a denial of service.

6.3.176. An attacker intercepts communications, resulting in the loss of confidentiality.

6.3.177. An attacker manipulates a Web application to distribute malicious code.

CONTROLS

[U,IC-HP,R-TS] Agency website content

6.3.178. Agencies **should** review all active content on their Web servers for information security issues.

[U,IC-HP,R-TS] Segregation of Web application components

6.3.179. Agencies **should** minimise connectivity and access between each Web application component.

GUIDANCE

[U,IC-HP,R-TS] Web applications

6.3.180. It is **recommended** that agencies follow the documentation provided in the Open Web Application Security Project (OWASP) guide to building secure Web applications and Web services.

RATIONALE

Segregation of Web application components

6.3.181. Web applications are typically very exposed services that provide complex interactions with system users. This greatly increases the security risk of being compromised. By segregating components the impact of potential application flaws is limited.

Web applications

6.3.182. The OWASP guide provides a comprehensive resource to consult when developing Web applications.

REFERENCES

6.3.183. Further information on Web application security is available from the OWASP at http://www.owasp.org.

Databases

PRINCIPLE

6.3.184. Labelling information within a database ensures that data can be protected appropriately and that information is not accidentally disclosed to those without a need-to-know.

OBJECTIVE

6.3.185. To ensure that agencies properly secure databases, contents are labelled and search results are appropriately filtered based on a system user's security clearances.

CONTEXT

Scope

6.3.186. This section covers information relating to databases and interfaces to databases such as search engines.

RISKS

6.3.187. An agency stores information within a database containing inadequate protective markings resulting in incorrect handling.

6.3.188. An attacker bypasses normal database access controls to gain unauthorised access to information.

6.3.189. A system user accidentally, or maliciously, exploits a search engine, returning metadata which contains information they do not have sufficient security clearances to access.

CONTROLS

[U,IC-HP,R-S] Data labelling

6.3.190. Agencies **should** ensure that all information stored within a database is associated with an appropriate protective marking if the information:

a. could be exported to a different system, or
b. contains differing security classifications or different handling requirements.

6.3.191. Agencies **should** ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any information retrieved or exported from a database.

[–,–,TS] Data labelling

6.3.192. Agencies **must** ensure that all information stored within a database is associated with an appropriate protective marking if the information:

a. could be exported to a different system, or
b. contains differing security classifications or different handling requirements.

6.3.193. Agencies **must** ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any information retrieved or exported from a database.

[U,IC-HP,R-S] Database files

6.3.194. Agencies **should** protect database files from access that bypasses the database's normal access controls.

[–,–,TS] Database files

6.3.195. Agencies **must** protect database files from access that bypasses the database's normal access controls.

[U,IC-HP,R-TS] Accountability

6.3.196. Agencies **should** ensure that databases provide functionality to allow for auditing of system users' actions.

[U,IC-HP,R-TS] Search engines

6.3.197. Agencies **should** ensure that system users who do not have sufficient security clearances to view database contents cannot see associated metadata in a list of results from a search engine query.

6.3.198. If results from database queries cannot be appropriately filtered, agencies **must** ensure that all query results are appropriately sanitised to meet the minimum security clearances of system users.

RATIONALE

Data labelling

6.3.199. Protective markings can be applied to records, tables or to the database as a whole, depending on structure and use. Query results will often need a protective marking to reflect the aggregate of the information retrieved.

Search engines

6.3.200. Even if a search engine restricts viewing of information that a system user does not have sufficient security clearances to access, the associated metadata could contain information above the security clearances of the system user. In such cases, restricting access to, or sanitising, this metadata effectively controls the possible release of information the system user is not cleared to view.

Access Control Security

Identification and Authentication

PRINCIPLE

6.4.1. Implementing password selection policies and password management practices prevents system users and systems from having authentication information easily subverted by brute force attacks against weak authenticators.

OBJECTIVE

6.4.2. To ensure that access to an agency's system is controlled by insisting on an authentication procedure to establish, with some minimum degree of confidence, the identity of the system user.

CONTEXT

Scope

6.4.3. This section covers information on the identification and authentication of all system users.

Methods for user identification and authentication

6.4.4. User authentication can be achieved by various means, including biometrics, cryptographic tokens, pass phrases, passwords and smartcards.

RISKS

6.4.5. The agency uses an inappropriate authentication method, increasing the chance of unauthorised access.

6.4.6. An attacker bypasses weak authentication mechanisms to gain access to systems.

6.4.7. An agency, by allowing the use of shared accounts, reduces system user accountability.

6.4.8. An attacker gains access to authentication information that is stored on a system to which they have access, allowing them to masquerade as another authorised system user.

6.4.9. An attacker intercepts authentication information that is communicated in the clear, allowing them to access systems.

6.4.10. An attacker gains access to a session in which the victim has already authenticated, resulting in an ability to access information or assume the victim's identity.

6.4.11. An attacker gains access to a system by brute force attacks against the authentication method.

CONTROLS

[U,IC-HP,R-TS] Documentation

6.4.12. Agencies **must**:

a. develop and maintain a set of policies, plans and procedures, derived from a security risk assessment, covering system users':
   1) identification
   2) authentication, and
   3) authorisation; and
b. make their system users aware of the agency's policies, plans and procedures.

[–,IC-HP,R-TS] System user identification

6.4.13. Agencies **must** ensure that all system users are:

a. uniquely identifiable, and
b. authenticated on each occasion that access is granted to a system.

[–,–,TS] Shared accounts

6.4.14. Agencies **should not** use shared, non user-specific, accounts.

[U,IC-HP,R-TS] System user identification for shared accounts

6.4.15. If agencies choose to allow shared, non-user specific accounts they **must** ensure that another method of determining the identification of the system user is implemented.

[U,IC-HP,R-TS] Methods for system user identification and authentication

6.4.16. Agencies **must not** use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system.

[U,IC-HP,R-TS] Protecting stored authentication information

6.4.17. Agencies **must not** allow storage of unprotected authentication information that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access.

[U,IC-HP,R-TS] Protecting authentication data in transit

6.4.18. Agencies **must** ensure that when system authentication data is communicated it is not susceptible to attacks including, but not limited to, replay, man-in-the-middle and session hijacking.

[U,IC-HP,R-TS] Identification of foreign nationals

6.4.19. Where systems contain AUSTEO, AGAO or other nationality releasability marked information, agencies **must** provide a mechanism that allows system users and processes to identify system users who are foreign nationals, including seconded foreign nationals.

[U,IC-HP,R-S] Password selection policy

6.4.20. Agencies **should** implement a password policy enforcing either:

a. a minimum password length of 12 characters with no complexity requirement; or
b. a minimum password length of seven characters, consisting of at least three of the following character sets:
   1) lowercase characters (a-z)
   2) uppercase characters (A-Z)
   3) digits (0-9), and
   4) punctuation and special characters.

[–,–,TS] Password selection policy

6.4.21. Agencies **must** implement a password policy enforcing either:

a. a minimum password length of 15 characters with no complexity requirement; or
b. a minimum password length of eight characters, consisting of at least three of the following character sets:
   1) lowercase characters (a-z)
   2) uppercase characters (A-Z)

Continued on next page

3) digits (0-9), and
4) punctuation and special characters.

[U,IC-HP,R-S] Password management

6.4.22. Agencies **should**:

a. ensure that passwords are changed at least every 90 days
b. prevent system users from changing their password more than once a day
c. check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements, and
d. force the system user to change an expired password on initial logon or if reset.

6.4.23. Agencies **should not**:

a. allow predictable reset passwords
b. reuse passwords when resetting multiple accounts
c. allow passwords to be reused within eight password changes, and
d. allow system users to use sequential passwords.

[–,–,TS] Password management

6.4.24. Agencies **must**:

a. ensure that passwords are changed at least every 90 days
b. prevent system users from changing their password more than once a day
c. check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements
d. force the user to change an expired password on initial logon or if reset, and
e. have system users physically present themselves to the person who is resetting their password.

6.4.25. Agencies **must not**:

a. allow predictable reset passwords
b. reuse passwords when resetting multiple accounts
c. store passwords in the clear on the system
d. allow passwords to be reused within eight password changes
e. allow system users to use sequential passwords, and
f. use a shared login or password unless the practices have been approved by DSD.

[U,IC-HP,R-TS] Session termination

6.4.26. Agencies **should** develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity.

[U,IC-HP,R-S] Screen and session locking

6.4.27. Agencies **should**:

a. configure systems with a session or screen lock
b. configure the lock to activate:
   1) after a maximum of 15 minutes of system user inactivity, or
   2) if manually activated by the system user

Continued on next page

c. configure the lock to completely conceal all information on the screen
d. ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated
e. have the system user reauthenticate to unlock the system; and
f. deny system users the ability to disable the locking mechanism.

[–,–,TS] Screen and session locking

6.4.28. Agencies **must**:

a. configure systems with a session or screen locks
b. configure the lock to activate:
   1) after a maximum of 10 minutes of system user inactivity, or
   2) if manually activated by the system user
c. configure the lock to completely conceal all information on the screen
d. ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated
e. have the system user reauthenticate to unlock the system; and
f. deny system users the ability to disable the locking mechanism.

[U,IC-P,R] Suspension of access

6.4.29. Agencies **should**:

a. lock system user accounts after a specified number of failed logon attempts
b. remove or suspend system user accounts as soon as possible after personnel no longer needs access, due to changing roles or leaving the agency, and
c. suspend inactive accounts after a specified number of days.

[–,HP,C-TS] Suspension of access

6.4.30. Agencies **must**:

a. lock system user accounts indefinitely after three failed logon attempts
b. have a system administrator reset locked accounts, and
c. remove or suspend system user accounts as soon as possible after personnel no longer needs access, due to changing roles or leaving the agency.

6.4.31. Agencies **should**:

a. ensure that repeated account lockouts are investigated before reauthorising access, and
b. suspend inactive accounts after an agency-specified number of days.

GUIDANCE

[U,–,–] System user identification

6.4.32. It is **recommended** that agencies ensure that system users are:

a. uniquely identifiable, and
b. authenticated on each occasion that access is granted to a system.

[U,IC-HP,R-S] Shared accounts

6.4.33. It is **recommended** that agencies do not use shared, non-user specific accounts.

[U,IC-HP,R-TS] Methods for system user identification and authentication

6.4.34. It is **recommended** that agencies ensure that they combine the use of multiple methods when identifying and authenticating system users.

[U,IC-HP,R-TS] Identification of foreign nationals

6.4.35. It is **recommended** that agencies using AUSTEO or AGAO systems that provide a mechanism that allows system users and processes to identify system users who are foreign nationals, including seconded foreign nationals, ensure that this identification includes their specific nationality.

[U,IC-HP,R-S] Password management

6.4.36. It is **recommended** that agencies ensure that system users physically present themselves to the person who is resetting their password.

[U,IC-HP,R-TS] Displaying when a system user last logged in

6.4.37. It is **recommended** that agencies configure systems to display the date and time of the system user's previous login during the login process.

[U,IC-P,R] Suspension of access

6.4.38. It is **recommended** that agencies ensure that:

a. a limit of three failed logon attempts be permitted, and
b. account resets can only be performed by a system administrator.

RATIONALE

Documentation

6.4.39. Developing policies, plans and procedures will ensure consistency in identification, authentication and authorisation.

6.4.40. Deriving policies, plans and procedures from a security risk assessment will ensure that they are appropriate and specific to the security objectives of the agency.

System user identification

6.4.41. Having uniquely identifiable system users ensures accountability.

Methods of system user identification and authentication

6.4.42. A personal identification number is typically short in length and employs a small character set, making it susceptible to brute force attacks.

Protecting stored authentication information

6.4.43. Limiting the storage of unprotected authentication information reduces the possibility of an attacker finding and using the information to access a system under the guise of a valid system user.

Protecting authentication data in transit

6.4.44. Secure transmission of authentication information will reduce the security risk of interception and subsequent use of the authentication information by an attacker to access a system under the guise of a valid system user.

Password selection policy

6.4.45. A simple six-letter password can be brute-forced in minutes by software available on the Web. Passwords with at least seven characters utilising upper and lower case, numbers and special characters have a much greater resistance to brute force attacks.

Password management

6.4.46. Requiring a password to be changed at least every 90 days will limit the time period in which a disclosed password could be used by an unauthorised system user.

6.4.47. Preventing a system user from changing their password more than once a day will stop the system user from immediately changing their password back to their old password.

6.4.48. Checking passwords for compliance with the password selection policy will allow system administrators to detect unsafe password selection and ensure that the system user changes it.

6.4.49. Forcing a system user to change a password on account reset will ensure that the system user has a password that only they know and is more easily remembered.

6.4.50. Disallowing predictable reset passwords will reduce the security risk of brute force attacks and password guessing attacks.

6.4.51. Using different passwords when resetting multiple accounts will prevent a system user whose account has been recently reset from logging into another such account.

6.4.52. Disallowing passwords from being reused within eight changes will prevent a system user from cycling between a small subset of passwords.

6.4.53. Disallowing sequential passwords will reduce the security risk of an attacker easily guessing a system user's next password based on their knowledge of the system user's previous password.

Screen and session locking

6.4.54. Screen and session locking will prevent access to a system to which a system user has already been authenticated into when they are away from their workstation.

6.4.55. Ensuring that the screen does not appear to be turned off while in the locked state will prevent system users from forgetting they are still logged in and will prevent other system users from mistakenly thinking there is a problem with a workstation and resetting it.

Suspension of access

6.4.56. Locking a system user account after a specified number of failed logon attempts will reduce the security risk of brute force attacks.

6.4.57. Removing a system user account when it is no longer required will prevent personnel from accessing their old account and reduce the number of accounts that an attacker can target.

6.4.58. Suspending inactive accounts after a specified number of days will reduce the number of accounts that an attacker can target.

6.4.59. Investigating repeated account lockouts will reduce the security risk of any ongoing brute force logon attempts and allow security management to act accordingly.

REFERENCES

6.4.60. Additional information relating to user authentication is contained in:

- AS/NZS ISO/IEC 17799:2006, 11.2.3, *User Password Management*
- AS/NZS ISO/IEC 17799:2006, 11.3.1, *Password Use*, and
- AS/NZS ISO/IEC 17799:2006, 11.5.2, *User Identification and Authentication*.

Authorisation and System Access

PRINCIPLE

6.4.61. Access to information on systems can be controlled through the use of appropriate authorisations and system access requirements.

OBJECTIVE

6.4.62. To ensure that the need-to-know principle is enforced with user access controls and authorisation procedures.

CONTEXT

Scope

6.4.63. This section covers information on access requirements for all system users. Additional information on privileged users and system accounts can be found in the *Privileged Access* section of this chapter whilst addition information on security clearance requirements can be found in the *Security Clearances and Briefings* section.

RISKS

6.4.64. A system user gains access to information to which they do not have a valid need-to-know or have not been appropriately authorised to access.

6.4.65. System user logs are not retained for the life of a system, hindering the investigation of information security incidents.

6.4.66. Information about system user authorisation is not properly recorded or retained, resulting in more access being granted to a system user than for which they were authorised.

6.4.67. Information about system user authorisation is not properly recorded or retained, resulting in a lack of evidence that personnel are authorised to access a system.

CONTROLS

[U,IC-HP,R-S] Authorisation and system access

6.4.68. Agencies **should**:

a. limit system access on a need-to-know basis
b. provide system users with the least amount of privileges needed to undertake their duties, and
c. have any requests for access to a system authorised by the supervisor or manager of the system user.

[–,–,TS] Authorisation and system access

6.4.69. Agencies **must**:

a. limit system access on a need-to-know basis
b. provide system users with the least amount of privileges needed to undertake their duties, and
c. have any requests for access to a system authorised by the supervisor or manager of the system user.

[U,IC-HP,R-TS] Additional authorisation

6.4.70. System users that need to bypass security mechanisms for any reason **must** seek formal authorisation from an ITSM.

[U,IC-HP,R-TS] Recording authorisation for personnel to access systems

6.4.71. Agencies **should**:

a. maintain a secure record of:
   1) all authorised system users
   2) their user identification
   3) who provided the authorisation to access the system, and
   4) when the authorisation was granted; and
b. maintain the record for the life of the system to which access is granted.

[U,IC-HP,R-TS] Logon banner

6.4.72. Agencies **should** have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted.

[–,IC-HP,R-TS] Access from foreign controlled systems and facilities

6.4.73. Agencies **must not** allow access to AUSTEO or AGAO information from systems and facilities not under the sole control of the Australian Government.

6.4.74. Unless a bi-lateral security instrument is in place, agencies **should not** allow access to security classified information from systems and facilities not under the sole control of the Australian Government.

[U,IC-HP,R-TS] System high mode

6.4.75. Systems operating in system high mode **must** have need-to-know access controls enforced by the system.

[U,IC-HP,R-TS] Compartmented mode

6.4.76. Systems operating in compartmented mode **must** have restricted access to compartmented information enforced by the system.

GUIDANCE

[U,IC-HP,R-TS] Logon banner

6.4.77. It is **recommended** that agencies seek legal advice on the exact wording of logon banners.

6.4.78. It is **recommended** that agency logon banners cover issues such as:

a. access only being permitted to authorised system users
b. the system user's agreement to abide by relevant security policies
c. the system user's awareness of the possibility that system usage is being monitored
d. the definition of acceptable use for the system, and
e. legal ramifications of violating the relevant policies.

[U,IC-HP,R-TS] Developing an access control list

6.4.79. It is **recommended** that agencies follow the process in the table below for developing an access control list:

STAGE	DESCRIPTION
1	Establish groups of all system resources based on similar security objectives.
2	Determine the information owner for each group of resources.
3	Establish groups encompassing all system users based on similar functions or security objectives.
4	Determine the group owner or manager for each group of system users.
5	Determine the degree of access to the resource for each system user group.
6	Decide on the degree of delegation for security administration, based on the internal security policy.

RATIONALE

Recording authorisation for personnel to access systems

6.4.80. In many cases the requirement to maintain a secure record of all personnel authorised to access a system, their user identification, who provided the authorisation and when the authorisation was granted, can be met by retaining a completed system account request form signed by the supervisor or manager of the system user.

Privileged Access

PRINCIPLE

6.4.81. Privileged and system accounts are created to allow trusted personnel to undertake maintenance work on systems.

OBJECTIVE

6.4.82. To ensure that as privileged and system accounts are capable of bypassing security controls, they are controlled, accounted for and their use kept to a minimum.

CONTEXT

Scope

6.4.83. This section covers information relating specifically to systems users that are granted privileged access to systems.

Privileged access

6.4.84. Within this section, privileged access is considered to be access which can give a system user:

- the ability to change key system configurations
- the ability to change control parameters
- access to audit and security monitoring information
- the ability to circumvent security measures
- access to data, files and accounts used by other system users, including backups and media, or
- special access for troubleshooting the system.

RISKS

6.4.85. A privileged user uses their privileged account in a manner that is not controlled or accountable, resulting in actions that cannot be audited at a later date.

6.4.86. An agency grants a system user privileged access above the level needed to perform their duties, resulting in increased exposure to potential abuse of power.

6.4.87. A foreign national is given inappropriate privileged access to systems that process, store or communicate unprotected AUSTEO or AGAO information, resulting in the exposure of sensitive information.

6.4.88. An agency inappropriately controls generic system administrator passwords resulting in their use by personnel not authorised to use them.

6.4.89. Due to a lack of detailed information concerning a system on which an information security incident took place, it cannot be properly investigated.

6.4.90. Due to the lack of retention of system management logs, an information security incident cannot be properly investigated

6.4.91. A privileged user participating in data transfers from a system security classified higher than their security clearance is exposed to information they are not cleared, nor briefed, to access.

CONTROLS

[U,IC-HP,R-S] Use of privileged accounts

6.4.92. Agencies **should**:

a. ensure that the use of privileged accounts is controlled and accountable
b. ensure that system administrators are assigned an individual account for the performance of their administration tasks
c. keep privileged accounts to a minimum, and
d. allow the use of privileged accounts for administrative work only.

[–,–,TS] Use of privileged accounts

6.4.93. Agencies **must**:

a. ensure that the use of privileged accounts is controlled and accountable
b. ensure that system administrators are assigned an individual account for the performance of their administration tasks
c. keep privileged accounts to a minimum, and
d. allow the use of privileged accounts for administrative work only.

[–,IC-HP,R-TS] Privileged system access by foreign nationals

6.4.94. Agencies **must not** allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate AUSTEO information.

6.4.95. Agencies **must not** allow foreign nationals, excluding seconded foreign nationals, to have privileged access to systems that process, store or communicate AGAO information.

6.4.96. Agencies **should not** allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate security classified information.

[–,–,TS] Generic system administrator passwords

6.4.97. Generic system administrator passwords **must**:

a. meet the agency's password selection policy
b. be stored in a secure manner consistent with the security classification of the system to which they give access
c. be auditable and accountable, and
d. be changed if the password is known by personnel who are no longer authorised to have privileged or system access.

[U,IC-HP,R-TS] Privileged access accountability

6.4.98. A system management log **should** be manually updated to record the following information:

a. sanitisation activities
b. system startup and shutdown
c. component or system failures
d. maintenance activities
e. backup and archival activities
f. system recovery activities, and
g. special or out of hours activities.

[–,HP,C-S] Privileged access accountability

6.4.99. Agencies **should** maintain system management logs for the life of a system.

[–,–,TS] Privileged access accountability

6.4.100. Agencies **must** maintain system management logs for the life of a system.

GUIDANCE

[U,IC-P,R] Privileged access accountability

6.4.101. It is **recommended** that agencies maintain system management logs for the life of a system.

[U,IC-HP,R-TS] Retention of logs

6.4.102. It is **recommended** that agencies seek advice to determine if their system management logs are subject to the *Archives Act 1983* (Archives Act).

[U,IC-HP,R-TS] Security clearances for privileged users

6.4.103. It is **recommended** that agencies involved in frequent transfers of data from another system to their system with a lesser security classification clear at least one privileged user to the security classification of the higher system.

RATIONALE

Use of privileged accounts

6.4.104. Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures or information security breaches of systems.

6.4.105. Privileged access rights allow for system wide changes to be made and as such an appropriate and effective mechanism to log privileged users will provide greater accountability and auditing capability.

Generic system administrator passwords

6.4.106. Due to the system changes that are possible through the use of administrative passwords, appropriate password management when personnel leave will reduce the chances of information compromise

Privileged access accountability

6.4.107. Having thorough information on the operations of a system can better assist system administrators in their role, potentially having a positive flow on effect for the information security of the system.

REFERENCES

6.4.108. Additional information relating to privileged and system accounts, including monitoring, is contained in AS/NZS ISO/IEC 27001:2006, A.11.2.2, *Privilege Management*.

EXAMPLES

6.4.109. In a Linux system, controlled and accountable use of privileged accounts can be ensured by requiring system administrators to login using their own user identification and then a sudo to perform privileged actions.

6.4.110. A situation that would warrant the changing of generic system administrator passwords would be when a database administrator within a support section leaves the section to work within another part of the agency. In such circumstances the person must be prevented from using their privileged access in their new section unless they have a demonstrated requirement to do so.

Remote Access

PRINCIPLE

6.4.111. Remote access provides the means for personnel working off-site to connect to agency systems.

OBJECTIVE

6.4.112. To ensure that when remote access is implemented it is done in a sure manner that will not compromise agency systems.

CONTEXT

Scope

6.4.113. This section covers information relating to the method used by personnel to access an agency system from an off-site location to process or store information.

RISKS

6.4.114. An attacker takes advantage of inadequate authentication controls to gain remote access to an agency system, resulting in the compromise of information.

6.4.115. An attacker compromises a remote connection of a privileged system user, gaining privileged remote access to an agency system.

CONTROLS

[U,IC-HP,R-TS] Authentication

6.4.116. Agencies **must** authenticate each remote connection prior to permitting access to an agency system.

6.4.117. Agencies **should** authenticate both the remote system user and device during the authentication process.

[–,HP,C-TS] Remote privileged access

6.4.118. Agencies **must not** allow the use of privileged access remotely, including logging in as an unprivileged system user and then escalating privileges.

GUIDANCE

[U,IC-P,R] Remote privileged access

6.4.119. It is **recommended** that agencies do not allow the use of privileged access remotely, including logging in as an unprivileged system user and then escalating privileges.

RATIONALE

Authentication

6.4.120. Authenticating remote system users and devices ensures that only authorised system users and devices are allowed to connect to agency systems.

Event Logging and Auditing

PRINCIPLE

6.4.121. Correctly configured event logging will provide a sufficient level of detail on actions conducted on a system and allows for more accurate and effective auditing to be conducted.

OBJECTIVE

6.4.122. To ensure that logged information is stored appropriately and reviewed regularly.

CONTEXT

Scope

6.4.123. This section covers information covering the automatic logging of information relating to network activities. Information regarding manual logging of system management activities can be found in the *Privileged Access* section of this manual.

RISKS

6.4.124. A system user with a privileged account abuses the use of their privileges, breaching the agency's ISP.

6.4.125. A system user intentionally or inadvertently violates their ISP, reducing the security posture of the system.

6.4.126. A system user performs a malicious act on a system, which goes undetected and unhindered, leading to unauthorised information leakage or damage to the system or data it contains.

6.4.127. An attacker performs an information security breach of a system that cannot be properly investigated due to a lack of sufficient event logging.

6.4.128. An attacker modifies event logs to cover their actions, resulting in their presence remaining undetected or the full extent of their actions never being discovered.

6.4.129. A privileged user with malicious intent modifies event logs in order to hide abuse of those privileges, resulting in the abuse remaining undetected.

6.4.130. An agency does not adequately manage audit requirements, which allows information security violations to go unnoticed or to be inadequately addressed.

CONTROLS

[U,IC-HP,R-TS] Logging requirements

6.4.131. Agencies **must** develop and document logging requirements covering:

a. the logging facility, including:
   1) log server availability requirements, and
   2) the reliable delivery of log information to the log server
b. the list of events associated with a system or software component to be logged; and
c. event log protection and archival requirements.

[–,HP,C-S] Events to be logged

6.4.132. Agencies **should** log, at a minimum, the following events for all software components:

a. all privileged operations
b. failed attempts to elevate privileges
c. security related system alerts and failures
d. system user and group additions, deletions and modification to permissions, and
e. unauthorised access attempts to systems and files identified as critical to the agency.

[–,–,TS] Events to be logged

6.4.133. Agencies **must** log, at a minimum, the following events for all software components:

a. all privileged operations
b. failed attempts to elevate privileges
c. security related system alerts and failures
d. system user and group additions, deletions and modification to permissions, and
e. unauthorised access attempts to systems and files identified as critical to the agency.

[–,HP,C-TS] Events to be logged

6.4.134. Agencies **must** log the following events for all software components:

a. logons
b. failed logon attempts, and
c. logoffs.

[U,IC-HP,R-TS] Event log facility

6.4.135. For each event identified as needing to be logged, agencies **must** ensure that the log facility records at least the following details, where applicable:

a. date and time of the event
b. relevant system user(s) or process
c. event description
d. success or failure of the event
e. event source (e.g. application name), and
f. terminal location/identification.

[U,IC-HP,R-TS] Event log protection

6.4.136. Event logs **must** be protected from:

a. modification and unauthorised access, and
b. whole or partial loss within the defined retention period.

[U,IC-HP,R-TS] Event log archival

6.4.137. Event logs **must** be archived and retained for an appropriate period as determined by the agency.

[–,HP,C-TS] Remote logging

6.4.138. Agencies **should** configure systems to save event logs to separate secure servers as soon as possible after each event occurs.

[U,IC-HP,R-TS] Audit requirements

6.4.139. Agencies **must** develop and document audit requirements covering:

a. the scope of audits
b. the audit schedule
c. action to be taken when violations are detected
d. reporting requirements, and
e. specific responsibilities.

6.4.140. The system owner **should** be responsible for determining the audit requirements of a system, consistent with the requirements of the ISP and SRMP.

GUIDANCE

[U,IC-P,R] Events to be logged

6.4.141. It is **recommended** that agencies log, at a minimum, the following events for all software components:

a. all privileged operations
b. failed attempts to elevate privileges
c. security related system alerts and failures
d. system user and group additions, deletions and modification to permissions, and
e. unauthorised access attempts to systems and files identified as critical to the agency.

[U,IC-HP,R-TS] Additional events to be logged

6.4.142. It is **recommended** that agencies log the events listed in the table below for specific software components:

SOFTWARE COMPONENT	EVENTS TO LOG
Database	• System user access to the database. • Attempted access that is denied. • Changes to system user roles or database rights. • Addition of new system users, especially privileged users. • Modifications to the data. • Modifications to the format of the database.
Network/operating system	• Successful and failed attempts to logon and logoff. • Changes to system administrator and system user accounts. • Failed attempts to access data and system resources. • Attempts to use special privileges. • Use of special privileges. • System user or group management. • Changes to the security policy. • Service failures and restarts. • System startup and shutdown. • Changes to system configuration data. • Access to sensitive data and processes. • Data export operations.

Continued on next page

SOFTWARE COMPONENT	EVENTS TO LOG
Web application	• System user access to the Web application. • Attempted access that is denied. • System user access to the Web documents. • Search engine queries initiated by system users.

[U,IC-HP,R-TS] Event log facility

6.4.143. It is **recommended** that agencies establish an accurate time source and use it consistently throughout their systems to assist with the correlation of logged events across multiple systems.

[U,IC-HP,R-TS] Event log protection

6.4.144. It is **recommended** that agencies ensure that:

a. systems are configured to save event logs to a separate secure log server, and
b. event log data be archived in a manner that maintains its integrity.

[U,IC-HP,R-TS] Event log archival

6.4.145. It is **recommended** that agencies seek advice to determine if their access and event logs are subject to the Archives Act.

6.4.146. It is **recommended** that agencies retain DNS and proxy logs for at least 18 months.

RATIONALE

Logging requirements

6.4.147. Event logging can help raise the security posture of a system by increasing the accountability for all system user actions.

6.4.148. Event logging can increase the chances that malicious behaviour will be detected by logging the actions of a malicious party.

6.4.149. Well configured event logging allows for easier and more effective auditing if an information security incident occurs.

Event log facility

6.4.150. The act of logging events is not enough in itself. For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed.

Event log protection

6.4.151. Effective log protection and storage (possibly involving the use of a dedicated event logging server) will help ensure the integrity and availability of the collected logs when they are audited.

Audit requirements

6.4.152. Conducting audits of events should been seen as an integral part of the maintenance of systems, as they will assist in the detection and attribution of any violations of agency security policy—including information security incidents, breaches and intrusions.

REFERENCES

6.4.153. Additional information relating to event logging is contained in AS/NZS ISO/IEC 27001:2006, A.10.10, *Monitoring*.

Cryptographic Security

Cryptographic Fundamentals

PRINCIPLE

6.5.1. The degree of assurance in a DCE is associated with the degree of assurance in the associated formal evaluation of the product. The greater the level of assurance in the formal evaluation of the product the greater the level of assurance there will be in the associated cryptographic evaluation.

OBJECTIVE

6.5.2. To allow agencies to use encryption to reduce the storage and physical transfer requirements for information as outlined in the PSM.

CONTEXT

Scope

6.5.3. This section covers information on the fundamentals of cryptography including the use of encryption to protect data at rest and in transit. Detailed information on algorithms and protocols approved to protect information can be found in the *DSD Approved Cryptographic Algorithms* and *DSD Approved Cryptographic Protocols* sections of this chapter.

Purpose of cryptography

6.5.4. Encryption is primarily used to provide confidentiality—protecting against the security risk of information being intercepted by an attacker. More broadly, cryptography can provide authentication, non-repudiation and integrity.

6.5.5. The use of approved encryption will generally reduce the likelihood of an unauthorised party gaining access to the encrypted information. However, it does not reduce the consequences of a successful attack.

6.5.6. Care needs to be taken with encryption systems that do not encrypt the entire media content to ensure that either all of the security classified data is encrypted or that the media is handled in accordance with the highest security classification of the unencrypted data.

Using encryption

6.5.7. Encryption of data at rest can be used to reduce the physical storage and handling requirements of the media or systems containing the information.

6.5.8. Encryption of data in transit can be used to provide protection for information being communicated over communication mediums and hence reduce the security requirements of the communication medium.

6.5.9. When agencies use encryption for data at rest or in transit, they are not reducing the security classification of the information. When encryption is used the consequences of the potential disclosure of the information is considered to be less, and as such, the PSM requirements for a lower security classification can be considered to be more appropriate to the state of the information. As the security classification of the information does not change, agencies cannot use the lowered storage, physical transfer or security requirements as a baseline to further lower requirements with an additional cryptographic product.

6.5.10. In each case, the level of assurance in the encryption is defined in terms of Common Criteria EALs, or in some cases DACAs or DSD approved cryptographic protocols (DACPs).

Product specific cryptographic requirements

6.5.11. While this section provides requirements for the use of cryptography to protect information. Additional requirements can exist in consumer guides for products once they have completed a DCE. Such requirements supplement this manual and where conflict occurs the product specific requirements take precedence.

Exceptions for using cryptographic products

6.5.12. Agencies using a product that implement a DACP or DACA to provide protection of X-IN-CONFIDENCE data at rest or in transit do not need to have undergone a DCE. Similarly when agencies are using cryptographic functionality within a product to lower requirements where the requirement is a DACP or DACA do not need to use a product that has undergone a DCE.

Federal Information Processing Standard 140

6.5.13. The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of cryptographic modules—both hardware and software.

6.5.14. FIPS 140 is in its second iteration and is formally referred to as FIPS 140-2. This section refers to the standard as FIPS 140 but applies to both FIPS 140-1 and FIPS 140-2. The third iteration, FIPS 140-3, has been released in draft and this section also applies to that iteration.

6.5.15. FIPS 140 is not a substitute for a DCE of a product with cryptographic functionality. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other information security functionality.

6.5.16. Cryptographic evaluations of products will normally be conducted by DSD. Where a product's cryptographic functionality has been validated under FIPS 140, DSD can, at its discretion, and in consultation with the vendor, reduce the scope of a DCE.

6.5.17. DSD will review the FIPS 140 validation report to confirm compliance with Australia's national cryptographic policy.

Communicating with private citizens and businesses

6.5.18. Private citizens and businesses are not bound by the controls relating to the protection of data at rest and in transit within this manual. As such the requirements for the protection of data at rest and in transit do not apply when communicating with private citizens and businesses.

RISKS

6.5.19. An attacker finds and exploits vulnerabilities in a cryptographic product being used by an agency that has not undergone a DCE, or cryptographic evaluation recognised by DSD, resulting in the disclosure of information.

6.5.20. An attacker reads information that is stored or communicated without any cryptographic protection.

6.5.21. An attacker finds and exploits a weakness in a cryptographic product with insufficient assurance for the information it is used to protect, resulting in an ability to access the information.

6.5.22. An attacker captures personal communications between a private citizen or business and an agency, resulting in a loss of confidentiality.

CONTROLS

[–,IC-HP,R] Using cryptographic products

6.5.23. Agencies using cryptographic functionality within a product for the protection of security classified information **must** ensure that the product has completed a DCE or other cryptographic evaluation recognised by DSD.

[–,–,C-TS] Using cryptographic products

6.5.24. Agencies using cryptographic functionality within HGCE for the protection of security classified information **must** ensure that the product has completed a DCE or other cryptographic evaluation recognised by DSD.

[U,IC-HP,R] Data recovery

6.5.25. Where practical, cryptographic products **must** provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

[–,–,C-TS] Data recovery

6.5.26. Where practical, cryptographic products are **required** to provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

[–,IC-HP,R] Reducing storage and physical transfer requirements

6.5.27. If an agency wishes to use encryption to reduce the storage or physical transfer requirements, as outlined in the PSM, for equipment or media that contains security classified information, they **must** use an encryption product that meets the minimum level of assurance as shown in the following table.

ORIGINAL SECURITY CLASSIFICATION	CRYPTOGRAPHIC PRODUCT ASSURANCE OR ALGORITHM ASSURANCE LEVEL MANDATED TO REDUCE SECURITY REQUIREMENTS		
	P/C	IC/R	U
IC	-	-	DACA
R	-	-	EAL2
P	-	DACA	EAL2
HP	DACA	EAL2	EAL4

6.5.28. If an agency wishes to use encryption to reduce the storage or physical transfer requirements, as outlined in the PSM, for equipment or media that contains security classified information, they **should** use:

a. full disk encryption, or
b. partial encryption where the access control will only allow writing to the encrypted partition.

[–,–,C-TS] Reducing storage and physical transfer requirements

6.5.29. If an agency wishes to use encryption to reduce the storage or physical transfer requirements, as outlined in the PSM, for equipment or media that contains security classified information, they are **required** to use HGCE.

6.5.30. If an agency wishes to use encryption to reduce the storage or physical transfer requirements, as outlined in the PSM, for equipment or media that contains security classified information, they are **required** to use:

a. full disk encryption, or
b. partial encryption where the access control will only allow writing to the encrypted partition.

[–,IC-HP,R-TS] Reducing storage and physical transfer requirements

6.5.31. When equipment storing encrypted information is turned on and authenticated it **must** be treated as per the original security classification of the equipment.

[–,IC-HP,R-TS] Product specific requirements

6.5.32. Agencies **must** check consumer guides for products, where available, to determine any product specific requirements.

6.5.33. Where product specific requirements exist in a consumer guide, agencies **must** comply with the requirements outlined in the consumer guide.

[–,IC-HP,R] Reducing transit encryption requirements

6.5.34. Agencies **must** use encryption products that meet the minimum level of assurance, as shown in the following table, if they wish to use encryption to reduce the requirements for communicating security classified information over networks of a lower security classification than that of the information.

ORIGINAL SECURITY CLASSIFICATION	CRYPTOGRAPHIC PRODUCT ASSURANCE OR ALGORITHM ASSURANCE LEVEL MANDATED TO REDUCE SECURITY REQUIREMENTS			
	P	R	IC	U
IC	-	-	-	DACP
R	-	-	DACP	EAL2
P	-	DACP	DACP	EAL2
HP	DACP	EAL2	EAL2	EAL4

[–,–,C-TS] Reducing transit encryption requirements

6.5.35. Agencies are **required** to use HGCE if they wish to communicate security classified information over national security classified networks of a lower security classification, non-national security classified networks or UNCLASSIFIED networks.

[–,IC-HP,R-TS] Reducing transit encryption requirements

6.5.36. In addition to any encryption already in place for communication mediums, agencies **should** encrypt:

a. AUSTEO information if foreign nationals have access to the communication mediums or systems that can process the information
b. AGAO information if system users not authorised to access AGAO information have access to the communication mediums or systems that can process the information, and
c. AUSTEO or AGAO information if the communication mediums or systems that can process the information have not been accredited to handle the information.

6.5.37. Agencies **must**, at a minimum, use a DACP to protect AUSTEO and AGAO information.

[U,IC-HP,R-TS] Communicating with private citizens and businesses

6.5.38. When personal information is sent to a private citizen or business via electronic means, agencies **must** ensure that prior to sending the information they document any security risks that could be associated with the communication.

GUIDANCE

[U,IC-HP,R-TS] Communicating with private citizens and businesses

6.5.39. It is **recommended** that when personal information is sent to a private citizen or business via electronic means, agencies inform the entity of the security risks and seek their acceptance to undertake the communications.

6.5.40. The protection of personal information could be subject to the Privacy Act, as such, it is **recommended** that agencies seek legal advice before communicating with private citizens or businesses via electronic means.

RATIONALE

Using cryptographic products

6.5.41. No real-world product can ever be guaranteed to be free of vulnerabilities. The best that can be done is to increase the amount of assurance in a product to a point that represents satisfactory risk management. A product having a higher EAL has undergone a greater amount of assurance scrutiny and can therefore be used to protect information of a higher security classification.

6.5.42. If an agency uses a product that contains cryptographic functionality but the agency does not use this functionality then the product doesn't need to have undergone a DCE. Likewise if the agency is using the functionality but doesn't use it in a capacity to reduce the security requirements of the information, i.e. no assurance is afforded to the cryptographic functionality, then the product also doesn't need to have undergone a DCE.

Data recovery

6.5.43. The requirement for an encryption product to provide a key escrow function, where practical, was issued under a Cabinet directive in July 1998.

Communicating with private citizens and businesses

6.5.44. When agencies communicate with private citizens and businesses they need to be aware that private citizens and businesses are not bound by the requirements of this manual. As such the requirements for the protection of data in transit do not apply.

6.5.45. Even though the requirements do not apply to such communications, agencies should still make a reasonable effort to inform the private citizen or business of the security risks and seek their acceptance before undertaking the communications.

REFERENCES

6.5.46. Further information on the FIPS 140 standards can be found at:

- http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, and
- http://www.csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf.

6.5.47. The Office of the Privacy Commissioner has guidelines for agencies interacting with private citizens at http://www.privacy.gov.au.

DSD Approved Cryptographic Algorithms

PRINCIPLE

6.5.48. A wide array of cryptographic algorithms exists and many implementations of such algorithms are available, some of which are approved to protect the confidentiality and integrity of information.

OBJECTIVE

6.5.49. To allow agencies to use a DACA for the protection of information at certain security classifications without the need for a formal product and cryptographic evaluation.

CONTEXT

Scope

6.5.50. This section covers information on the cryptographic algorithms that DSD has approved for the protection of national security information up to RESTRICTED and non-national security information up to HIGHLY PROTECTED.

6.5.51. Implementations of the named algorithms in this section need to undergo a DCE before they can be approved to protect information above the security classification of X-IN-CONFIDENCE. Products relying on algorithms not listed as DACAs will not be accepted into evaluation.

Categories of approved algorithms

6.5.52. The approved algorithms fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

Approved asymmetric/public key algorithms

6.5.53. The approved asymmetric/public key algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Digital Signature Algorithm (DSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for agreeing on encryption session keys
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures, and
- Rivest-Shamir-Adleman (RSA) for digital signatures and passing encryption session keys or similar keys.

Approved hashing algorithms

6.5.54. The approved hashing algorithms are:

- Secure Hashing Algorithm 1 (i.e. SHA-1), and
- Secure Hashing Algorithm 2 (i.e. SHA-224, SHA-256, SHA-384 and SHA-512).

Approved symmetric encryption algorithms

6.5.55. The approved symmetric encryption algorithms are:

- Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and
- Triple Data Encryption Standard (3DES).

RISKS

6.5.56. An attacker intercepts information that is not protected by a robust encryption algorithm allowing them to decrypt and read the cleartext.

6.5.57. An attacker decrypts information that is encrypted with a key of insufficient length allowing them to read the cleartext.

6.5.58. An attacker spoofs the identity of some entity and from there gain access to information.

6.5.59. An attacker interferes with information thereby destroying its availability.

6.5.60. An attacker modifies information thereby compromising its integrity.

CONTROLS

[–,IC-HP,R-TS] Using DACAs

6.5.61. Agencies using an unevaluated product that implements a DACA **must** ensure that:

a. only DACAs can be used, and
b. any residual security risks have been determined and documented.

[–,IC-HP,R-TS] Using DH

6.5.62. Agencies using DH, for the approved use of agreeing on encryption session keys, **must** use a modulus of at least 1024 bits.

[–,IC-HP,R-TS] Using DSA

6.5.63. Agencies using DSA, for the approved use of digital signatures, **must** use a modulus of at least 1024 bits.

[–,IC-HP,R-TS] Using ECDH

6.5.64. Agencies using ECDH, for the approved use of agreeing on encryption session keys, **must** use a field/key size of at least 160 bits.

[–,IC-HP,R-TS] Using ECDSA

6.5.65. Agencies using ECDSA, for the approved use of digital signatures, **must** use a field/key size of at least 160 bits.

[–,IC-HP,R-TS] Using RSA

6.5.66. Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, **must** use a modulus of at least 1024 bits.

6.5.67. Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, **must** ensure that the public keys used for passing encrypted session keys are different to the keys used for digital signatures.

[–,IC-HP,R-TS] Approved symmetric encryption algorithms

6.5.68. Agencies using AES or 3DES **should not** use electronic codebook mode.

[–,IC-HP,R-TS] Using 3DES

6.5.69. 3DES **must** use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.

GUIDANCE

[–,IC-HP,R-TS] Approved asymmetric/public key algorithms

6.5.70. It is **recommended** that agencies use ECDH and ECDSA before using DH and DSA.

RATIONALE

DSD approved cryptographic algorithms

6.5.71. Usually there is no guarantee or proof of security of an algorithm against presently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. There have been some cases where theoretically impressive vulnerabilities have been found, however these results are not of practical application.

6.5.72. Where there are a range of possible key sizes for an algorithm, some of the smaller key sizes do not provide an adequate safety margin against attacks that might be found in the future. For example, future advances in number factorisation could render the use of smaller RSA moduli as a security vulnerability.

Using DACAs

6.5.73. If a product implementing a DACA has been inappropriately configured, it is possible that relatively weak cryptographic algorithms could be selected without the system user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

6.5.74. When configuring unevaluated products that implement a DACA, agencies can ensure that only the DACA can be used by disabling the unapproved algorithms within the products (preferred) or advising system users not to use them via a policy.

Approved symmetric encryption algorithms

6.5.75. The use of Electronic Code Book mode in block ciphers allows repeated patterns in plaintext to appear as repeated patterns in the ciphertext. Most cleartext, including written language and formatted files, contains significant repeated patterns. An attacker can use this to deduce possible meanings of ciphertext by comparison with previously intercepted data. In other cases they might be able to determine information about the key by inferring certain contents of the cleartext. The use of other modes such as Cipher Block Chaining, Cipher Feedback, Output Feedback or Counter prevents such attacks.

REFERENCES

6.5.76. The following references are provided for the approved asymmetric/public key algorithms, hashing algorithms and encryption algorithms.

6.5.77. Further information on DH can be found in W. Diffie and M. E. Hellman, 'New Directions in Cryptography', *IEEE Transactions on Information Theory*, vol. 22, is. 6, pp. 644-654, November 1976.

6.5.78. Further information on DSA can be found in FIPS 186.

6.5.79. Further information on ECDH can be found in ANSI X9.63 and ANSI X9.42.

6.5.80. Further information on ECDSA can be found in FIPS 186-2 + Change Notice, ANSI X9.63 and ANSI X9.62

6.5.81. Further information on RSA can be found in Public Key Cryptography Standards #1, RSA Laboratories.

6.5.82. Further information on SHA can be found in AS 2805.13.3 and FIPS 180-2.

6.5.83. Further information on AES can be found in FIPS 197.

6.5.84. Further information on 3DES can be found in AS 2805.5.4 and ANSI X9.52.

DSD Approved Cryptographic Protocols

PRINCIPLE

6.5.85. A wide array of protocols exist that implement cryptographic algorithms, some of these protocols are approved to protect the confidentiality and integrity of information.

OBJECTIVE

6.5.86. To allow agencies to use a DACP that implements a DACA for the protection of information at certain security classifications without the need for a formal product and cryptographic evaluation.

CONTEXT

Scope

6.5.87. This section covers information on some of the cryptographic protocols that DSD has approved for the protection of national security information up to RESTRICTED and non-national security information up to HIGHLY PROTECTED.

6.5.88. Implementations of the named protocols in this section need to undergo a DCE before they can be approved to protect information above the security classification of X-IN-CONFIDENCE.

6.5.89. Protocols other than those named in this section can be use for the protection of information above X-IN-CONFIDENCE if they use DACAs and are found suitably implemented within a product that has undergone a DCE.

6.5.90. Agencies implementing a protect that uses a DACP will need to consult the requirements for cryptographic fundamentals and DACAs, as well as protocol specific requirements, as outlined in the relevant sections of this chapter.

Approved protocols

6.5.91. The approved cryptographic protocols are:

- Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- Secure Shell (SSH)
- Secure Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format, and
- Internet Protocol Security (IPSec).

RISKS

6.5.92. An attacker intercepts communications in one or both directions under a weak protocol, or a weakly configured protocol, and from this gains unauthorised access to information.

6.5.93. An attacker intercepts communications in one or both directions under a weak protocol, or a weakly configured protocol, and from this falsely claims or appears to be a legitimate identity.

6.5.94. An attacker intercepts communications in one or both directions under a weak protocol, or a weakly configured protocol, and from this interferes with the information.

CONTROLS

[–,IC-HP,R-TS] Using DACPs

6.5.95. Agencies using an unevaluated product that implements a DACP **must** ensure that:

a. only DACAs can be used, and
b. any residual security risks have been determined and documented.

RATIONALE

DSD approved cryptographic protocols

6.5.96. In general, DSD only approves the use of cryptographic products that have passed a formal evaluation. However, DSD approves the use of some commonly available cryptographic protocols even though their implementations within specific products have not been formally evaluated by DSD. This approval is limited to cases where they are used in accordance with the requirements in this manual.

Using DACPs

6.5.97. If a product implementing a DACP has been inappropriately configured, it is possible that relatively weak cryptographic algorithms could be selected without the system user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

6.5.98. When configuring unevaluated products that implement a DACP, agencies can ensure that only the DACA can be used by disabling the unapproved algorithms within the products (which is preferred) or advising system users not to use them via a policy.

6.5.99. While many DACPs support authentication, agencies should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms must also be securely implemented and protected. This can be achieved by:

- providing an assurance of private key protection
- ensuring the correct management of certificate authentication processes including certificate revocation checking, and
- using a legitimate identity registration scheme.

Secure Sockets Layer and Transport Layer Security

PRINCIPLE

6.5.100. SSL/TLS can be used as a DACP to protect data in transit.

OBJECTIVE

6.5.101. To ensure that if agencies use SSL or TLS it is configured securely.

CONTEXT

Scope

6.5.102. This section covers the conditions under which SSL and TLS can be used as DACPs. Additionally, as File Transfer Protocol over SSL is built on SSL/TLS it is also considered within scope.

6.5.103. When using a product that implements SSL/TLS, requirements for using DACPs will also need to be referenced in the *DSD Approved Cryptographic Protocols* section of this chapter.

RISKS

6.5.104. An attacker exploits known security flaws in older versions of SSL to gain access to information.

6.5.105. An agency configures SSL/TLS in a poor manner resulting in the protocol being insufficiently secure for purpose.

CONTROLS

[–,IC-HP,R-TS] Using SSL and TLS

6.5.106. Agencies **should not** use versions of SSL prior to version 3.0.

6.5.107. Agencies permitting SSL or TLS through their gateway/CDS **should** implement:

a. a product that decrypts and applies content filtering to SSL traffic, or
b. a whitelist specifying the external addresses to which encrypted connections are permitted, with all other addresses blocked.

GUIDANCE

[–,IC-HP,R-TS] Inspection of SSL and TLS traffic

6.5.108. It is **recommended** that agencies seek legal advice regarding the inspection of encrypted SSL or TLS traffic by their gateway/CDS.

[–,IC-HP,R-TS] Using SSL and TLS

6.5.109. It is **recommended** that agencies using a whitelist on their gateway/CDS to specify the external addresses to which encrypted connections are permitted specify whitelist addresses by domain name or IP address.

RATIONALE

Secure Sockets Layer and Transport Layer Security

6.5.110. SSL and TLS do not protect data during storage. As a result, there is usually a greater security risk that data will be accessed while stored at either end of the communication path, where SSL/TLS does not protect it.

REFERENCES

6.5.111. Further information on SSL and TLS can be found in:

- the SSL 3.0 specification at http://wp.netscape.com/eng/ssl3, and
- the TLS 1.1 definition at http://tools.ietf.org/html/rfc4346.

Secure Shell

PRINCIPLE

6.5.112. SSH can be used as a DACP to protect data in transit.

OBJECTIVE

6.5.113. To ensure that if agencies use SSH it is configured securely.

CONTEXT

Scope

6.5.114. This section covers information on the conditions under which commercial and open-source implementations of SSH can be used as a DACP. Additionally, secure copy and Secure File Transfer Protocol use SSH and are therefore also covered by this section.

6.5.115. When using a product that implements SSH, requirements for using DACPs will also need to be referenced from the *DSD Approved Cryptographic Protocols* section of this chapter.

RISKS

6.5.116. An attacker conducts a man-in-the-middle attack, capturing security classified unencrypted information, and continues to use the open session for malicious purposes.

6.5.117. An attacker exploits a server that accepts password authentication by automating the brute-forcing of password attempts over a long period of time, eventually gaining access to the server.

6.5.118. An agency approves the use of remote root/administrator access for backups, however a lack of control leads to unauthorised root access occurring.

6.5.119. An agency enables Transmission Control Protocol port forwarding, allowing a system user to obtain access to another system to which they should not have access.

6.5.120. An attacker passively collects SSH-agent passwords or keys sent in the clear as part of Transmission Control Protocol packets to gain access to agency ICT assets.

CONTROLS

[–,IC-HP,R-TS] Using SSH

6.5.121. The table below outlines the settings that **should** be implemented.

CONFIGURATION DESCRIPTION	CONFIGURATION DIRECTIVE
Disallow the use of SSH version 1	Protocol 2
On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces	ListenAddress xxx.xxx.xxx.xxx
Disable connection forwarding	AllowTCPForwarding no
Disable gateway ports	Gatewayports no

Continued on next page

CONFIGURATION DESCRIPTION	CONFIGURATION DIRECTIVE
Disable the ability to login directly as root	PermitRootLogin no
Disable host-based authentication	HostbasedAuthentication no
Disable rhosts-based authentication	RhostsAuthentication no IgnoreRhosts yes
Do not allow empty passwords	PermitEmptyPasswords no
Configure a suitable login banner	Banner/directory/filename
Configure a login authentication timeout of no more than 60 seconds	LoginGraceTime xx
Disable X forwarding	X11Forwarding no

[–,IC-HP,R-TS] Authentication mechanisms

6.5.122. Agencies **should** use public key-based authentication before using password-based authentication.

6.5.123. Agencies that allow password authentication **should** use techniques to block brute force attempts against the password.

[–,IC-HP,R-TS] Automated remote access

6.5.124. Agencies that use logins without a password for automated purposes **should**, where possible, disable:

a. access from Internet Protocol addresses that do not need access
b. port forwarding
c. agent credential forwarding
d. X11 display remoting, and
e. console access.

6.5.125. Agencies that use remote access without the use of a password **should** use the 'forced command' option to specify what command is executed.

[–,IC-HP,R-TS] SSH-agent

6.5.126. Agencies that use SSH-agent or other similar key caching programs **should**:

a. only use the software on workstation and servers with screenlocks
b. ensure that the key cache expires within four hours of inactivity, and
c. ensure that agent credential forwarding is used when multiple SSH transversal is needed.

GUIDANCE

[–,IC-HP,R-TS] Automated remote access

6.5.127. It is **recommended** that agencies use parameter checking when using the 'forced command' option.

RATIONALE

Secure Shell

6.5.128. SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to a man-in-the-middle attack, where an attacker who can intercept the protocol in each direction can make each node believe they are talking to the other. SSH version 2 does not have this vulnerability.

Using SSH

6.5.129. The configuration directives provided are based on the OpenSSH implementation of SSH. Agencies implementing SSH will need to adapt these settings to suit other SSH implementations.

6.5.130. SSH has the ability to forward connections and access privileges in a variety of ways. This means that an attacker who can exploit any of these features can gain unauthorised access to a potentially large amount of information.

6.5.131. Host-based authentication requires no credentials (password, public key etc.) to authenticate (though in some cases it might make use of a host key). This renders SSH vulnerable to an Internet Protocol spoofing attack.

6.5.132. An attacker who gains access to a system with system administrator privileges will have the ability to not only access information but to control that system completely. Given the clearly more serious consequences of this, system administrator login should not be permitted.

REFERENCES

6.5.133. Further information on SSH can be found in the SSH specification at http://tools.ietf.org/html/rfc4252.

Secure Multipurpose Internet Mail Extension

PRINCIPLE

6.5.134. S/MIME can be used as a DACP to protect data in transit.

OBJECTIVE

6.5.135. To ensure that if agencies use S/MIME it is configured securely.

CONTEXT

Scope

6.5.136. This section covers information on the conditions under which S/MIME can be used as a DACP.

6.5.137. When using a product that implements S/MIME, requirements for using DACPs will also need to be referenced from the *DSD Approved Cryptographic Protocols* section of this chapter.

6.5.138. Information relating to the development of password selection policies and password requirements can be found in the *Identification and Authentication* section of this manual.

RISKS

6.5.139. An attacker attacks a weak implementation of the protocol thereby gaining unauthorised access to information.

6.5.140. An attacker exploits vulnerabilities in older versions of the protocol thereby gaining unauthorised access to information.

CONTROLS

[–,IC-HP,R-TS] Using S/MIME

6.5.141. Agencies **should not** allow versions of S/MIME earlier than 3.0 to be used.

6.5.142. Agencies **must** enforce the use of the agency password policy for selecting passwords to use with S/MIME.

RATIONALE

Using S/MIME

6.5.143. S/MIME 2.0 required the use of weaker cryptography (40-bit keys) than is approved for use by the Australian Government. Version 3.0 was the first version to become an Internet Engineering Taskforce standard.

6.5.144. Agencies choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and any attachments for inappropriate content, and for server-based antivirus software to scan for viruses and other malicious code.

REFERENCES

6.5.145. Further information on S/MIME can be found in the S/MIME charter at http://www.ietf.org/html.charters/smime-charter.html.

OpenPGP Message Format

PRINCIPLE

6.5.146. The OpenPGP Message Format can be used as a DACP to protect data in transit.

OBJECTIVE

6.5.147. To ensure that if agencies use the OpenPGP Message Format it is configured securely.

CONTEXT

Scope

6.5.148. This section covers information on the conditions under which the OpenPGP Message Format can be used as a DACP. It applies to the protocol as specified in IETF's RFC 2440 and RFC 4880, which obsoletes RFC 2440.

6.5.149. When using a product that implements the OpenPGP Message Format, requirements for using DACPs will also need to be referenced from the *DSD Approved Cryptographic Protocols* section of this chapter.

6.5.150. Information relating to the development of password selection policies and password requirements can be found in the *Identification and Authentication* section of this manual.

RISKS

6.5.151. An attacker launches malicious code onto a machine on which OpenPGP Message Format is used, thereby gaining access to passwords or keys which in turn would give access to cleartext.

6.5.152. An attacker launches a password-guessing attack (such as a dictionary attack) to find the key, thereby allowing decryption and unauthorised access to cleartext

6.5.153. An attacker exploits properties of insufficiently strong hashing algorithms to gain information about the private key or cleartext from the message signature.

CONTROLS

[–,IC-HP,R-TS] Using OpenPGP Message Format

6.5.154. Agencies **should** ensure that systems on which OpenPGP Message Format messages are accessed are sufficiently hardened to protect against malicious code.

6.5.155. Agencies **must** enforce the use of the agency password policy for selecting passwords to use with the OpenPGP Message Format.

RATIONALE

Using OpenPGP Message Format

6.5.156. Passwords need to be strong to protect the keys in order to prevent attacks such password guessing attacks including dictionary attacks.

REFERENCES

6.5.157. Further information on the OpenPGP Message Format can be found in the OpenPGP Message Format specification at http://tools.ietf.org/html/rfc4880.

Internet Protocol Security

PRINCIPLE

6.5.158. IPSec can be used as a DACP to protect data in transit.

OBJECTIVE

6.5.159. To ensure that if agencies use IPSec it is configured securely.

CONTEXT

Scope

6.5.160. This section covers information on the conditions under which IPSec can be used as a DACP.

6.5.161. When using a product that implements IPSec, requirements for using DACPs will also need to be referenced from the *DSD Approved Cryptographic Protocols* section of this chapter.

Modes of operation

6.5.162. IPSec can be operated in two modes: transport mode or tunnel mode.

Cryptographic algorithms

6.5.163. Most IPSec implementations can handle a number of cryptographic algorithms for encrypting data when the Encapsulating Security Payload (ESP) protocol is used. These include 3DES and AES.

Key exchange

6.5.164. Most IPSec implementations handle a number of methods for sharing keying material used in hashing and encryption processes. Two common methods are manual keying and Internet Key Exchange (IKE) using the Internet Security Association Key Management Protocol (ISAKMP). Both methods are considered suitable for use.

ISAKMP authentication

6.5.165. Most IPSec implementations handle a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonces or pre-shared keys. These methods are considered suitable for use.

ISAKMP modes

6.5.166. ISAKMP uses two modes to exchange information as part of IKE. These are main mode and aggressive mode.

RISKS

6.5.167. An attacker analysing IPSec traffic operating in transport mode gains information that allows traffic analysis activities to be undertaken.

6.5.168. An attacker capturing cleartext IPSec traffic and reads the traffic contents.

6.5.169. An attacker modifies the contents of IPSec traffic to cause a DoS attack.

6.5.170. An attacker exploiting vulnerabilities in the cryptographic algorithm used in the ESP protocol of an IPSec connection reads the traffic contents.

6.5.171. An attacker exploiting vulnerabilities in the underlying cryptographic hashing function used in hashed message authentication code (HMAC) to modify data without detection.

6.5.172. An attacker exploiting a small modulus size used in a DH key exchange can read the contents of encrypted traffic.

6.5.173. An attacker capturing cleartext information from an ISAKMP aggressive mode exchange can read security association identifier information.

6.5.174. An attacker compromising a security association of an IPSec connection can gather identification information including the knowledge of encryption algorithms and keys used to initiate them.

6.5.175. An attacker exploiting vulnerabilities in the IKE Extended Authentication (XAUTH) functionality of an IPSec gateway/CDS might be able to complete authorisation procedures.

CONTROLS

[–,IC-HP,R-TS] Mode of operation

6.5.176. Agencies **should** use tunnel mode for IPSec connections.

6.5.177. Agencies choosing to use transport mode **should** additionally use an Internet Protocol tunnel for IPSec connections.

[–,IC-HP,R-TS] Protocols

6.5.178. Agencies **should** use the ESP protocol for IPSec connections.

[–,IC-HP,R-TS] ISAKMP modes

6.5.179. Agencies using ISAKMP **should** disable aggressive mode for IKE.

[–,IC-HP,R-TS] Security association lifetimes

6.5.180. Agencies **should** use a security association lifetime of less than four hours or 14400 seconds.

GUIDANCE

[–,IC-HP,R-TS] HMAC algorithms

6.5.181. It is **recommended** that agencies use HMAC-SHA-1-96 as the HMAC algorithm.

[–,IC-HP,R-TS] DH groups

6.5.182. It is **recommended** that agencies use the largest modulus size available for the DH exchange.

[–,IC-HP,R-TS] Perfect Forward Secrecy

6.5.183. It is **recommended** that agencies use Perfect Forward Secrecy for IPSec connections.

[–,IC-HP,R-TS] IKE Extended Authentication

6.5.184. It is **recommended** that agencies disable the use of XAUTH for IPSec connections.

RATIONALE

Internet Protocol Security

6.5.185. In order to provide a secure virtual private network (VPN) style connection both authentication and encryption are needed. ESP is the only way of providing encryption yet Authentication Header (AH) and ESP can both provide authentication. It is possible to use ESP instead of AH, yet that is generally not used due to AHs limitation in regards to network address translation. If however maximum security is desired at the expense of such functionality, then ESP can be wrapped inside of AH to authenticate the entire Internet Protocol packet and not just the encrypted payload. Using ESP with authentication in tunnel mode provides full encapsulation of traffic across an un-trusted network by using both encryption and authentication.

ISAKMP modes

6.5.186. Using main mode instead of aggressive mode provides greater security since all exchanges are protected.

Security association lifetimes

6.5.187. Using a secure association lifetime of four hours or 14400 seconds provides a balance between security and usability.

DH groups

6.5.188. Using a larger DH group provides more entropy for the key exchange.

Perfect Forward Secrecy

6.5.189. Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

IKE Extended Authentication

6.5.190. XAUTH has documented vulnerabilities associated with its use.

REFERENCES

6.5.191. Further information on IPSec can be found in the security architecture for the Internet Protocol overview at http://tools.ietf.org/html/rfc2401.

Key Management

PRINCIPLE

6.5.192. The deployment of cryptographic equipment is ineffective without the appropriate implementation of cryptographic keying material. As keying material provides the real security, protection needs to be applied to ensure the integrity of that keying material.

OBJECTIVE

6.5.193. To ensure that a cryptographic system and its associated materials are managed appropriately to assist in mitigating the security risk of compromise.

CONTEXT

Scope

6.5.194. This section covers information relating to the general management of cryptographic system material. Due to the wide variety of cryptographic systems and technologies available, and the varied security risks for each, detailed key management guidance is not provided in this manual.

6.5.195. If HGCE is being used agencies are advised to consult the respective ACSI for the equipment.

Cryptographic systems

6.5.196. In general, the requirements specified for systems apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained in this section, and overrule all requirements specified elsewhere in this manual.

RISKS

6.5.197. An agency allows uncontrolled access to a cryptographic system and its materials, resulting in actions being made on the system without being directly attributable to an individual.

6.5.198. An agency fails to properly account for cryptographic system materials, resulting in an inability to identify when materials go missing and where they could have last resided.

6.5.199. An agency fails to audit records at regular intervals, or when there is a change in personnel, rendering controls to reduce uncontrolled access and loss of materials ineffective.

6.5.200. An agency becomes confused as to which standard(s), and their associated precedence(s), apply to their cryptographic system, adversely affecting its correct operation.

6.5.201. An agency fails to document the intent and implementation details of a cryptographic system and associated material, resulting in the agency having no baseline from which to ensure that configuration control processes are appropriately adhered to.

6.5.202. An agency fails to clearly define the roles and responsibilities of personnel in regards to administration, information security incident reporting and recovery actions for their cryptographic system, resulting in the system operating outside its intended configuration without the agency noticing.

CONTROLS

[U,IC-HP,R-TS] High grade cryptography

6.5.203. Agencies are **required** to comply with ACSI 53 and ACSI 105 when using HGCE.

[U,IC-HP,R-TS] Unkeyed commercial grade cryptography

6.5.204. Unkeyed commercial grade cryptographic equipment **must** be distributed and managed by a means approved for the transportation and management of government property.

[U,IC-HP,R-TS] Keyed commercial grade cryptography

6.5.205. Keyed commercial grade cryptographic equipment **must** be distributed, managed and stored by a means approved for the transportation and management of government property based on the security classification of the key within the equipment.

[U,IC-HP,R-TS] Cryptographic system administrator access

6.5.206. Before personnel are granted cryptographic system administrator access, agencies **must** ensure that they:

a. has a demonstrated need for access
b. has read and agreed to comply with the relevant key management plan (KMP) for the cryptographic system they are using
c. possess a security clearance at least equal to the highest security classification of information processed by the system
d. has agreed to protect the authentication information for the system at the highest security classification of information it secures
e. has agreed not to share authentication information for the system without approval
f. has agreed to be responsible for all actions under their accounts, and
g. has agreed to report all potentially security related problems to an ITSM or the ASA.

[U,IC-HP,R-TS] Accounting

6.5.207. Agencies **should** be able to readily account for all transactions relating to cryptographic system material including identifying hardware and software: that had been issued with the equipment and materials, when they were issued, and where they were issued.

[U,IC-HP,R-TS] Audits

6.5.208. Agencies **should** conduct audits of cryptographic system material:

a. on handover/takeover of administrative responsibility for the cryptographic system
b. on change of personnel with access to the cryptographic system, and
c. at least annually.

[U,IC-HP,R-TS] Area security and access control

6.5.209. Cryptographic system equipment **should** be stored in a room that meets the requirements for a server room of an appropriate level based on the security classification of information the system processes.

6.5.210. Areas in which cryptographic system material is used **should** be separated from other areas and designated as a cryptography controlled area.

[U,IC-P,R] Developing KMPs

6.5.211. Agencies **should** develop a KMP when they have implemented a cryptographic system.

[–,HP,–] Developing KMPs

6.5.212. Agencies **must** develop a KMP when they have implemented a cryptographic system.

[–,–,C-TS] Developing KMPs

6.5.213. Agencies are **required** to develop a KMP when they have implemented a cryptographic system.

[U,IC-HP,R-TS] Contents of KMPs

6.5.214. The table below describes the minimum contents which **should** be documented in the KMP.

TOPIC	CONTENT
Objectives	• Objectives of the cryptographic system and KMP, including organisational aims.
References	• Relevant ACSIs. • Vendor documentation. • Related policies.
Security classification	• Security classification of the cryptographic system hardware. • Security classification of the cryptographic system software. • Security classification of the cryptographic system documentation.
System description	• Maximum security classification of information protected. • The use of keys. • The environment. • Administrative responsibilities. • Key algorithm. • Key length. • Key lifetime.
Topology	• Diagram(s) and description of the cryptographic system topology including data flows.
Key management	• Who generates keys. • How keys are delivered. • How keys are received. • Key distribution, including local, remote and central. • How keys are installed. • How keys are transferred. • How keys are stored. • How keys are recovered. • How keys are revoked. • How keys are destroyed.
Accounting	• How accounting will be undertaken for the cryptographic system. • What records will be maintained. • How records will be audited.
Maintenance	• Maintaining the cryptographic system software and hardware. • Destroying equipment and media.
Information security Incidents	• A description of the conditions under which compromise of key material should be declared. • References to procedures to be followed when reporting and dealing with information security incidents.

[U,IC-HP,R] Contents of KMPs

6.5.215. The level of detail included in a KMP **must** be consistent with the criticality and security classification of the information to be protected.

[–,–,C-TS] Contents of KMPs

6.5.216. The level of detail included in a KMP is **required** to be consistent with the criticality and security classification of the information to be protected.

GUIDANCE

[U,IC-HP,R-TS] Commercial grade cryptography

6.5.217. It is **recommended** that agencies do not transport equipment in a keyed state.

[U,IC-HP,R-TS] Access register

6.5.218. It is **recommended** that agencies hold and maintain an access register that records cryptographic system information such as:

a. details of personnel with system administrator access
b. details of those whose system administrator access was withdrawn
c. details of system documents
d. accounting activities, and
e. audit activities.

[U,IC-HP,R-TS] Audits

6.5.219. It is **recommended** that agencies perform audits to:

a. check all cryptographic system material as per the accounting documentation, and
b. to confirm that agreed security measures documented in the KMP are being followed.

6.5.220. It is **recommended** that agencies conduct audits using two personnel with cryptographic system administrator access.

RATIONALE

Key management

6.5.221. Most modern cryptographic systems are designed to be highly resistant to cryptographic analysis but it must be assumed that a determined attacker could obtain details of the cryptographic logic either by stealing or copying relevant material directly or by suborning an Australian national or allied national. The safeguarding of cryptographic system material by using adequate personnel, physical, documentation and procedural security measures is therefore crucial.

REFERENCES

6.5.222. Further information key management practices can be found in AS 11770.1:2003, *Information Technology – Security Techniques – Key Management*.

6.5.223. The following references can be consulted for additional information on high grade cryptography:

- ACSI 53, *Communications Security Handbook*, and
- ACSI 105, *Cryptographic Controlling Authorities and Keying Material Management*.

Network Security

Network Management

PRINCIPLE

6.6.1. Proper network management is based upon configuration management and retaining detailed up to date network diagrams.

OBJECTIVE

6.6.2. To ensure that network management decisions are made based on an accurate depiction of the status of the network.

CONTEXT

Scope

6.6.3. This section covers information relating to the documentation and management of network infrastructure.

Network diagrams

6.6.4. An agency's network diagram illustrates all network devices including firewalls, IDSs, routers, switches, hubs, etc. It does not need to illustrate all terminal devices on the network, such as workstations or printers, although the inclusion of significant devices such as servers could aid in its interpretation.

RISKS

6.6.5. An attacker targets an unmanaged section of an agency network, compromising the confidentiality, integrity and availability of the data contained on the network.

6.6.6. A system administrator makes an undocumented change to the network that exposes internal systems, inadvertently allowing unauthorised access to information.

6.6.7. An attacker makes a change to the configuration of communication equipment in order to access information on the network.

6.6.8. A system administrator makes a change to the network without understanding the impact to other parts of the network, inadvertently allowing unauthorised access to information, affecting the integrity of network data or denying network access to authorised system users.

6.6.9. An attacker intercepts traffic being communicated over the network, allowing them unauthorised access to information.

6.6.10. An attacker intercepts traffic relating to the management of the network, subsequently using this information to develop more focused attacks.

6.6.11. An attacker with access to one part of a network is able to propagate this access across other sections of the network which contain information or data of a higher security classification.

CONTROLS

[U,IC-HP,R-TS] Configuration management

6.6.12. Agencies **should** keep the network configuration under the control of a central network management authority.

6.6.13. All changes to the configuration **should** be:

a. approved through a formal change control process
b. documented, and
c. comply with the network security policy and security plan.

6.6.14. Agencies **should** regularly review their network configuration to ensure that it conforms to the documented network configuration.

[U,IC-HP,R-TS] Network diagrams

6.6.15. For each network an agency manages they **must** have:

a. a high-level diagram showing all connections into the network, and
b. a logical network diagram showing all communication equipment.

[U,IC-P,R] Updating network diagrams

6.6.16. An agency's network diagrams **should**:

a. be updated as network changes are made, and
b. include a 'Current as at [date]' statement on each page.

[–,HP,C-TS] Updating network diagrams

6.6.17. An agency's network diagrams **must**:

a. be updated as network changes are made, and
b. include a 'Current as at [date]' statement on each page.

[U,IC-HP,R-TS] Network configuration

6.6.18. Agencies **should** configure networks to limit opportunities for unauthorised access to information being communicated over the network.

[–,HP,C-TS] Limiting network access

6.6.19. Agencies **should** implement network access controls on all networks within an area if at least one system is security classified above PROTECTED or RESTRICTED within the physical space.

GUIDANCE

[U,IC-HP,R-TS] Management traffic

6.6.20. It is **recommended** that agencies implement protection measures to minimise the security risk of unauthorised access to network management traffic travelling across a network.

[U,IC-HP,R-TS] Network configuration

6.6.21. It is **recommended** that agencies deploy an automated tool that compares the running configuration of network devices against the documented configuration.

[U,IC-P,R] Limiting network access

6.6.22. It is **recommended** that agencies implement network access controls on all networks within an area if the systems located within the physical space are PROTECTED, RESTRICTED, X-IN-CONFIDENCE or UNCLASSIFIED.

RATIONALE

Configuration management

6.6.23. If the network is not centrally managed there could be sections of the network that do not comply with the agency's security policies.

6.6.24. Changes should be approved by a change management process, including representatives from all parties involved in the management of the network. This process ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the network.

Network diagrams

6.6.25. As most decisions are made on the documentation that illustrates the network, it is important that:

- a network diagram exists
- the network diagram is an accurate depiction of the network, and
- the network diagram indicates when it was last updated.

6.6.26. Due to the importance of the network diagram and decisions made based upon its contents, it should be updated as changes are made. This will assist system administrators to completely understand and adequately protect the network.

Limiting network access

6.6.27. If an attacker has limited opportunities to connect to a given network, they have limited opportunities to attack that network. Network access controls not only prevent against attackers propagating across a network but also prevent against system users carelessly connecting a network to another network of a different security classification. It is also useful in segregating sensitive or compartmented information for specific system users with a need-to-know.

6.6.28. Although circumventing some network access controls can be trivial, their use is primarily aimed at the protection they provide against accidental connection to another network.

Management traffic

6.6.29. Implementing protection measures specifically for management traffic provides another layer of defence on the network, should an attacker find an opportunity to connect to a given network. This also makes it more difficult for an attacker to enumerate their target network.

EXAMPLES

6.6.30. Limiting opportunities for unauthorised access to information being communicated over a network can be achieved by:

- using switches rather than hubs
- using routers/firewalls to isolate parts of the network on a need-to-know basis
- implementing encryption on the network, or
- using application-level encryption.

6.6.31. Implementing measures to protect access to management traffic being communicated over a network, can be achieved by:

- implementing network layer encryption, or
- creating a dedicated management network using physically separate or virtually separate infrastructure.

6.6.32. Implementing network access controls can be achieved by:

- using network access control protocols on all network ports (e.g. 802.1x)
- using static media access control to Internet Protocol address assignments for networks using the Dynamic Host Configuration Protocol, or
- using port security on network switches to:
  - limit access based on media access control addresses, or
  - disable all unused ports.

Virtual Local Area Networks

PRINCIPLE

6.6.33. Virtual local area networks (VLANs) implemented securely allow for multiple layer 3 networks to exist separately on a layer 2 switch, resulting in a network of computers behaving as if it were a member of the same physical local area network, even if located on separate segments.

OBJECTIVE

6.6.34. To ensure that VLANs are implemented within agencies in a secure manner.

CONTEXT

Scope

6.6.35. This section covers information relating to the use of VLANs within agency networks.

Multi Protocol Label Switching

6.6.36. For the purposes of this section Multi Protocol Label Switching is considered to be equivalent to VLANs and is subject to the same controls.

Exceptions for connectivity

6.6.37. A single network, managed in accordance with a single SSP, for which some separation is needed for administrative or similar reasons, can use VLANs to achieve that separation.

6.6.38. VLANs can also be used to separate IPT traffic from data traffic at the same security classification.

RISKS

6.6.39. An attacker on one VLAN intercepts frames from a second VLAN, compromising the confidentiality of the data on the second VLAN.

6.6.40. An attacker on one VLAN injects frames into a second VLAN, impacting the integrity of the data on the second VLAN.

6.6.41. A common switch allows traffic to pass between two VLANs of differing security classifications that share the switch, resulting in data leakage.

6.6.42. A system administrator modifies the switch configuration which connects to networks of a higher security classification than the one from which the system administrator is connecting, inadvertently causing a data leak.

6.6.43. An attacker bypasses the physical security of a switch, gaining access to the data it carries.

6.6.44. An attacker connects to an unused port on a switch and takes advantage of a switch vulnerability to intercept VLAN traffic.

6.6.45. An attacker takes advantage of VLAN trunking vulnerabilities to bypass VLAN filters, gaining the ability to communicate data across the VLAN.

CONTROLS

[U,IC-HP,R-TS] Connectivity

6.6.46. Agencies using VLANs to connect networks of the same security classification **must** accept the security risks associated with the activity.

[U,IC-HP,R] Connectivity

6.6.47. Agencies **should not** use VLANs between the networks with security classifications of:

a. HIGHLY PROTECTED and PROTECTED
b. PROTECTED and RESTRICTED
c. PROTECTED and X-IN-CONFIDENCE
d. RESTRICTED and X-IN-CONFIDENCE, and
e. X-IN-CONFIDENCE and UNCLASSIFIED.

6.6.48. Agencies **must not** use VLANs between the networks with security classifications of:

a. HIGHLY PROTECTED and RESTRICTED
b. HIGHLY PROTECTED and X-IN-CONFIDENCE
c. HIGHLY PROTECTED and UNCLASSIFIED
d. PROTECTED and UNCLASSIFIED, and
e. RESTRICTED and UNCLASSIFIED.

[–,–,C-TS] Connectivity

6.6.49. Agencies **must not** use VLANs between national security classified networks above CONFIDENTIAL and any other network of a different security classification.

[U,IC-HP,R-TS] Configuration and administration

6.6.50. Administrative access **must** only be permitted from the highest security classified network connected to a switch, or for networks of the same security classification, the most trusted network as determined by the accreditation authority.

6.6.51. Personnel with administrative access or unsupervised physical access to the switch **must** have a security clearance of at least the security classification of the highest security classified network carried on the switch.

[U,IC-HP,R-TS] Physical security

6.6.52. The physical security of the switch **must** meet the requirements for the highest security classified network carried on the switch.

[U,IC-HP,R-S] Disabling unused ports

6.6.53. Unused ports on the switches **should** be disabled.

[–,–,TS] Disabling unused ports

6.6.54. Unused ports on the switches **must** be disabled.

[U,IC-HP,R-TS] VLAN trunking

6.6.55. VLAN trunking **must not** be used on switches managing VLANs of differing security classifications.

RATIONALE

Connectivity

6.6.56. Limiting the sharing of a common switch between VLANs of differing security classifications reduces the chance of data leaks that could occur due to VLAN vulnerabilities.

Configuration and administration

6.6.57. When administrative access is limited to originating from the highest security classified network on a switch, the security risk of a data spill is reduced.

Physical security

6.6.58. Security classified network data is assured the appropriate physical security when a switch carrying the network data meets the physical security requirements for the highest security classified network carried on the switch.

Disabling unused ports

6.6.59. Disabling unused ports on a switch will reduce the attack landscape from which attacks could be launched.

VLAN Trunking

6.6.60. Disabling trunking on switches that carry VLANs of differing security classifications will reduce the security risk of data leakage across the VLANs due to VLAN vulnerabilities.

Wireless Local Area Networks

PRINCIPLE

6.6.61. Wi-Fi Protected Access 2 (WPA2) and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) are currently the most secure methods of ensuring the integrity and confidentiality of information communicated using 802.11-based wireless communications.

OBJECTIVE

6.6.62. To ensure that wireless local area networks (WLANs) are implemented within agencies in a secure manner secured by configuring wireless access points (WAPs) and clients to use appropriate cryptographic and authentication protocols.

CONTEXT

Scope

6.6.63. This section covers information on 802.11 WLANs. It does not cover other wireless communications. These communication methods are covered in the *Communications Systems and Devices* chapter of this manual.

RISKS

6.6.64. An attacker intercepts unencrypted WLAN transmissions, resulting in a loss of confidentiality.

6.6.65. An attacker uses cryptographic attacks to gain unauthorised access to information communicated by an encrypted WLAN.

6.6.66. An attacker uses authentication brute force attacks to gain unauthorised access to information communicated by an encrypted WLAN.

6.6.67. An attacker establishes a rogue WAP which an unaware target connects to, compromising information.

6.6.68. An attacker performs a WLAN man-in-the-middle attack and monitors WLAN communications.

6.6.69. An attacker supplies malicious or voluminous data to WLAN, causing a denial of service.

6.6.70. An attacker supplies malicious data to a WLAN client or WAP exploiting vulnerabilities in the device and subverting communications carried by the device.

6.6.71. A system user connects to a WLAN using a compromised device, resulting in unauthorised access to the WLAN.

6.6.72. An internal attacker uses their knowledge of encryption keys to decrypt WLAN data, gaining access to information traversing the WLAN.

6.6.73. An attacker can intentionally or unintentionally transmit in the same RF spectrum as a WLAN causing a denial of service of the network.

6.6.74. An attacker can transmit specific WPA2 management frames causing network clients to be disassociated from WAPs.

6.6.75. An attacker can exploit vulnerabilities in wireless device drivers and obtain full access to the network.

CONTROLS

[U,–,–] Providing wireless communications for public access

6.6.76. Agencies deploying a wireless network for public access **should** segregate the public access network from other agency systems.

[–,IC-HP,R-TS] Using wireless communications

6.6.77. Agencies **should** address the following vulnerabilities if they choose to use wireless communications:

a. man-in-the-middle and rogue WAP attacks
b. weak cryptography
c. unauthenticated system users brute-forcing authentication, and
d. availability requirements.

[–,–,TS] Using wireless communications

6.6.78. Agencies **must not** use wireless communications unless the security of the agency's wireless deployment has been approved by DSD.

[–,IC-HP,R-TS] Wired Equivalent Privacy

6.6.79. Agencies **must not** use Wired Equivalent Privacy (WEP) for wireless deployments.

[–,IC-HP,R-TS] Wi-Fi Protected Access

6.6.80. Agencies **should not** use Wi-Fi Protected Access for wireless deployments.

[–,IC-HP,R-TS] Authentication

6.6.81. Agencies **should** use WPA2 with EAP-TLS for wireless deployments.

6.6.82. Agencies not using WPA2 with EAP-TLS **should** use an authentication protocol that authenticates each end of the link.

[–,IC-HP,R-TS] Encryption

6.6.83. Agencies using wireless communications **must** ensure that security classified information is protected by cryptography that meets the assurance level mandated for the communication of information over UNCLASSIFIED network infrastructure.

[–,IC-HP,R-TS] Documentation

6.6.84. Key generation, distribution and rekeying procedures **should** be documented in a SSP for the wireless network.

6.6.85. Wireless device drivers and versions of wireless devices drivers and WAPs **should** be documented in the SSP for the wireless network.

[–,IC-HP,R-TS] Agency controlled devices

6.6.86. Agencies **must** determine the security risks associated with:

a. allowing non-agency accredited devices to connect to agency controlled wireless infrastructure, or
b. allowing agency accredited devices to connect to non-agency controlled wireless infrastructure.

GUIDANCE

[U,–,–] 802.11 deployment

6.6.87. It is **recommended** that agencies implement the requirements for security classified wireless networks.

[–,IC-HP,R-TS] 802.11 deployment

6.6.88. It is **recommended** that agencies take steps to ensure the confidentiality, integrity and authenticity of 802.11 management frames.

6.6.89. It is **recommended** that agencies do not use pre-shared keys for wireless authentication.

6.6.90. It is **recommended** that if pre-shared keys are to be used, agencies use random keys of the maximum allowable length.

[U,IC-HP,R-TS] RF controls

6.6.91. It is **recommended** that agencies limit the effective range of communications outside the agency's area of control by:

a. minimising the output power level of wireless devices, or
b. RF shielding.

RATIONALE

Using wireless communications

6.6.92. Security risks in wireless networks are equal to the sum of the security risk of operating a wired network plus the new security risks introduced by weaknesses in wireless protocols.

Wired Equivalent Privacy

6.6.93. WEP has serious flaws which allow it to be trivially compromised. A WEP network should be considered equivalent to an unprotected network.

Authentication

6.6.94. Authenticating each end of a wireless link will prevent a range of man-in-the-middle and rogue WAP attacks.

6.6.95. The use of WPA2 with EAP-TLS or an evaluated VPN solution will satisfy the requirement for mutual authentication and reduce the security risk of off-line brute-forcing of passwords when using pre-shared keys.

Documentation

6.6.96. Wireless device driver and WAP vulnerabilities are very exposed to the threat environment and require specific attention as exploits can gain immediate unauthorised access to the network.

802.11 deployment

6.6.97. The security risk of DoS attacks cannot effectively be reduced when the RF transmission medium is essentially open and susceptible to unintended or intentional interference or jamming. Effective DoS attacks can also be performed on the 802.11 protocol by exploiting unprotected management frames using inexpensive commercial hardware.

6.6.98. WPA2 provides no protection for management frames and therefore does not prevent spoofing or DoS attacks.

6.6.99. Availability is not currently addressed by the 802.11 standards in use at the time of writing. The 802.11w Task Group has been established to address this. There are vendor-specific solutions currently available.

REFERENCES

6.6.100. Information on wireless vulnerabilities can be found at http://www.wve.org. This website is run by the SANS Institute, Aruba Networks, WNP and the Center for Advanced Defense Studies.

EXAMPLES

6.6.101. An agency with a PROTECTED network could create an UNCLASSIFIED wireless network external to their gateway/CDS and allow system users to connect in through the gateway/CDS with an evaluated VPN solution.

6.6.102. An agency could expand their internal PROTECTED network to include wireless functionality if they deploy EAL2 traffic encryptors between their PROTECTED network and the WAPs to ensure that all traffic reaching the WAPs is already encrypted to a sufficient degree such that it could be handled as per the requirements for UNCLASSIFIED information when communicated over the wireless network.

Internet Protocol Telephony

PRINCIPLE

6.6.103. Ensuring IPT calls are protected from unauthorised access and the introduction of IPT equipment is undertaken in a controlled manner will prevent the introduction of additional attack vectors into the network.

OBJECTIVE

6.6.104. To ensure that IPT calls are protected from unauthorised access by protecting IPT signalling and data, using local area network traffic separation, using call authentication and authorisation, and appropriate setup procedures.

CONTEXT

Scope

6.6.105. This section covers information on IPT. Although IPT refers to the transport of telephone calls over Internet Protocol networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

6.6.106. Additional information relating to topics covered in this section can be found in the *Product Security* chapter, the *Telephone and Telephone Systems* section, the *Gateway/Cross Domain Solutions Security* chapter and any section relating to the protection of data networks in this manual.

Exception for IPT a gateway/CDS

6.6.107. Where a gateway/CDS connects between an analogue telephone network such as the PSTN and a computer network, the *Gateway/Cross Domain Solutions* section of this manual does not apply.

6.6.108. Where a gateway/CDS connects between an IPT network and an IPT network the *Gateway/Cross Domain Solutions* section of this manual still applies.

RISKS

6.6.109. An attacker eavesdrops on an IPT call, resulting in the disclosure of security classified discussions.

6.6.110. An attacker performs a DoS attack against an IPT system, resulting in a lack of availability of communications.

6.6.111. An attacker monitors the usage of an IPT network, resulting in the disclosure of information regarding the operational tempo of the agency.

6.6.112. An attacker masquerades as another person, resulting in the ability to socially engineer information from other personnel.

6.6.113. Authorised personnel make security classified phone calls which traverses a network of a lower security classification, resulting in an information security incident.

6.6.114. An attacker propagates between voice and data networks when there is insufficient separation, resulting in gaining an attacker vector into the data network.

6.6.115. An attacker exploits or abuses functionality of a softphone to gain access to the voice network, resulting in the disclosure of information.

6.6.116. An attacker exploits or abuses functionality of a softphone to gain access to the data network, resulting in the disclosure of information.

6.6.117. An agency having deployed a converged architecture losses data network services leading to a loss of voice network services.

CONTROLS

[U,IC-HP,R-TS] IPT gateway/CDS

6.6.118. Agencies using IPT that have a requirement to implement a firewall within a deployed gateway/CDS between computer networks **should** use an evaluated voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls.

[U,IC-HP,R-TS] Protecting IPT signalling and data

6.6.119. Agencies **should** protect IPT signalling and data to ensure confidentiality, integrity, availability, authenticity and non-replayability.

[U,IC-HP,R-TS] Establishment of secure IPT signalling and data

6.6.120. Agencies **should** ensure that IPT functions can only be established using the secure signalling and data protocols.

[U,IC-HP,R] Local area network traffic separation

6.6.121. Agencies **should** either physically or logically separate the IPT traffic from other data traffic.

[–,–,C-TS] Local area network traffic separation

6.6.122. Agencies **must** either physically or logically separate the IPT traffic from other data traffic.

[U,IC-P,R] Internet Protocol phone setup

6.6.123. Agencies **should**:

a. configure Internet Protocol phones to authenticate themselves to the call controller upon registration
b. disable phone auto-registration and only allow a whitelist of authorised devices to access the network
c. block unauthorised devices by default, and
d. disable all unused functionality such as speakerphones, USB ports, management interfaces etc.

[–,HP,C-TS] Internet Protocol phone setup

6.6.124. Agencies **must**:

a. configure Internet Protocol phones to authenticate themselves to the call controller upon registration
b. disable phone auto-registration and only allow a whitelist of authorised devices to access the network
c. block unauthorised devices by default, and
d. disable all unused functionality such as speakerphones, USB ports, management interfaces etc.

[U,IC-HP,R-TS] Call authentication and authorisation

6.6.125. Authentication and authorisation **should** be used for all actions on the IPT network, including:

a. call setup
b. changing settings, and
c. checking voice mail.

6.6.126. An encrypted and non-replayable two-way authentication scheme **should** be used for call authentication and authorisation.

6.6.127. Authentication **should** be enforced for:

a. registering a new phone
b. changing phone users
c. changing settings, and
d. accessing voice mail.

[U,IC-HP,R] Phone to workstation connections

6.6.128. Agencies **should not** connect workstations to Internet Protocol phones unless the workstation or the phone, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between IPT and other data traffic.

[–,–,C-TS] Phone to workstation connections

6.6.129. Agencies **must not** connect workstations to Internet Protocol phones unless the workstation or the phone, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between IPT and other data traffic.

[U,IC-HP,R-TS] Lobby and shared area phones

6.6.130. Where an agency uses an Internet Protocol phone in a lobby or shared area they **should** limit the phone's:

a. ability to access data networks, and
b. functionality for voice mail and directory services.

[U,IC-HP,R-TS] Softphone usage

6.6.131. Agencies **should not** use software phones.

GUIDANCE

[–,HP,C-TS] Internet Protocol phone setup

6.6.132. It is **recommended** that agencies use individual logins for Internet Protocol phones.

[U,IC-HP,R-TS] Lobby and shared areas

6.6.133. It is **recommended** that agencies use traditional analog phones in lobby and shared areas.

[U,IC-HP,R-TS] Softphone usage

6.6.134. It is **recommended** that agencies using softphones have separate dedicated network interface cards on the host for IPT network access.

6.6.135. It is **recommended** that agencies using softphones install a host-based firewall on workstations utilising softphones that only allows traffic to and from the minimum number of Real-time Transport Protocol (RTP) ports required.

[U,IC-HP,R-TS] Workstations using softphones

6.6.136. It is **recommended** that agencies use access control software to control USB ports on workstations using softphones by utilising the specific vendor and product identifier of the authorised phone.

[U,IC-HP,R-TS] Risk reduction

6.6.137. It is **recommended** that agencies plan a risk reduction strategy for DoS attacks, including:

a. how to diagnose the source of the denial of service
b. what actions can be taken to clear the denial of service condition, and
c. how voice capability could be maintained during an attack.

6.6.138. It is **recommended** that a risk reduction strategy for DoS attacks include monitoring and use of:

a. router and switch logging and flow data
b. packet captures
c. proxy and call manager logs and access control lists
d. IPT-aware firewalls and voice gateway/CDS
e. network redundancy
f. load balancing, and
g. PSTN failover.

RATIONALE

Internet Protocol telephony

6.6.139. Voice data in an IPT network consists of Internet Protocol packets and should not be treated any differently to other data. As such, in accordance with the principles of least-privilege and security-in-depth, hardening can be applied to handsets, software, servers and a gateway/CDS. For example a Session Initiation Protocol server could:

- have a fully patched software and operating system
- only required services running
- use encrypted non-replayable authentication, and
- apply network restrictions that only allow secure Session Initiation Protocol and secure RTP traffic from phones on a VLAN to reach the server.

IPT gateway/CDS

6.6.140. The use of a voice-aware firewall ensures that only voice traffic (e.g. signalling and data) is allowed for a given call and that session state is maintained throughout the transaction.

Protecting IPT signalling and data

6.6.141. IPT voice and signalling data is more vulnerable to eavesdropping and can be easily protected with encryption. This control helps protect against DoS, man-in-the-middle and call spoofing attacks made possible by inherent weaknesses in the IPT protocols.

6.6.142. When protecting IPT signalling and data, voice control signalling can be protected using Transport Layer Security (TLS) and the 'sips://' identifier to force the encryption of all legs of the connection. Similar protections are available for RTP and the Real-time Control Protocol.

Local area network traffic separation

6.6.143. Availability and quality of service are the main drivers for logical and physical separation.

Call authentication and authorisation

6.6.144. This control ensures server to the client and the client to the server authentication.

Softphone usage

6.6.145. Softphones can introduce additional attack vectors into the network as they are exposed to threats from the data network via the workstation and can subsequently be used to gain access to the voice network.

6.6.146. Softphones typically require workstation to workstation communication on (potentially) a number of randomly assigned ports to facilitate RTP data exchange. This presents a security risk as workstations generally should be separated using host-based firewalls that deny all connections between workstations to make malicious code propagation inside the network difficult.

Workstations using softphones

6.6.147. Adding softphones to a whitelist of allowed USB devices on a workstation will assist with restricting access to only authorised devices, and allowing the SOE to maintain defences against removable media storage and other unauthorised USB devices.

Risk reduction

6.6.148. Telephony is considered critical for any business and is therefore especially vulnerable to a DoS attack. The guidance provided will assist in protecting against IPT DoS attacks, signalling floods, established call teardown and RTP data floods.

EXAMPLES

6.6.149. A PROTECTED data network could have a PROTECTED IPT network run over it with appropriate logical separation. The IPT network can connect to the UNCLASSIFIED PSTN and personnel could converse with external clients at UNCLASSIFIED if there is appropriate education and a sufficient notification that an external call is being made. Alternatively, internal personnel could communicate at PROTECTED providing policy and controls were in place to ensure that all voice data was contained within the PROTECTED network.

6.6.150. An agency running a closed PROTECTED data network could have a number of remote sites connected via a wide area network. As each Internet connected wide area network link is PROTECTED by a VPN solution certified at Common Criteria EAL2, the agency could use an IPT network to connect to each of the remote sites.

Email Infrastructure

PRINCIPLE

6.6.151. Configuring email servers in a secure manner and enforcing protective markings will maintain the integrity of email infrastructure and prevent the spread of malicious code.

OBJECTIVE

6.6.152. To ensure the appropriately hardening and configuring of email servers and network infrastructure processing email.

CONTEXT

Scope

6.6.153. This section covers information on email infrastructure security. Information on using email applications can be found in the *Email Applications* section of the *Software Security* chapter in this manual.

RISKS

6.6.154. An attacker sends excessive amounts of email data to an agency email server, causing a denial of service against the server.

6.6.155. An attacker sends an email that contains a malicious payload to personnel. The email gateway/CDS does not check the attachment for malicious code. Personnel open the email, resulting in workstation infection.

6.6.156. An attacker intercepts an agency email without transport encryption, resulting in information being exposed.

6.6.157. An attacker spoofs an agency email address, causing the recipient to perform actions as if the agency had sent the email.

6.6.158. An attacker sends an email via an alternate email gateway/CDS with poorly maintained content filters, resulting in malicious code being delivered to personnel.

6.6.159. A system forwards an email that contains a protective marking which exceeds the security classification of the path over which the email would be communicated, resulting in a data spill.

6.6.160. A system accepts an email that contains a protective marking which exceeds the security classification of the system, resulting in a data spill on that system.

6.6.161. An agency does not quarantine outgoing email attachments it cannot scan, resulting in unauthorised information being released from the agency.

6.6.162. An agency does not quarantine incoming email attachments it cannot scan, resulting in malicious code being delivered to personnel.

CONTROLS

[U,IC-HP,R-TS] Blocking emails

6.6.163. Agencies **should** block:

a. inbound and outbound email, including any attachments, that contain:
   1) malicious code
   2) content in conflict with the agency's email policy

Continued on next page

3) content that cannot be identified, or
4) encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source

b. emails addressed to internal email aliases with source addresses located from outside the domain; and
c. all emails arriving via an external connection where the source address uses an internal agency domain name.

[–,IC-P,R] Preventing unmarked or inappropriately marked emails

6.6.164. Agencies **should** prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server.

[–,HP,C-TS] Preventing unmarked or inappropriately marked emails

6.6.165. Agencies **must** prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server.

[U,IC-HP,R-TS] Blocking of outbound emails

6.6.166. Agencies **must** configure systems to block any outbound emails with a valid protective marking indicating that the content of the email exceeds the security classification of the path over which the email would be communicated.

6.6.167. Agencies **should** configure systems to log every occurrence of a blocked email.

[U,IC-HP,R-TS] Blocking of inbound emails

6.6.168. Agencies **must** configure email systems to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the accreditation of the receiving system.

[U,IC-HP,R-TS] Automatic forwarding of emails

6.6.169. Agencies **must** ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

[U,IC-HP,R-TS] Email servers

6.6.170. Agencies **should** disable open email relaying so that email servers will only relay messages destined for the agency's domain(s) and those originating from within the domain.

[U,IC-HP,R-TS] Email server maintenance activities

6.6.171. Agencies **should** perform regular email server auditing, security reviews and vulnerability analysis activities.

[U,IC-HP,R-TS] Centralised email gateway/CDS

6.6.172. Agencies **should** route email through a centralised email gateway/CDS.

6.6.173. Where backup or alternative email gateway/CDS are in place, additional email gateway/CDS **should** be maintained at the same standard as the primary email gateway/CDS.

6.6.174. Where an agency has system users that send email from outside the agency's network, an authenticated and encrypted channel **must** be configured to allow email to be sent via the centralised email gateway/CDS.

[U,IC-HP,R-TS] Email server transport encryption

6.6.175. Agencies **must** enable opportunistic TLS encryption as defined in IETF's RFC 3207 on email servers that make incoming or outgoing email connections over public infrastructure.

[U,IC-HP,R-TS] Email server transport authentication

6.6.176. Agencies **should** implement TLS authentication between email servers where significant volumes of information is passed via email to other agencies.

[U,IC-HP,R-TS] Sender Policy Framework

6.6.177. Agencies **should** implement the email Sender Policy Framework (SPF) following the recommendations in IETF's RFC 4408.

[U,IC-HP,R-TS] DomainKeys Identified Mail signing

6.6.178. Agencies **should** enable DomainKeys Identified Mail (DKIM) signing on all email originating from their domain.

GUIDANCE

[U,–,–] Preventing unmarked or inappropriately marked emails

6.6.179. It is **recommended** that agencies prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server.

[U,IC-HP,R-TS] Preventing unmarked or inappropriately marked emails

6.6.180. It is **recommended** that agencies prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the workstation.

[U,IC-HP,R-TS] Blocking of inbound emails

6.6.181. It is **recommended** that agencies notify the intended recipient of any blocked emails.

[U,IC-HP,R-TS] Undeliverable messages

6.6.182. It is **recommended** that agencies send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means.

[U,IC-HP,R-TS] DomainKeys Identified Mail

6.6.183. It is **recommended** that agencies use DKIM in conjunction with SPF.

6.6.184. It is **recommended** that agencies verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.

6.6.185. It is **recommended** that where agencies operate email distribution list software that is used by external senders, they configure the software so that it does not break the validity of the sender's DKIM signature.

RATIONALE

Preventing unmarked or inappropriately marked emails

6.6.186. Unmarked or inappropriately marked emails can be blocked at two points, the workstation or the email server. The email server is the preferred location to block emails as it is a single location under the control of system administrators that can enforce the requirement for the entire network. In addition email servers can apply controls for emails generated by applications.

6.6.187. Whilst blocking at the email server is considered the most appropriate control there is still an advantage in blocking at the workstation as this approach adds an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

6.6.188. For security classified systems is it important to note that all security classified emails must have an appropriate security classification. This requirement is outlined in the *Email Applications* section of this manual and mirrors the requirements within Part C of the PSM for paper-based material. The reason blocking of unmarked or inappropriately marked emails on X-IN-CONFIDENCE, RESTRICTED and PROTECTED systems is a should requirement is to allow for the should requirement within the *Email Applications* section relating to the protective marking of non-security classified information on systems processing information of these security classifications. Additionally the recommended requirement for blocking unmarked or inappropriate marked emails on an UNCLASSIFIED system is a reflection of the optional nature of the protective marking for non-security classified information within Part C of the PSM.

Blocking of outbound emails

6.6.189. Blocking an outbound email with a valid protective marking that indicates the email exceeds the security classification of the path over which it would be communicated, stops data spills that could occur due to interception or storage of the email at any point along the path.

6.6.190. Agencies may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from the agency's gateway/CDS.

Blocking of inbound emails

6.6.191. Blocking an inbound email with a valid protective marking that indicates the email or its attachment exceeds the security classification the receiving system is accredited to process will prevent a data spill from occurring on the receiving system.

Centralised email gateway/CDS

6.6.192. Without a centralised email gateway/CDS it is exceptionally difficult to deploy SPF, DKIM and outbound email protective markings verification.

6.6.193. Attackers will almost invariably avoid using the primary email server when sending malicious emails. This is because the backup or alternative gateway/CDS are often poorly maintained in terms of out-of-date blacklists and content filtering.

Email server transport encryption

6.6.194. Email can be intercepted anywhere between the originating email server and the destination email server. Enabling TLS on the originating and accepting email server will defeat passive attacks on the network, with the exception of cryptanalysis against email traffic. TLS encryption between email servers will not interfere with email content filtering schemes. Email servers will remain compatible with other email servers as IETF's RFC 3207 specifies the encryption as opportunistic.

Sender Policy Framework

6.6.195. SPF aids in the detection of spoofed email server address domains. The SPF record specifies a list of Internet Protocol addresses or domains that are allowed to send mail from a specific domain. If the email server that sent the email is not in the list, the verification fails (there are a number of different fail types available).

6.6.196. Undeliverable or bounce emails are commonly sent by email servers to the original sender when the email cannot be delivered, usually because the destination address is invalid. Due to the common spamming practice of spoofing sender addresses, this often results in a large amount of bounce emails being sent to an innocent third party. Only sending bounces to senders that can be verified via SPF or other trusted means avoids contributing to this problem and allows other government agencies and trusted parties to receive legitimate bounce messages.

DomainKeys Identified Mail

6.6.197. DKIM enables a method of determining spoofed email content. The DKIM record specifies a public key that will sign the content of the message. If the signed digest in the email header doesn't match the signed content of the email the verification fails.

REFERENCES

6.6.198. Further information on email security is available from the following IETF documents:

- RFC 3207, *SMTP Service Extension for Secure SMTP over Transport Layer Security*
- RFC 4408, *Sender Policy Framework*
- RFC 4686, *Analysis of Threats Motivating DomainKeys Identified Mail*
- RFC 4871, *DomainKeys Identified Mail Signatures*, and
- RFC 5617, *DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP).*

6.6.199. Further information on email server security can be obtained from NIST publication SP 800-45 v2, *Guidelines on Electronic Mail Security*.

Intrusion Detection and Prevention

PRINCIPLE

6.6.200. Intrusion detection and prevention is achieved by the development of intrusion detection strategies including the deployment of IDSs and host-based antivirus measures.

OBJECTIVE

6.6.201. To ensure that an intrusion detection strategy and deployment of IDSs are undertaken within agencies to assist in detecting, terminating and preventing subsequent intrusions into networks.

CONTEXT

Scope

6.6.202. This section covers information relating to detection and prevention of malicious code propagating through networks as well as the detection and prevention of unusual or malicious activities.

Methods of infections or delivery

6.6.203. Malicious code can spread through a system from a number of sources including:

- files containing macro viruses or worms
- email attachments and Web downloads with malicious active content
- executable code in the form of applications
- security weaknesses in a system or network
- security weaknesses in an application, and
- contact with an infected system or media.

RISKS

6.6.204. An agency deploys IDSs inappropriately or in an inappropriate location, resulting in a false sense of security in their network.

6.6.205. An agency does not sufficiently monitor or maintain deployed IDSs, subsequently failing to notice intrusion attempts.

6.6.206. An attacker implants a virus into a system with no protection mechanism present, subsequently subverting the system.

6.6.207. A system user disables a host-based protection mechanism, allowing an attacker to subvert the system.

6.6.208. An attacker infects a system by modifying a virus to bypass signature-based detection mechanisms.

6.6.209. An attacker gains the ability to subvert a system by creating a virus to exploit a recently released vulnerability that has not been patched by the owner of the system.

6.6.210. An agency fails to adequately train personnel on how to monitor and configure IDSs resulting in intrusions going unnoticed.

CONTROLS

[U,IC-HP,R] Intrusion detection strategy

6.6.211. Agencies **should** develop, implement and maintain an intrusion detection strategy, based on the results of a security risk assessment, that includes:

a. appropriate intrusion detection mechanisms, including network-based IDSs and host-based IDSs as necessary
b. the audit analysis of event logs, including IDS logs
c. a periodic audit of intrusion detection procedures
d. information security awareness and training programs, and
e. a documented IRP.

[–,–,C-TS] Intrusion detection strategy

6.6.212. Agencies **must** develop, implement and maintain an intrusion detection strategy, based on the results of a security risk assessment, that includes:

a. appropriate intrusion detection mechanisms, including network-based IDSs and host-based IDSs as necessary
b. the audit analysis of event logs, including IDS logs
c. a periodic audit of intrusion detection procedures
d. information security awareness and training programs
e. a documented IRP, and
f. provide the capability to detect information security incidents and attempted network intrusions on gateway/CDS and provide real-time alerts.

[U,IC-HP,R-TS] IDSs on Internet gateway/CDS

6.6.213. Agencies **should** deploy IDSs in all gateway/CDS between the agency's networks and unsecured public networks.

[U,IC-HP,R-TS] Signature-based intrusion detection

6.6.214. When signature-based intrusion detection is used, agencies **should** keep the signatures up to date.

[U,IC-HP,R-TS] Malicious code counter-measures

6.6.215. Agencies **must**:

a. develop and maintain a set of policies, plans and procedures, derived from a security risk assessment, covering how to:
   1) minimise the likelihood of malicious code being introduced into a system
   2) prevent all unauthorised code from executing on an agency network, and
   3) detect any malicious code installed on a system
b. make their system users aware of the agency's policies, plans and procedures; and
c. ensure that all instances of detected malicious code outbreaks are handled according to the procedures.

GUIDANCE

[U,IC-HP,R-TS] IDSs on Internet gateway/CDS

6.6.216. It is **recommended** that agencies locate IDSs within the gateway/CDS environment, immediately inside the outermost firewall.

[U,IC-HP,R-TS] IDSs on other gateway/CDS

6.6.217. It is **recommended** that agencies deploy IDSs at all gateway/CDS between the agency's networks and any network not managed by the agency.

[U,IC-HP,R-TS] Configuring the IDS

6.6.218. It is **recommended** that in addition to agency defined configuration requirements, agencies ensure that IDSs located inside a firewall be configured to generate a log entry, and an alert, for any information flows that contravene any rule within the firewall rule set.

6.6.219. It is **recommended** that agencies test IDSs rule sets prior to implementation to ensure that they perform as expected.

[U,IC-HP,R-TS] Event management and correlation

6.6.220. It is **recommended** that agencies deploy tools for:

a. the management and archival of security event information, and
b. the correlation of events of interest across all agency networks.

[U,IC-HP,R-TS] Antivirus software

6.6.221. It is **recommended** that agencies ensure that for all servers and workstations:

a. they install agency approved antivirus software
b. that system users do not have the ability to disable the software
c. they check vendor virus pattern signatures for updates daily
d. they apply virus pattern signature updates as soon as possible after vendors make them available, and
e. they regularly scan all disks.

[U,IC-HP,R-TS] Host-based IDSs

6.6.222. It is **recommended** that agencies install host-based IDSs on high security risk servers.

[U,IC-HP,R-TS] Active content blocking

6.6.223. It is **recommended** that agencies use:

a. filters to block:
   1) unwanted content, and
   2) exploits against applications that cannot be patched
b. settings within the applications to disable unwanted functionality; and
c. digital signatures to restrict active content to trusted sources only.

RATIONALE

IDSs on Internet gateway/CDS

6.6.224. If the firewall is configured to block all traffic on a particular range of port numbers, then the IDS should inspect traffic for these port numbers and alert if they are detected.

Malicious code counter-measures

6.6.225. Implementing policies and procedures for preventing and dealing with malicious code outbreaks that enables agencies to provide consistent incident response, as well as giving clear directions to system users about what to do in the case of an information security incident.

Antivirus software

6.6.226. Antivirus software, while important, can be defeated by malicious code that has yet to be identified by antivirus vendors. This can include targeted attacks, where a new virus is engineered or an existing one modified to defeat the signature-based detection schemes used by most antivirus software.

6.6.227. The use of antivirus software, while adding value to the defence of workstations, cannot be relied solely upon to protect the workstation. As such agencies can deploy appropriately hardened SOEs to assist with the protection of workstations against a broader range of security risks.

Host-based IDSs

6.6.228. Host-based IDSs use behaviour-based detection schemes and can therefore detect malicious code that has yet to be identified by antivirus vendors.

Active content blocking

6.6.229. Filtering unnecessary content and disabling unwanted functionality reduces the number of possible entry points that an attacker can exploit.

REFERENCES

6.6.230. Additional information relating to intrusion detection and audit analysis is contained in:

- AS/NZS ISO/IEC 27001:2006, A.15.3, *Information Systems Audit Considerations*, and
- HB 171:2003, *Guidelines for the Management of Information Technology Evidence*.

Internet Protocol Version 6

PRINCIPLE

6.6.231. Disabling Internet Protocol version 6 (IPv6) functionality until appropriate security mechanisms can be implemented and accredited will assist in mitigating specific IPv6 attacks against a network.

OBJECTIVE

6.6.232. To ensure that agencies do not begin to implement IPv6 capable devices in their networks without considering security risks and associated threats specified to IPv6 technology.

CONTEXT

Scope

6.6.233. This section covers information on IPv6 and its deployment within networks. Where this manual specifies requirements for network devices, the requirements apply equally whether deploying Internet Protocol version 4 or 6.

6.6.234. Agencies unable to meet the compliance requirements as specified for a control when deploying IPv6 network infrastructure will need to follow the procedures as specified in this manual for varying from a control and the associated compliance requirements.

IPSec within IPv6

6.6.235. The use of IPSec within IPv6 does not meet the requirements for use as a DACP as specified in this manual.

RISKS

6.6.236. An agency purchases network devices unaware that IPv6 functionality is enabled by default, providing attackers an unobstructed attack vector into the agency network.

6.6.237. An unplanned and uncontrolled implementation of IPv6 equipment into government networks results in failures and loss of service delivery capability.

6.6.238. An agency decides to implement IPv6 within their network infrastructure without due consideration of new security risks that will be introduced as a result.

CONTROLS

[U,IC-HP,R-TS] Use of dual-stack equipment

6.6.239. Agencies not using IPv6 but which have deployed dual-stack network devices or operating systems that support IPv6 **must** disable the functionality.

[U,IC-HP,R-TS] Using IPv6

6.6.240. Agencies using IPv6 **must** conduct a security risk assessment on any security risks that could be introduced as a result of running a dual stack environment or transitioning completely to IPv6.

[U,IC-HP,R-TS] Introducing IPv6 capable equipment to a gateway/CDS

6.6.241. Agencies deploying IPv6 equipment in their gateway/CDS **should** undergo reaccreditation.

[U,IC-HP,R-TS] Enabling IPv6 in a gateway/CDS

6.6.242. Agencies enabling IPv6 in their gateway/CDS **must** undergo reaccreditation.

RATIONALE

Using IPv6

6.6.243. The information security implications around the use of IPv6 are still largely unknown and untested. As many of the current network protection technologies such as firewalls and IDSs do not currently support IPv6, agencies choosing to implement IPv6 face a significant security risk of being compromised.

Enabling IPv6 in a gateway/CDS

6.6.244. Introducing IPv6 capable network devices into an agency gateway/CDS introduces a significant number of new security risks. Undergoing reaccreditation when new IPv6 equipment is introduced will ensure that any IPv6 functionality that is not intended to be used cannot be exploited by an attacker before appropriate information security mechanisms have been put in place. Likewise, once agencies have completed the transition to a dual-stack environment or completely to an IPv6 environment, reaccreditation will assist in ensuring that the associated information security mechanisms for IPv6 are working effectively.

REFERENCES

6.6.245. *A Strategy for the Transition to IPv6 for Australian Government agencies* can be found on the AGIMO website at http://www.finance.gov.au/e-government/infrastructure/internet-protocol-version-6.html.

6.6.246. Additional IPv6 information can be found at:

- http://www.nsa.gov/ia/guidance/security_configuration_guides/IPv6.shtml, and
- https://www.cpni.gov.uk/Products/technicalnotes/3008.aspx.

Multifunction Devices

PRINCIPLE

6.6.247. Networked MFDs can be prevented from spilling information onto an attached network by controlling their usage based on the accredited security classification of the attached network.

OBJECTIVE

6.6.248. To ensure that data spills do not occur on networks attached to MFDs.

CONTEXT

Scope

6.6.249. This section covers information on MFDs that communicate information over computer networks. Such MFDs may include several or all of the following functions:

- printing
- scanning
- photocopying
- faxing
- e-mailing
- reading from memory cards, and
- communicating via Ethernet, wireless, infrared and Bluetooth.

6.6.250. Additional information and requirements relating to MFDs can be found in the following chapters and sections of this manual:

- *Radio Frequency and Infrared Devices*
- *Fax Machines and Multifunction Devices*
- *Product Security*
- *Media Security*
- *Remote Access*, and
- *Wireless Local Area Networks.*

RISKS

6.6.251. A system user assumes that, because the capability exists, it is acceptable to fax a security classified document from their workstation.

6.6.252. Personnel scan information on a MFD and send it across an attached network that is accredited at a lower security classification than that of the scanned document resulting in a data spill.

6.6.253. An attacker gains access to networked resources through a compromised MFD and compromises information.

6.6.254. An attacker gains access to networked resources through a wireless connection on a MFD and compromises information.

CONTROLS

[U,IC-HP,R-TS] Policies, plans and procedures

6.6.255. Agencies deploying MFDs **must** develop a set of policies, plans and procedures governing the use of the equipment.

[U,IC-HP,R-TS] Copying documents on networked MFDs

6.6.256. Agencies **must not** permit network connected MFDs to be used to copy security classified documents above the security classification of the connected network.

[U,IC-HP,R-TS] Communicating information using networked MFDs

6.6.257. Where network connected MFDs have the ability to communicate information via a gateway/CDS to another network, agencies **must** ensure that:

a. each MFD applies user identification, authentication and audit functions for all information communicated by system users from that device
b. these mechanisms are of similar strength to those specified for workstations on that network, and
c. the gateway/CDS can identify and filter the information in accordance with the requirements for the export of data.

GUIDANCE

[U,IC-HP,R-TS] Observing MFD use

6.6.258. It is **recommended** that agencies ensure that MFDs are located in an area where their use can be observed.

RATIONALE

Copying documents on networked MFDs

6.6.259. As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel need to be aware that if they scan or copy documents at a security classification higher than that of the network the device is connected to they could be causing a data spill onto the connected network.

Communicating information using networked MFDs

6.6.260. As network connected MFDs are considered to be device that resides on a computer network they need to be able to process the same security classification of information that the network is capable of processing.

Gateway/Cross Domain Solutions Security

Gateway/Cross Domain Solutions

PRINCIPLE

6.7.1. A gateway/CDS can be used in a secure manner by understanding security risks involved in using the technology and applying appropriate risk reduction strategies to protect all connected domains.

OBJECTIVE

6.7.2. To ensure that appropriate security mechanisms are implemented to use the operational benefits of gateway/CDS technology.

CONTEXT

Scope

6.7.3. Gateways can be considered information flow control mechanisms at the network layer while CDS control information flow at the application layer. The same security information applies to both gateways and CDS so this section covers general information for all gateways and CDS. Specific controls for different technologies can be found in later sections on firewalls, diodes and peripheral switches.

6.7.4. Additional information relating to topics covered in this section can be found in the following sections of this manual:

- *Information System Accreditation*
- *Servers and Network Devices*
- *Network Infrastructure*
- *Hardware Products*
- *Identification and Authentication*
- *Event Logging and Auditing*
- *Data Import and Export*
- *Content Filtering*
- *Firewalls*
- *Diodes*, and
- *Peripheral Switches.*

Deploying a gateway/CDS

6.7.5. This section provides a baseline for agencies deploying a gateway/CDS. Agencies will need to consult additional sections of this manual depending on the specific type of gateway/CDS deployed.

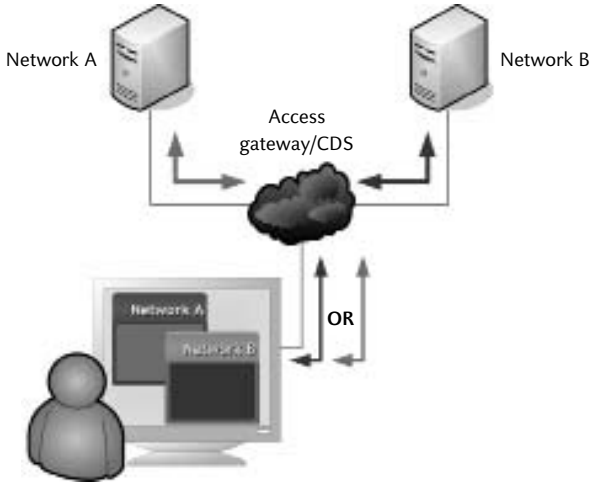
6.7.6. For network devices used to control data flow in a bi-directional gateway/CDS the *Firewalls* section of this manual will need to be consulted while the *Diodes* section will also need to be consulted for a one-way gateway/CDS. Additionally, for both types of gateway/CDS the *Data Import and Export* section will need to be consulted for requirements on appropriately controlling data flows.

6.7.7. The requirements in this manual for content filtering, data import and data export apply to all types of gateway/CDS.

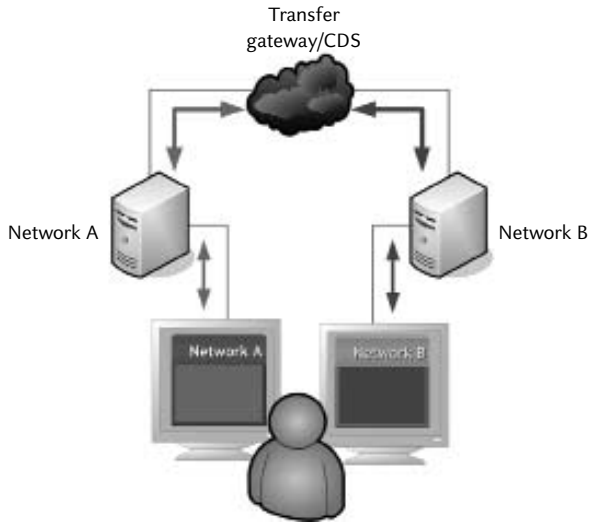
Types of gateways/cross domain solutions

6.7.8. This manual defines three types of gateway/CDS: access gateway/CDS, multilevel gateway/CDS and transfer gateway/CDS.

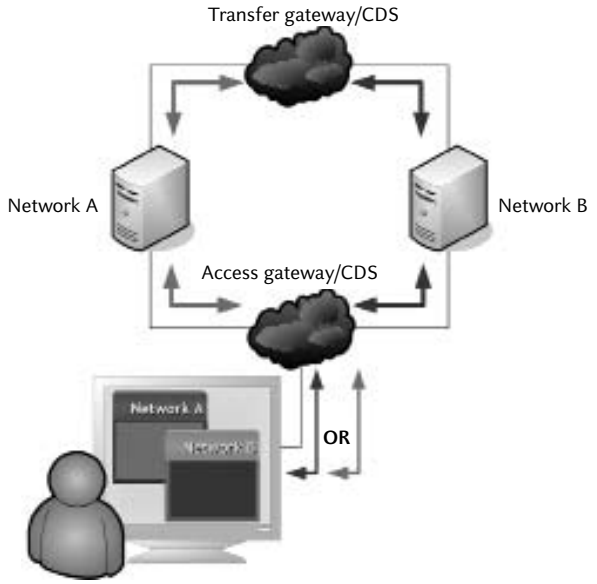
6.7.9. An access gateway/CDS provides the system user with access to multiple security domains from a single device.



6.7.10. A transfer gateway/CDS facilitates the transfer of information, in one or multiple directions (low to high or high to low) between different security domains. A traditional gateway to the Internet is considered a transfer gateway/CDS.



6.7.11. A multilevel gateway/CDS enables access, based on authorisations, to data at multiple security classification and releasability levels.



Logging and auditing controls and guidance

6.7.12. The requirements in this manual for event logging, user logs, system management logs and auditing apply to the gateway/CDS and the connected domains.

Accreditation of a gateway/CDS

6.7.13. The requirements in this manual for accreditation apply to the gateway/CDS and the connected domains.

Applying the controls

6.7.14. For the purposes of this section, the gateway/CDS assumes the highest security classification of the connected domains.

Exceptions for allowable gateway/CDSs

6.7.15. Agencies can use cascaded connections to establish indirect connections between TOP SECRET and less than SECRET networks as well as from SECRET to UNCLASSIFIED networks.

RISKS

6.7.16. A system user accidentally enters higher security classified information on a lower security domain.

6.7.17. An agency misconfigures the gateway/CDS accounts and compromises system user access to the domains, which results in a denial of service or data spill.

6.7.18. An agency installs the gateway/CDS hardware incorrectly and compromises system user access to the domains, which results in a denial of service or data spill.

6.7.19. An agency misconfigures the gateway/CDS application or operating system software and compromises system user access to the domains resulting in a denial of service or data spill.

6.7.20. The gateway/CDS has inadequate backup and restore mechanisms and a routine fault causes a DoS attack.

6.7.21. The owner of the lesser security domain managing shared components in gateway/CDS is unaware of the proper configuration to control data flow from the higher security domain and causes a data spill.

6.7.22. An agency fails to appropriately filter communications across a gateway/CDS causing a data spill.

6.7.23. An attacker executes malicious code on the gateway/CDS that subsequently releases unauthorised data from a higher security domain or grants the attacker greater access to the gateway/CDS functions.

6.7.24. A domain connected through the gateway/CDS is also connected through another gateway/CDS to a further domain (in a cascaded connection) that:

a. exposes vulnerabilities in the first gateway/CDS network
b. increases the opportunity for malicious attack, and
c. increases the likelihood of unauthorised release of data from a higher security domain.

6.7.25. An attacker sends manipulated packets to the gateway/CDS to release unauthorised data from a higher security domain or causes a DoS attack.

6.7.26. An attacker exploits the complexity and native vulnerabilities of the allowed data types to launch a malicious attack on the gateway/CDS, using legitimate data, which may include unauthorised release of data from a higher security domain.

6.7.27. An attacker masquerades unauthorised data as legitimate data to release the unauthorised data from a higher security domain.

6.7.28. An attacker releases unauthorised data from a higher security domain through the aggregation of legitimate data.

6.7.29. An attacker gains unauthorised control of the gateway/CDS and invokes a data spill from a higher security domain.

6.7.30. An attacker modifies gateway/CDS hardware or software (e.g. connecting the physical domain interfaces at the gateway/CDS), allowing uncontrolled data transfer between domains.

6.7.31. An attacker gains access to the gateway/CDS over a domain network and reconfigures the filter or network architecture to launch an attack.

6.7.32. An attacker gains access to the gateway/CDS administration network and reconfigures the filter or network architecture to introduce vulnerabilities.

6.7.33. An attacker exploits normal access to the gateway/CDS administration processes to reconfigure the filter or network architecture to make it less secure.

6.7.34. An attacker or system user labels data with an inappropriate security marking, causing unauthorised data release from a higher security domain.

6.7.35. An attacker compromises an automatic labelling mechanism that causes data to be labelled with inappropriate security markings and invokes a data spill from a higher security domain.

6.7.36. An attacker exploits poor quarantine measures in the gateway/CDS to transfer malicious code between domains.

6.7.37. A developer introduces a vulnerability to the gateway/CDS hardware or software that gives an attacker greater access to the gateway/CDS or invokes a data spill from a higher security domain.

6.7.38. An attacker exploits the reuse of software objects in the gateway/CDS application or operating system software to release unauthorised data from a higher security domain or transfer malicious code between security domains.

6.7.39. An attacker installs network monitoring software on the gateway/CDS and captures unauthorised data as it is processed.

6.7.40. An attacker uses network monitoring software on a domain network to capture unauthorised data at the gateway/CDS interfaces.

6.7.41. An attacker, with knowledge of the gateway/CDS operation, targets a single point of failure in the gateway/CDS.

6.7.42. An attacker flooding the data channels to the gateway/CDS causes a DoS attack.

6.7.43. An attacker masquerades as an authorised higher security domain system user within a multilevel gateway/CDS to obtain unauthorised data.

6.7.44. Personnel maliciously or inadvertently interfere with a gateway/CDS component, stopping all data from flowing across the gateway/CDS.

6.7.45. An attacker bypasses gateway/CDS controls by using an alternative communications route to access an agency network.

6.7.46. An attacker attempts network intrusion over a period of time, which goes undetected, leading to eventual penetration and exploitation of the agency network.

CONTROLS

[U,IC-HP,R-TS] Applying the controls

6.7.47. Agencies **must** apply controls for the highest security classified domain connected to the gateway/CDS.

[–,–,S-TS] Allowable gateway/CDS

6.7.48. Agencies **must not** implement a gateway/CDS permitting data to flow directly from:

a. a TOP SECRET network to any network below SECRET, and
b. a SECRET network to an UNCLASSIFIED network.

[U,IC-HP,R-TS] Gateway/CDS involving cascaded connections

6.7.49. When agencies have cascaded connections between networks involving multiple gateway/CDS they **must** ensure that the assurance levels specified for network devices between the lowest and highest networks are met by the gateway/CDS between the highest security classified system and the next highest classified system within the cascaded connection.

[U,IC-HP,R-TS] Using a gateway/CDS

6.7.50. Agencies **must** ensure that:

a. all agency networks are protected from networks in other security domains by one or more gateway/CDS
b. all gateway/CDS contain mechanisms to limit data flow at the network and content level to only the information necessary for business purposes, and
c. all gateway/CDS components are physically located within an appropriately secured server room to protect the most sensitive information processed by the gateway/CDS.

6.7.51. For a gateway/CDS between networks in different security domains, any shared components **must** be managed by the system owners of the highest security domain.

[U,IC,R] Gateway/CDS configuration

6.7.52. Agencies **should** ensure that gateway/CDSs:

a. are the only communications paths into and out of internal networks
b. by default, deny all connections into and out of the network
c. allow only explicitly authorised connections
d. are managed via a secure path isolated from all connected networks (i.e. physically at the gateway/CDS or on a dedicated administration network)
e. provide sufficient audit capability to detect gateway/CDS information security breaches and attempted intrusions, and
f. provide real-time alerts.

[–,P-HP,C-TS] Gateway/CDS configuration

6.7.53. Agencies **must** ensure that gateway/CDSs:

a. are the only communications paths into and out of internal networks
b. by default, deny all connections into and out of the network
c. allow only explicitly authorised connections
d. are managed via a secure path isolated from all connected networks (i.e. physically at the gateway/CDS or on a dedicated administration network)
e. provide sufficient audit capability to detect gateway/CDS information security breaches and attempted intrusions, and
f. provide real-time alerts.

[–,–,C-TS] Gateway/CDS operation

6.7.54. Agencies **must** ensure that all gateway/CDSs connecting networks in different security domains:

a. include a firewall of an appropriate assurance level on all gateway/CDSs, including one-way gateway/CDSs, to filter and log network traffic attempting to enter the gateway/CDS
b. are configured to save event logs to a separate secure log server
c. are protected by authentication, logging and audit of all physical access to gateway/CDS components, and
d. have all security controls tested to verify their effectiveness after any changes to their configuration.

[–,–,S-TS] Separation of data flows

6.7.55. Agencies **must** ensure that all bi-directional gateway/CDSs between TOP SECRET and SECRET networks, and between SECRET and less security classified networks, have separate upward and downward paths using physically separate infrastructure for each path within the gateway/CDS.

[U,IC-HP,R-TS] Demilitarised zones

6.7.56. Agencies **should** use demilitarised zones to house systems directly accessed externally and mediate external access to information held on internal systems.

[–,HP,C] Product selection

6.7.57. Agencies **should** consult with DSD on the security and applicability of a proposed gateway/CDS.

[–,–,S-TS] Product selection

6.7.58. Agencies **must** consult with DSD on the security and applicability of a proposed gateway/CDS.

[U,IC-HP,R-TS] Security risk assessment

6.7.59. Agencies **must** perform a security risk assessment on the specific gateway/CDS installation network and configuration prior to implementing a gateway/CDS.

6.7.60. Agencies **must** include the specific threats to AUSTEO, AGAO and other caveated (e.g. communities of interest) information when performing a security risk assessment for a network including a gateway/CDS.

[U,IC-P,R] Security risk management

6.7.61. Agencies **should** seek to manage security risks resulting from the security risk assessment.

[–,HP,C-TS] Security risk management

6.7.62. Agencies **must** seek to manage security risks resulting from the security risk assessment.

[U,IC-HP,R-TS] Security risk transfer

6.7.63. All domain owners connected through the gateway/CDS **must** understand and accept the security architecture and risks of the other domains.

6.7.64. All domain owners connected through the gateway/CDS **should**

a. obtain accreditation details from the other domain owners
b. review the details to determine the security characteristics of the domain, and
c. identify any additional security controls necessary to effectively manage the connection in accordance with their ISP.

6.7.65. All domain owners connected through the gateway/CDS **must** understand and accept all security risks associated with cascaded connections involved in moving data from its original source to the final destination (e.g. data originates from domain A and is destined for domain C. To achieve this, domain A connects through a gateway/CDS to domain B, which is connected to domain C through another gate/CDS).

6.7.66. All domain owners connected through the gateway/CDS **must** accept any residual security risks of the gateway/CDS or gateway/CDS network.

[U,IC-HP,R-C] Information stakeholders

6.7.67. Once connectivity is established, domain owners **should** become information stakeholders for all connected domains.

[–,–,S-TS] Information stakeholders

6.7.68. Once connectivity is established, domain owners **must** become information stakeholders for all connected domains.

[U,IC-HP,R-C] System user training

6.7.69. All system users **should** be trained on the secure use and security risks of the gateway/CDS before being granted access.

[–,–,S-TS] System user training

6.7.70. All system users **must** be trained on the secure use and security risks of the gateway/CDS before being granted access.

[U,IC-HP,R-TS] Gateway/CDS administration

6.7.71. Agencies **must** limit access to gateway/CDS administration functions.

6.7.72. Agencies **must** ensure that system administrators are fully trained to manage the gateway/CDS by qualified trainers.

6.7.73. Agencies **must** ensure that all system administrators of a gateway/CDS that processes AUSTEO or AGAO information meet the nationality requirements for these caveats.

[U,IC-HP,R-C] Gateway/CDS administration

6.7.74. Agencies **should** separate roles for gateway/CDS configuration (e.g. separate network and security policy configuration roles).

[–,–,S-TS] Gateway/CDS administration

6.7.75. Agencies **must** separate roles for gateway/CDS administration (e.g. separate network and security policy configuration roles).

[U,IC-HP,R-TS] System user authentication

6.7.76. Agencies **must** authenticate system users to all security classified domain networks accessed through a gateway/CDS.

6.7.77. Agencies **must** ensure that only users authenticated and authorised to the gateway/CDS can use the gateway/CDS.

[U,IC-HP,R-TS] Hardware authentication

6.7.78. Agencies **should** authenticate hardware (e.g. by media access control address) to domain networks accessed through a gateway/CDS.

[U,IC-HP,R-TS] Configuration control

6.7.79. Agencies **must** have the gateway/CDS reaccredited after any security relevant changes are made.

[U,IC-HP,R-C] Configuration control

6.7.80. Agencies **should** limit changes to the gateway/CDS after installation.

[–,–,S-TS] Configuration control

6.7.81. Agencies **must** limit changes to the gateway/CDS after installation.

GUIDANCE

[–,–,C-TS] Gateway/CDS testing

6.7.82. It is **recommended** that agencies ensure that security control testing is performed at random intervals no more than six months apart.

[–,–,C] Separation of data flows

6.7.83. It is **recommended** that agencies ensure that all bi-directional gateway/CDSs between CONFIDENTIAL and less security classified networks have separate upward and downward paths using physically separate infrastructure for each path.

[U,IC-HP,R-TS] System user authentication

6.7.84. It is **recommended** that agencies use multi-factor authentication for access to domain networks and the gateway/CDS.

[U,IC-P,R] Product selection

6.7.85. It is **recommended** that agencies consult with DSD on the security and applicability of a proposed gateway/CDS.

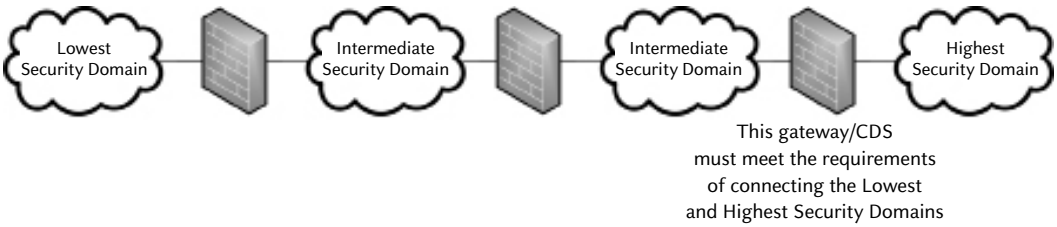
[U,IC-HP,R-TS] Security risk transfer

6.7.86. It is **recommended** that agencies annually review the security architecture and risks of all connected domains in accordance with controls for security risk transfer in this manual.

RATIONALE

Gateway/CDSs involving cascaded connections

6.7.87. Protecting a cascaded connection path with the minimum assurance requirement of a direct connection between the most and least security classified networks ensures appropriate reduction in security risks of the extended connection. An example of this can be seen below.



Using gateway/CDSs

6.7.88. Physically locating all gateway/CDS components inside a server room will reduce the security risk of unauthorised access to the device.

6.7.89. The system owner of the higher security domain of connected security domains would be most familiar with the security controls required to protect the more sensitive information and as such is best placed to manage any shared gateway/CDS components.

Gateway/CDS configuration

6.7.90. Given the criticality of gateway/CDS in controlling the flow of information between security domains, any failure, particularly at the higher security classifications may have serious consequences. Hence mechanisms for alerting personnel to situations that may potentially give rise to information security incidents are especially important for gateway/CDS.

Gateway/CDS operation

6.7.91. Providing a sufficient audit capability will help to detect gateway/CDS information security breaches and attempted network intrusions, allowing the agency to take appropriate measures to reduce the security risk of future attempts.

6.7.92. Storing event logs on a separate secure log server will prevent attackers from deleting logs in an attempt to destroy evidence of their attack.

DSD consultation on gateway/CDS technology

6.7.93. DSD has particular insight into gateway/CDS technologies and the large number of associated security risks of each. Through consulting with DSD on the security and application of a gateway/CDS, DSD will assist agencies to develop a comprehensive picture of the security risk for the gateway/CDS technology. Agencies will thus be better placed to identify and implement risk reduction measures that are appropriate to their environment.

Gateway/CDS network architecture

6.7.94. A gateway/CDS, being part of a network architecture, is exposed to security risks from connected domain networks. These security risks are managed through implementation of the requirements identified in this manual

Transferring security risk across agency boundaries

6.7.95. A gateway/CDS could connect networks with different domain owners including across agency boundaries. As a result, all domain owners must understand and accept the security risks of all other networks before a gateway/CDS is implemented. The domain owners also become stakeholders of the information in all the connected domains to maintain visibility of any changes in the level of security risk of the networks.

Installed configuration of the gateway/CDS

6.7.96. Not all security risks in the gateway/CDS network can be reduced by the gateway/CDS technology and therefore require reduction by the agency during implementation. Additionally, vulnerabilities can be introduced if gateway/CDS are not installed and configured securely. Independent assessment of the installed configuration will assess both these measures.

Isolating the administration network

6.7.97. An in-band ability to manage the gateway/CDS provides a potential attacker with a much more easily accessible avenue through which to launch an attack than a separate, controlled and isolated out-of-band administrative channel.

Role separation

6.7.98. Application of role separation in administration activities protect against security risks posed by a malicious system user with extensive access to the gateway/CDS.

User and workstation authentication

6.7.99. Authentication to domain networks and gateway/CDS reduce the security risk of unauthorised access and provide audit capability to support the investigation of information security incidents.

Hiding versus. masquerading information

6.7.100. Hiding and masquerading unauthorised information or malicious code within legitimate data differ, as hiding involves embedding the unauthorised content in the legitimate data while masquerading does not involve any legitimate data but rather makes the unauthorised content appear to be legitimate.

Data Import and Export

PRINCIPLE

6.7.101. The import of data to a network needs scanning for malicious content whilst the export of data from a network needs scanning for content not approved for release. In addition both import and export of data needs an appropriate authority to undertake the transfer and be accountable for the data being imported and exported.

OBJECTIVE

6.7.102. To ensure that the import of data is handled correctly and in a secure manner, including scanning and appropriate approvals, whilst the export of data is handled correctly and in a secure manner, including appropriate scanning and approvals for release.

CONTEXT

Scope

6.7.103. This section covers the movement of data onto a system or network including:

- the retrieval of data onto the network; and
- movement of data off of a system or network, including pushing of data onto another network.

Exceptions for data import

6.7.104. Malicious content can be imported to isolated systems specifically designed for the storage, analysis or transmission of such content.

6.7.105. Where the type of data cannot be effectively scanned, and the source or content of the data is strictly limited to known safe states, the accreditation authority can choose to approve the importation of unscanned data.

RISKS

6.7.106. An agency incorrectly implements a gateway/CDS, increasing the chance a system could suffer from malicious infection or attack.

6.7.107. Personnel download an infected executable, allowing adversaries to gain access to systems.

6.7.108. Personnel inadvertently import data that the receiving network is not accredited to process or store causing a data spill.

6.7.109. An attacker uploads malicious code to the agency system, giving them access to information and the opportunity to conduct a DoS attack.

6.7.110. An agency does not use protective marking checks when transferring data, resulting in export of higher security classified data than that which the receiving network is approved to process causing a data spill.

6.7.111. An agency operating a higher security classified enclave on their network does not enforce information checks on data that is exported from the enclave, resulting in data spills from the enclave onto the network.

6.7.112. Personnel inadvertently export data to a receiving network that is not accredited to process or store causing the data a data spill.

6.7.113. A person or system maliciously or inadvertently modifies data in transit that has not been digitally signed, causing a loss of data integrity.

6.7.114. An agency fails to audit their event logs, resulting in them being unaware of unsafe exporting practices by personnel.

6.7.115. Personnel or an application exports data with the caveat of AUSTEO or AGAO onto a foreign system, resulting in a data spill.

CONTROLS

[U,IC-HP,R-TS] System user responsibilities

6.7.116. Agencies **must** ensure that system users:

a. are held accountable for the data they import and export, and
b. are instructed to perform a protective marking check and a visual inspection.

[U,IC-P,R] Data transfer authorisation

6.7.117. Agencies **should** ensure that data imports and exports are either:

a. performed in accordance with processes and procedures approved by the accreditation authority, or
b. individually approved by an ITSM.

[–,HP,C-TS] Data transfer authorisation

6.7.118. Agencies **must** ensure that data imports and exports are performed in accordance with processes and procedures approved by the accreditation authority.

[–,–,C-TS] Data transfer authorisation

6.7.119. Agencies **must** ensure that all data exported to a system of a lesser security classification is approved by a trusted source.

[–,–,C-TS] Trusted sources

6.7.120. Trusted sources **must** be:

a. a strictly limited list derived from business requirements and the results of a security risk assessment, and
b. approved by the accreditation authority.

6.7.121. A trusted source **must not** be permitted to approve multiple transfers of a single data item across different security classifications.

[U,–,–] Data import

6.7.122. Agencies importing data to an UNCLASSIFIED system **should** ensure that the data is scanned for malicious and active content.

[–,IC-HP,R] Data import

6.7.123. Agencies importing data to a security classified system **must** ensure that the data is scanned for malicious and active content.

[–,–,C-TS] Data import

6.7.124. Agencies importing data to a security classified system **must** implement the following controls:

a. scanning for malicious and active content
b. data format checks
c. log of each event, and
d. monitoring to detect overuse/unusual usage patterns.

[–,–,C-TS] Data import through a gateway/CDS

6.7.125. When agencies import data to a system through a gateway/CDS, the data **must** additionally be filtered by a product with at least an EAL2 level of assurance that has been specifically evaluated for that purpose.

6.7.126. When agencies import data to a system through a gateway/CDS, full or partial audits of the event logs **must** be performed at least monthly.

[U,IC-P,R] Export of data

6.7.127. Agencies **should** restrict the export of data to a system of a lesser security classification by filtering data using at least protective marking checks.

[–,HP,–] Export of data

6.7.128. Agencies **should** restrict the export of data to a system of a lesser security classification by filtering data using at least:

a. protective marking checks
b. limitations on data types, and
c. keyword searches.

[–,–,C-TS] Export of highly formatted textual data

6.7.129. When agencies export formatted textual data with no free text fields and all fields have a predefined set of permitted values agencies **must** implement the following controls:

a. protective marking checks
b. log of each event, and
c. monitoring to detect overuse/unusual usage patterns.

[–,–,C-TS] Export of other data

6.7.130. When agencies export data, other than highly formatted textual data, agencies **must** implement the following controls:

a. protective marking checks
b. log of each event
c. monitoring to detect overuse/unusual usage patterns
d. data format checks
e. keyword searches, and
f. size limits.

[–,–,C-TS] Export of highly formatted textual data through a gateway/CDS

6.7.131. When the export of highly formatted textual data occurs through a gateway/CDS agencies **must** additionally implement:

a. data filtering performed by a product with at least an EAL2 level of assurance that has been specifically evaluated for that purpose
b. data range checks, and
c. full or partial audits of the event logs performed at least monthly.

[–,–,C-TS] Export of other data through a gateway/CDS

6.7.132. When agencies export data, other than highly formatted textual data, through a gateway/CDS, agencies **must** additionally implement data filtering performed by a product with at least an EAL2 level of assurance that has been specifically evaluated for that purpose.

6.7.133. When the export of other data occurs through a gateway/CDS agencies **should** perform audits of the complete data transfer logs at least monthly.

6.7.134. When agencies do not perform audits of the complete data transfer logs at least monthly they **must** perform randomly timed audits of random subsets of the data transfer logs on a weekly basis.

[–,–,C-TS] Requirement to sign exported data

6.7.135. If, to reach the transfer point, the data is communicated over a network to which people or systems that are not trusted sources have access, the trusted source **must** sign the data to be exported.

6.7.136. Agencies **should** use a product evaluated to at least an EAL4 assurance level and having completed a DCE to perform data signing and signature confirmation.

6.7.137. Agencies **must** ensure that the gateway/CDS confirms the signature prior to the release of the data to be exported.

[–,IC-HP,R-TS] Preventing export of AUSTEO/AGAO data to foreign systems

6.7.138. Agencies **must**:

a. ensure that keyword searches are performed on all textual data
b. ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator
c. develop procedures to prevent AUSTEO or AGAO information in both textual and non-textual formats from being exported, and
d. implement data filtering performed by a product with at least an EAL2 level of assurance that has been specifically evaluated for that purpose.

GUIDANCE

[–,–,C-TS] Data import

6.7.139. It is **recommended** that agencies translate data being imported at the gateway/CDS into another format before entering the network.

RATIONALE

Data import

6.7.140. Scanning imported data for malicious content reduces the security risk of a system or network being infected, thus allowing the continued confidentiality, integrity and availability of the system or network.

6.7.141. Format checks provide a method to prevent known malicious formats from entering the system or network. Keeping and regularly auditing these logs allow for the system or network to be checked for any unusual usage.

6.7.142. In order to ensure the continued functioning of systems it is important to constantly run analysis on data being imported over a network.

6.7.143. Translating data from one format into another effectively destroys most malicious active content.

Export of data

6.7.144. In order to ensure the continued integrity and confidentiality of data on an agency network, data must pass through a series of checks before it is exported onto systems of a lesser security classification.

6.7.145. Filtering content based on protective markings is an adequate method to protect the confidentiality of low security classified material.

6.7.146. For HIGHLY PROTECTED material, to ensure confidentiality the added controls of data type checking and searches in the data for keywords also allows for a more in-depth check for information to prevent leaks.

6.7.147. Using a trusted source to approve the transfer of higher security classified data reduces the security risk by having another person or system trusted by the agency run through the data to determine if export is possible.

Export of highly formatted textual data

6.7.148. The security risks of releasing higher security classified data are partially reduced when the data is restricted to highly formatted textual data. In such cases the data is less likely to contain hidden data and have security classified content. Such data can be automatically scanned through a series of checks to detect security classified content. In addition, security risk is further reduced when there is a gateway/CDS filter that refuses to export data security classified above the security classification of the network outside of the gateway/CDS, and logs are regularly reviewed to detect if there has been unusual usage or overuse.

Export of other data

6.7.149. Textual data which is not highly formatted can contain hidden data as well as having a higher security classification due to the aggregated content. Security risk is somewhat reduced by running additional automated checks on non-formatted data being exported in addition to those for highly formatted textual data. A human trusted source also should assess the security classification of the content of the data, which cannot be interpreted by automated means.

Requirement to sign exported data

6.7.150. Digitally signing data being exported to systems where there is access by non-trusted sources reduces the security risk of compromising data integrity.

Preventing export of AUSTEO/AGAO data to foreign systems

6.7.151. In order to reduce the security risk of spilling data with a caveat onto foreign systems, it is important that procedures are developed to detect AUSTEO and AGAO data and to prevent it from crossing into foreign systems.

Content Filtering

PRINCIPLE

6.7.152. The control of the flow of data within a gateway/CDS is achieved by using a content filter that is capable of limiting transfers by file type and content.

OBJECTIVE

6.7.153. To ensure that files that can be communicated though a gateway/CDS, and the content of such files, contain only explicitly approved content.

CONTEXT

Scope

6.7.154. This section covers information relating to the use of content filters within bi-directional or one-way gateway/CDSs.

RISKS

6.7.155. An attacker sends a malicious email attachment that compromises the receiving host.

6.7.156. An attacker subverts a host by obfuscating a malicious payload and subsequently reads information.

6.7.157. An attacker sends a malicious email attachment that subverts the email proxy software and reads other email passing through the proxy.

6.7.158. An attacker sends a malicious payload to a Web service that compromises the Web server and queries the database for information.

6.7.159. A website with a malicious payload is accessed by a system user inside an agency, compromising the internal network.

6.7.160. An attacker sends malformed queries to a server, compromising integrity and causing a denial of service.

6.7.161. An attacker sends correctly formatted, but out-of-scope data to a server, compromising integrity and causing a denial of service.

6.7.162. Personnel accidentally or deliberately send information to a system of lower a security classification, compromising confidentiality.

6.7.163. Personnel send a document with security classified metadata to a system with a lesser security classification, compromising confidentiality.

6.7.164. Personnel send inappropriate material to other personnel or external parties and provoke legal or ethical consequences.

6.7.165. Personnel purposely or inadvertently access a website that contains inappropriate material, provoking legal or ethical consequences.

6.7.166. An external party sends inappropriate material, or spam email, to personnel, disturbing them.

CONTROLS

[U,IC-P,R] Limiting transfers by file type

6.7.167. Agencies **should** strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.

[–,HP,C-TS] Limiting transfers by file type

6.7.168. Agencies **must** strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.

[–,HP,C-TS] Blocking active content

6.7.169. Agencies **should** block all executables and active content from being communicated though a gateway/CDS.

[U,IC-HP,R-TS] Blocking suspicious data

6.7.170. Agencies **must** block or drop any data identified by a data filter as suspicious until reviewed and approved for transfer by a trusted source other than the originator.

GUIDANCE

[U,IC-HP,R-TS] Content filtering strategies

6.7.171. It is **recommended** that content filtering strategies employed by an agency include:

a. offensive language modification in chat applications
b. blocking emails being sent which contain content or attachments with 'dirty words'
c. blocking DoS attacks
d. blocking hate websites
e. blocking gambling websites
f. blocking pornographic images, and
g. blocking password-protected compressed files.

RATIONALE

Content filtering

6.7.172. The table below identifies some filtering techniques used to control data transfer.

TECHNIQUE	PURPOSE
Antivirus scan	Scans the data for viruses and other malicious code.
Data format check	Inspects data to ensure that it conforms to expected/permitted format(s).
Data range check	Checks the data within each field to ensure that it falls within the expected/permitted range.
Data type check	Inspects each file header to determine the file type.
File extension check	Checks file extensions to ensure that they are permitted.
Keyword search	Searches data for keywords or 'dirty words' that could indicate the presence of security classified or inappropriate material.
Metadata check	Inspects files for metadata that should be removed prior to release.
Protective marking check	Validates the protective marking of the data to ensure that it complies with the permitted security classifications and caveats.
Visual inspection	The manual inspection of data for over-information and other suspicious content that an automated system could miss, which is particularly important for the transfer of image files.

Limiting transfers by file types

6.7.173. The level of security risk will be effected by the degree of assurance agencies can place in the ability of their data transfer filters to:

- confirm the file type by examination of the contents of the file
- confirm the absence of malicious content
- confirm the absence of inappropriate content
- confirm the security classification of the content, and
- handle compressed files appropriately.

6.7.174. Reducing allowed file types reduces the number of potential vulnerabilities available for an attacker to exploit.

Blocking active content

6.7.175. Many files are executable and are potentially harmful if activated by a system user.

6.7.176. Many static file type specifications allow active content to be embedded within the file, which increases the attack surface.

Blocking suspicious data

6.7.177. The definition of suspicious content will depend on the system's risk profile and what is considered normal traffic.

Firewalls

PRINCIPLE

6.7.178. The protection of networks connected to a bi-directional gateway/CDS is achieved through the use of firewalls and traffic flow filters.

OBJECTIVE

6.7.179. To ensure that firewalls are used to protect connected networks and to control data flow through a bi-directional gateway/CDS.

CONTEXT

Scope

6.7.180. This section covers information relating to filtering requirements for bi-direction gateway/CDSs between networks of allowable security classifications achieved through discrete components.

6.7.181. Logging and filtering requirements for one-way gateway/CDSs involving national security classified networks above the security classification of CONFIDENTIAL are also covered in this section.

6.7.182. When a control specifies a requirement for a diode or filter the appropriate information can be found within the *Diodes* and *Content Filtering* sections of this chapter. Additional information that also applies to topics covered in the section can be found in the *Data Import and Export* section of this chapter.

Inter-connecting networks within an agency

6.7.183. When connecting networks accredited to the same security classification and set of caveats within an agency the requirements of this section do not apply.

6.7.184. When connecting networks accredited with different security classifications or caveats within an agency the information in this section still applies.

RISKS

6.7.185. An attacker on a less secure network (e.g. the Internet) launches a malicious attack on a more sensitive network that results in a data spill or denial of service.

6.7.186. An agency deploys a firewall that provides an inappropriate level of assurance for the security classification of the networks that it connects to resulting in unintended network traffic flow.

CONTROLS

[U,IC-HP,R-TS] Selecting a traffic flow filter

6.7.187. When selecting a traffic flow filter, agencies **should** use one or more of the following, in the order of preference as shown:

a. a firewall
b. a proxy, or
c. a router with appropriate access control lists configured.

[U,IC-HP,R-TS] Firewall assurance levels

6.7.188. Agencies **must** use devices as shown in the following table, for both gateway/CDSs, when connecting two networks of different security classifications or two networks of the same security classification but different security domains.

YOUR NETWORK	IS CONNECTED TO A NETWORK THAT IS	YOUR GATEWAY/ CDS REQUIRES
UNCLASSIFIED	• UNCLASSIFIED • non-national security • national security	a traffic flow filter
X-IN-CONFIDENCE	• UNCLASSIFIED	an EAL2 firewall
	• non-national security • national security	a traffic flow filter
RESTRICTED	• UNCLASSIFIED • X-IN-CONFIDENCE	an EAL2 firewall
	• PROTECTED • HIGHLY PROTECTED • national security	a traffic flow filter
PROTECTED	• UNCLASSIFIED	an EAL4 firewall
	• X-IN-CONFIDENCE • RESTRICTED	an EAL3 firewall
	• PROTECTED	an EAL2 firewall
	• HIGHLY PROTECTED • CONFIDENTIAL • SECRET • TOP SECRET	an EAL1 firewall
HIGHLY PROTECTED	• UNCLASSIFIED	an EAL4 firewall plus diodes with separate upward and downward data flows
	• X-IN-CONFIDENCE • RESTRICTED	an EAL4 firewall
	• PROTECTED	an EAL3 firewall
	• HIGHLY PROTECTED • CONFIDENTIAL • SECRET • TOP SECRET	an EAL2 firewall

Continued on next page

YOUR NETWORK	IS CONNECTED TO A NETWORK THAT IS	YOUR GATEWAY/ CDS REQUIRES
CONFIDENTIAL	• UNCLASSIFIED	an EAL4 firewall plus diodes with separate upward and downward data flows
	• X-IN-CONFIDENCE • RESTRICTED	an EAL4 firewall
	• PROTECTED	an EAL3 firewall
	• HIGHLY PROTECTED • CONFIDENTIAL • SECRET • TOP SECRET	an EAL2 firewall
SECRET	• UNCLASSIFIED	Consultation with DSD
	• non-national security • RESTRICTED • CONFIDENTIAL	an EAL4 firewall plus diodes with separate upward and downward data flows
	• SECRET • TOP SECRET	an EAL2 firewall
TOP SECRET	• UNCLASSIFIED • non-national security • RESTRICTED • CONFIDENTIAL	Consultation with DSD
	• SECRET	an EAL4 firewall plus diodes with separate upward and downward data flows
	• TOP SECRET	an EAL2 firewall

[–,IC-HP,R-TS] Firewall assurance levels for AUSTEO and AGAO networks

6.7.189. Agencies **must** use a firewall of at least an EAL4 assurance level between an AUSTEO or AGAO network and a foreign network in addition to the minimum assurance levels for firewalls between networks of different security classifications.

6.7.190. Agencies **should** use a firewall of at least an EAL2 assurance level between an AUSTEO or AGAO network and another Australian controlled network in addition to the minimum assurance levels for firewalls between networks of different security classifications.

GUIDANCE

[U,IC-HP,R-TS] Connecting networks within an agency

6.7.191. If connecting networks within an agency that have the same security classification and are accredited for the same set of caveats, no gateway/CDS controls are mandated; however it is **recommended** that agencies use at least a traffic flow filter.

RATIONALE

Firewall assurance levels

6.7.192. A firewall provides greater degree of control over filtering requirements than a proxy, which provides greater degree of control than a router. The higher the assurance level for a firewall the greater the assurance that it provides an appropriate level of assurance that the specified security functionality will operate as claimed.

6.7.193. If a uni-directional connection between two networks is being implemented only one gateway is required with requirements being determined based on the source and destination networks. However, if a bi-directional connection between two networks is being implemented two gateways will be required with requirements being determined based on the source and destination networks.

EXAMPLES

6.7.194. An agency owning a HIGHLY PROTECTED network and a SECRET network wishes to connect them together. As such the gateway/CDS between the HIGHLY PROTECTED network and the SECRET network requires an EAL2 firewall whilst the gateway/CDS between the SECRET network and the HIGHLY PROTECTED network requires an EAL4 firewall plus diodes with separate upward and downward data flows.

6.7.195. The reason for the different security measures is that as the SECRET network is more secure than the HIGHLY PROTECTED network the system owner of the HIGHLY PROTECTED network only needs to be concerned with the need-to-know principle relating to information being transferred upwards from their network. The system owner of the SECRET network however also needs to be concerned with a potential data spill of SECRET information onto the HIGHLY PROTECTED network if an appropriately secure gateway/CDS is not implemented.

Diodes

PRINCIPLE

6.7.196. The prevention of information spills from a more sensitive network connected to a less sensitive network via a one-way gateway/CDS is achieved through the use of diodes.

OBJECTIVE

6.7.197. To ensure that diodes are used to protect connected networks and to control data flow through a one-way gateway/CDS.

CONTEXT

Scope

6.7.198. This section covers information relating to filtering requirements for one-way gateway/CDSs used to facilitate data transfers. Additional information that also applies to topics covered in the section can be found in the *Content Filtering* and *Data Import and Export* section of this chapter.

RISKS

6.7.199. An attacker communicates malicious code to the higher security classified network that releases unauthorised data to the less sensitive network.

6.7.200. An agency deploys a diode that does not give an appropriate level of assurance for the security classification of the networks that it connects to resulting in unintended network traffic flow.

CONTROLS

[U,IC-P,R] Diode assurance levels

6.7.201. For controlling the data flow of one-way gateway/CDSs of different security classifications, where the highest security classification is PROTECTED or RESTRICTED, agencies **should** use a diode evaluated to at least an EAL2 assurance level.

[–,HP,–] Diode assurance levels

6.7.202. For controlling the data flow of one-way gateway/CDSs of different security classifications, where the highest security classification is HIGHLY PROTECTED, agencies **must** use a diode evaluated to at least the EAL4 assurance level.

[–,–,C-TS] Diode assurance levels

6.7.203. For controlling the data flow of one-way gateway/CDSs of different security classifications, where the highest security classification is TOP SECRET, agencies **must** use a diode evaluated to the high grade or EAL7 assurance level.

[–,IC-HP,R-TS] Diode assurance levels for AUSTEO and AGAO networks

6.7.204. Agencies **must** use a diode of at least an EAL4 assurance level between an AUSTEO or AGAO network and a foreign network in addition to the minimum assurance levels for diodes between networks of different security classifications.

6.7.205. Agencies **should** use a diode of at least an EAL2 assurance level between an AUSTEO or AGAO network and another Australian controlled network in addition to the minimum assurance levels for diodes between networks of different security classifications.

[U,IC-HP,R-TS] Volume checking

6.7.206. Agencies deploying a diode to control data flow within a one-way gateway/CDS **should** monitor the volume of the data being transferred.

RATIONALE

Diodes

6.7.207. A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. As such, it is much more difficult for an attacker to use the same path to both launch an attack and release the information.

Diode assurance levels

6.7.208. Using diodes of higher assurance levels for higher security classified networks provides an appropriate level of assurance to agencies that the specified security functionality of the product will operate as claimed.

Volume checking

6.7.209. Monitoring the volume of data being transferred across a diode will ensure that it conforms to expectations. It can also alert the agency to potential malicious activity if the volume of data suddenly changes from the norm.

Peripheral Switches

PRINCIPLE

6.7.210. Peripheral switches of appropriate assurance levels can prevent unintended connections occurring when connecting two systems to a peripheral switch.

OBJECTIVE

6.7.211. To ensure that evaluated peripheral switches are used to ensure that they do not leak information between connected systems.

CONTEXT

Scope

6.7.212. This section covers information relating specifically to the use of keyboard/video/mouse switches.

Peripheral switches with more than two connections

6.7.213. If the peripheral switch has more than two systems connected then the level of assurance needed is determined by the highest and lowest of the security classifications involved.

RISKS

6.7.214. Information is communicated between systems connected to a peripheral switch, resulting in a data spill.

CONTROLS

[–,P,R] Assurance requirements

6.7.215. Agencies accessing a security classified system and an UNCLASSIFIED system via a peripheral switch **should** use an evaluated product with an EAL2 level of assurance.

[–,HP,C-TS] Assurance requirements

6.7.216. Agencies accessing a security classified system and a less security classified system via a peripheral switch **must** use an evaluated product with a level of assurance as indicated in the table below.

	SYSTEMS CONNECTED VIA THE PERIPHERAL SWITCH						
	U	IC	R	P	HP	C	S
HP	EAL4	EAL2	EAL2	EAL2	-	-	-
C	EAL7	EAL4	EAL4	EAL2	EAL2	-	-
S	high grade	EAL7	EAL7	EAL7	EAL7	EAL4	-
TS	high grade	high grade	high grade	high grade	high grade	high grade	high grade

[–,IC-HP,R-TS] Assurance requirements

6.7.217. Agencies accessing a system containing AUSTEO or AGAO information and a system of the same security classification that is not accredited to process the same caveat **should** use an evaluated product with an EAL2 level of assurance.

GUIDANCE

[–,IC,–] Assurance requirements

6.7.218. It is **recommended** that agencies accessing a security classified system and an UNCLASSIFIED system via a peripheral switch use an evaluated product with an EAL2 level of assurance.

Working Off-Site Security

Working Off-Site Fundamentals

PRINCIPLE

6.8.1. Information can be accessed and communicated when working off-site, either from a home-based environment, outside of the office or from a contractor's facility, if appropriate security measures are implemented.

OBJECTIVE

6.8.2. To ensure that when working off-site that as many security measures as reasonable for the environment are implemented to prevent the compromise of information.

CONTEXT

Scope

6.8.3. This section covers information that is common to accessing information using devices, including portable electronic devices (PEDs), laptops and workstations, from a home-based environment, from outside the office or from a contractor's facility.

RISKS

6.8.4. An agency allows off-site users to use non-agency owned and controlled devices loosing control over how devices are used to process, store and communicate security classified information.

6.8.5. An attacker compromises a poorly controlled device and uses it to exploit connected systems and networks.

6.8.6. An attacker compromises a poorly controlled device and gains access to information.

6.8.7. An attacker infects a device when connected to an unsecured network which later infects an agency controlled network when the device next connects to it.

6.8.8. An attacker compromises a device through an unsecured network gaining access to information.

CONTROLS

[–,IC-P,R] Non-agency owned devices

6.8.9. Agencies **should not** allow devices not directly owned and controlled by the agency to be used with their systems.

[–,HP,C-TS] Non-agency owned devices

6.8.10. Agencies **must not** allow devices not directly owned and controlled by the agency to be used with their systems.

[U,IC-HP,R-TS] Non-agency owned devices

6.8.11. If a non-agency owned device is used, the owner **must** be made aware of any actions that might need to be taken as a result of information security incidents.

6.8.12. If a non-agency owned device is used it **should** be managed and accounted for in the same manner as agency owned devices.

[U,IC-HP,R-TS] Configuration control

6.8.13. Agencies **should** control the configuration of devices used for off-site work in the same manner as devices in the agency's corporate environment.

[U,IC-P,R] Configuration control

6.8.14. Agencies **should** prevent personnel from installing or uninstalling applications and enabling or disabling security functions of a device once supplied.

[–,HP,C-TS] Configuration control

6.8.15. Agencies **must** prevent personnel from installing or uninstalling applications and enabling or disabling security functions of a device once supplied.

[U,IC-HP,R-TS] VPN split tunnelling

6.8.16. Agencies **must** disable split tunnelling when using VPN technology from devices connecting to agency systems.

[U,IC-HP,R-TS] Connecting devices to unsecured networks

6.8.17. Agencies **should not** allow devices to connect to the Internet except when temporarily connecting to facilitate the establishment of a VPN connection to agency networks.

6.8.18. Agencies **should** ensure that a firewall is used to protect devices from any potential threats originating from unsecured networks.

[–,–,TS] Requirement for off-site work

6.8.19. Agencies **must not** work off-site using devices storing TOP SECRET information unless explicitly approved by DSD to do so.

GUIDANCE

[U,IC-HP,R-TS] Requirement for off-site work

6.8.20. It is **recommended** that agencies ensure that if they are allowing off-site work they:

a. have a policy and associated procedures for the issue and use of the devices and associated services
b. ensure that personnel acknowledge the policy and associated procedures
c. ensure that personnel are trained in the use of the devices and their associated services, and
d. have a policy and procedures governing connections from the devices to their agency systems.

[U,–,–] Non-agency owned devices

6.8.21. It is **recommended** that agencies ensure that devices not directly owned and controlled by the agency are not approved for use with their systems.

[U,IC-HP,R-TS] Configuration control

6.8.22. It is **recommended** that agencies regularly test agency provided devices to ensure that they are still secure.

6.8.23. It is **recommended** that agencies ensure that agency provided devices used for off-site work are brought back to the agency for periodic testing and security updates.

RATIONALE

Non-agency owned devices

6.8.24. Non-agency owned devices might need to be confiscated, examined, sanitised or destroyed in the case of an information security incident.

Configuration control

6.8.25. Poorly controlled devices are more vulnerable to compromise and provide an attacker with a potential access point into agency systems.

6.8.26. Although agencies may provide an initially secure device, the state of security may degrade over time. The agency will need to revaluate the security of the device occasionally to ensure its integrity.

VPN split tunnelling

6.8.27. A split tunnel VPN can allow access to an agency's systems from another network, including unsecured networks such as the Internet. If split tunnelling is not disabled there is an increased security risk that the VPN connection is susceptible to attack from such networks.

Connecting devices to unsecured networks

6.8.28. During the period that a device is connected to the Internet without a VPN connection being established it is exposed to attacks originating from the Internet. As such, this period needs to be minimised to reduce the security risks. Minimising this period includes ensuring that system users do not connect to the Internet to access the Web between VPN sessions.

Working From Home

PRINCIPLE

6.8.29. Security classified information can be accessed from a home environment in a secure manner when security measures are implemented to protect devices, systems and networks.

OBJECTIVE

6.8.30. To ensure that appropriate measures are applied to devices associated with accessing information from a home environment.

CONTEXT

Scope

6.8.31. This section covers information on accessing information using devices, including laptops and workstations, from a home environment in order to conduct home-based work.

RISKS

6.8.32. An attacker gains access to information stored on a device resulting in a compromise of the information.

6.8.33. An attacker develops a persistent exploit of the home environment resulting in a continual compromise of information.

CONTROLS

[–,IC-HP,R-TS] Storage requirements

6.8.34. Agencies **must** ensure devices with security classified media, when not being used, are secured in accordance with the minimum physical security storage requirements specified in the PSM.

[–,IC-HP,R-TS] Processing requirements

6.8.35. Agencies **must** ensure that the area (e.g. home office) within which devices with security classified media are used meets the minimum physical security requirements for processing information as specified in the PSM.

[–,IC-HP,R-TS] Protecting devices

6.8.36. Agencies **should** encrypt information on all devices using at least a DACA.

RATIONALE

Storage requirements

6.8.37. All devices have the potential to store information and therefore need protection against loss and compromise. As such even if the intent of the agency is not to reduce the storage or physical transfer requirements of the device using a product that has undergone a DCE they still should use a product that implements a DACA.

Processing requirements

6.8.38. When agencies consider allowing personnel to work from a home environment they need to be aware that the PSM requires the full security measures from Part E to be met. Implementing such measures may require modifications to the person's home at the expense of the agency.

EXAMPLES

6.8.39. An agency using X-IN-CONFIDENCE laptops for personnel working from home chooses to install an open source encryption product using a DACA to meet the requirement for encryption of the device. As a product implementing a DACA is approved for lowering the storage and physical transfer requirements of X-IN-CONFIDENCE assets to that of UNCLASSIFIED assets, the agency stores the devices during non-operational hours as per the PSM requirements for the storage of UNCLASSIFIED assets.

Working Outside the Office

PRINCIPLE

6.8.40. Security classified information can not be accessed from public locations.

OBJECTIVE

6.8.41. To ensure that security classified information is not accessed from public locations.

CONTEXT

Scope

6.8.42. This section covers information on accessing information using mobile devices, including PEDs and laptops, from unsecured locations outside the office, including public locations. This section does not apply to working from home and shouldn't be used as a substitute for specific requirements relating to such activities as outlined in the *Working From Home* section in this chapter.

Devices with data and voice functions

6.8.43. Mobile devices often have both a data and voice component capable of processing or communicating information. In such cases, personnel will need to be aware of the security classification that has been approved for being processed or communicated via each function.

Devices with multiple operating states

6.8.44. Some mobile devices may have functionality to allow it to operate in either an non-security classified state or a security classified state. In such cases the device will need to be handled according to the state that it is being operated in at the time. For example, some PEDs can start-up in an UNCLASSIFIED mode or start-up in a cryptographically protected mode.

RISKS

6.8.45. An attacker oversees information while a device is in use resulting in a compromise of the information.

6.8.46. An attacker overhears a conversation while a voice call is being made resulting in a compromise of the information

6.8.47. An attacker gains access to information stored on a device resulting in a compromise of the information.

6.8.48. An attacker exploits weak communications protocols used between devices and peripherals resulting in the compromise of information.

6.8.49. Personnel accidentally lose their device in a public location which is later found and compromised resulting in the unauthorised disclosure of information.

6.8.50. An agency uses traditional labelling on a device as a result raising its attractiveness to attackers looking to compromise government information.

CONTROLS

[–,IC-HP,R-TS] Working outside the office

6.8.51. Agencies **should not** allow personnel to access or communicate security classified information in public locations (e.g. public transport, transit lounges and coffee shops).

[–,IC,R] Working outside the office

6.8.52. Agencies **must not** allow personnel to access or communicate security classified information outside of areas certified to process the security classification of the information unless there is a reduced chance of being overheard or observed.

[–,P-HP,C-TS] Working outside the office

6.8.53. Agencies **must not** allow personnel to access or communicate security classified information outside of areas certified to process the security classification of the information.

[–,IC-HP,R-TS] Protecting devices

6.8.54. Agencies **should** encrypt information on all devices using at least a DACA.

[–,IC-HP,R-TS] Carrying devices

6.8.55. Agencies **must** ensure devices are protected as per the physical transfer requirements of the PSM.

[–,IC-HP,R-TS] Using devices

6.8.56. When in use devices **must** be kept under continual direct supervision.

[–,IC-HP,R-TS] Bluetooth-enabled peripherals

6.8.57. Personnel using devices capable of conducting phone conversations while using Bluetooth-enabled peripherals **must not** conduct conversations while Bluetooth functionality is enabled.

6.8.58. Devices with Bluetooth serial port connections **must not** have the port enabled if the device is to process or store security classified information.

[U,IC-P,R] Emergency destruction

6.8.59. Agencies **should** develop an emergency destruction plan for any devices used in situations where there is a higher probability of loss or compromise.

[–,HP,C-TS] Emergency destruction

6.8.60. Agencies **must** develop an emergency destruction plan for devices.

6.8.61. If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a device it **must** be used as part of the emergency destruction procedures.

GUIDANCE

[U,IC-P,R] Emergency destruction

6.8.62. It is **recommended** that agencies develop an emergency destruction plan for devices.

[U,IC-HP,R-TS] Labelling

6.8.63. It is **recommended** that agencies use soft labelling for devices where possible to reduce their attractiveness value.

RATIONALE

Working outside the office

6.8.64. As agencies have no control over public locations including, but not limited to, such locations as public transport, transit lounges and coffee shops, devices are not approved to process security classified information as the security risk is considered to be too high.

6.8.65. In some cases personnel may require access to security classified information when outside the office environment, e.g. when travelling for work. In such situations an appropriate facility certified to the security classification that needs to be accessed or communicated may not be readily available. As such a physically protected area that protects personnel from being overheard or observed can be used. However, agencies should note that in doing so they will still need to waive requirements from Part H of the PSM relating to the physical certification of areas where off-site work is conducted.

6.8.66. As the security risk relating to specific targeting of devices capable of processing higher security classifications is much higher than for lower security classifications, these devices can not be used outside of facilities certified to an appropriate level to allow for their use.

Carrying devices

6.8.67. As devices used outside the office are transferred through areas not certified to process the information on the device, protection mechanisms need to be put in place to protect the information. As the PSM requirements for the physical transfer of security classified information are based on paper-based material and not electronic-based material the security risk is vastly different.

6.8.68. When agencies apply encryption to devices it may reduce the requirements for physical transfer as outlined in the PSM. The application of encryption does not automatically render the device UNCLASSIFIED. The reduction of any requirements is based on the original security classification of information residing on the device and the level of assurance in the cryptographic function being used to encrypt the media.

6.8.69. In all cases a device with encryption can only be treated as per the requirements for a lesser security classification if the cryptographic function on the device has not been authenticated to. In most cases this will mean the device will be in an unpowered state (i.e. not turned on). However, some devices are capable of deauthenticating the cryptography when it enters a locked state after a predefined timeout period. Such devices can be carried in a locked state in accordance with reduced physical transfer requirements based on the assurance given in the cryptographic functions.

6.8.70. Further information on reducing physical transfer requirements can be found in the *Cryptographic Fundamentals* section within this manual.

Labelling

6.8.71. Agencies may wish to affix an additional label to devices used in public areas asking finders of lost devices to hand the equipment in to any Australian police station or, if overseas, an Australian embassy, consulate or high commission.

Outsourcing and Industry Engagement

PRINCIPLE

6.8.72. Government information can be accessed by contractors from off-site locations if they are compliant with the requirements of the ISM and PSM.

OBJECTIVE

6.8.73. To ensure that when contractors are provided with government information that it is appropriately protected.

CONTEXT

Scope

6.8.74. This section covers information on outsourcing information technology services and functions to contractors as well as providing those partners with government information in order to undertake their contracted duties.

RISKS

6.8.75. A contractor provided with government information fails to provide appropriate protection to the information which is subsequently disclosed in the public domain without the authorisation of the information owner.

6.8.76. An agency fails to implement a coordinated approach to industry engagement resulting in an ad-hoc and inconsistent approach to the engagement of contractors to provide outsourced information technology services.

CONTROLS

[U,IC-HP,R-TS] Outsourcing information technology services and functions

6.8.77. Agencies engaging industry for the provision of off-site information technology services and functions **must** accredit the systems used by the contractor to at least the same minimum standard as the agency's systems.

6.8.78. Agencies **should not** engage industry for the provision of off-site information technology services and functions in countries that Australia does not have a bi-lateral security agreement with for the protection of Australian government information.

GUIDANCE

[U,IC-HP,R-TS] Developing an industry security program

6.8.79. It is **recommended** that agencies develop an industry security program to manage contractors that have been accredited for the provision of off-site information technology services and functions.

RATIONALE

Outsourcing information technology services and functions

6.8.80. Contractors can be provided with government information, including security classified information, as long as their systems are accredited to process, store and communicate the information.

Developing an industry security program

6.8.81. The development of an agency industry security program will assist the agency in undertaking a coordinated approach to the engagement and use of contractors for outsourcing and provision of information technology services and functions.

Glossary of Acronyms and Initialisms

3DES	Triple Data Encryption Standard
ACSI	Australian Communications-Electronic Security Instruction
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AGIMO	Australian Government Information Management Office
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
ASA	agency security advisor
ASIO	Australian Security Intelligence Organisation
AUSTEO	Australian Eyes Only
CDS	cross domain solutions
CEO	chief executive officer
CISO	chief information security officer
COMSEC	communications security
CSO	chief security officer
DACA	DSD approved cryptographic algorithm
DACP	DSD approved cryptographic protocol
DCE	DSD cryptographic evaluation
DH	Diffie-Hellman
DIO	Defence Intelligence Organisation
DKIM	DomainKeys Identified Mail
DoS	Denial-of-Service
DSA	Digital Signature Algorithm
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	electrically erasable programmable read-only memory
EPL	*Evaluated Products List*
EPLD	*Evaluated Product List - Degausser*
EPROM	erasable programmable read-only memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GPU	graphics processing unit

HGCE	high grade cryptographic equipment
HMAC	hashed message authentication code
HTTPS	Hypertext Transfer Protocol Secure
ICT	information and communications technology
IDS	intrusion detection system
IETF	International Engineering Task Force
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
IRC	Internet Relay Chat
IPT	Internet Protocol telephony
IRP	incident response plan
ISAKMP	Internet Security Association Key Management Protocol
ISIR	Information Security Incident Reporting scheme
ISM	*Australian Government Information Security Manual*
ISP	information security policy
ITSA	information technology security advisor
ITSEC	Information Technology Security Evaluation Criteria
ITSM	information technology security manager
ITSO	information technology security officer
KMP	key management plan
MFD	multifunction device
OWASP	Open Web Application Security Project
PED	portable electronic device
PSM	*Australian Government Protective Security Manual*
PSTN	public switched telephone network
RAM	random access memory
RF	radio frequency
RFC	request for comments
RSA	Rivest-Shamir-Adleman
RTP	Real-time Transport Protocol
SCEC	Security Construction and Equipment Committee
SCIF	secure compartmented intelligence facility
SHA	Secure Hashing Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SOE	Standard Operating Environment
SOP	standard operating procedure
SPF	Sender Policy Framework

SRMP	security risk management plan
SSH	Secure Shell
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSP	system security plan
VLAN	virtual local area network
VPN	virtual private network
WAP	wireless access point
WEP	Wired Equivalent Privacy
WLAN	wireless local area network
WPA2	Wi-Fi Protected Access 2
XAUTH	IKE Extended Authentication

Glossary of Terms

802.11	The Institute of Electrical and Electronics Engineers standard defining WLAN communications.
absolute risk	The level of risk without taking into consideration existing controls.
access gateway/cross domain solution	A gateway/CDS that provides the system user access to multiple security domains from a single device, typically a workstation.
accountable COMSEC material	Security classified material bearing the CRYPTO caveat. It applies primarily to cryptographic keying material used in securing HGCE.
accreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system.
accreditation authority	The authoritative body associated with accreditation activities.
agency	Australian Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the Public Service Act.
agency head	The government employee with ultimate responsibly for the secure operation of agency functions, whether performed in-house or outsourced.
application whitelisting	An approach in which all executables and applications are prevented from executing by default, with an explicitly defined set of executables allowed to execute.
asset	Anything of value to an agency, such as hardware and software components, data, personnel, documentation, reputation and public confidence.
attack surface	The amount of hardware and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability.
audit	An independent review of event logs and related activities performed to determine the adequacy of current security measures, to identify the degree of conformance with established policy or to develop recommendations for improvements to the security measures currently applied.
Australasian Information Security Evaluation Program	A program under which evaluations are performed by impartial companies against the Common Criteria. The results of these evaluations are then certified by DSD, which is responsible for the overall operation of the program.
Australian Eyes Only	A caveat indicating that the information is not to be passed to or accessed by foreign nationals.
Australian Government Access Only	A caveat used by the Department of Defence and ASIO indicating the information is not to be passed to or accessed by foreign nationals, with the exception of seconded foreign nationals. Such material received in other agencies must be handled as if it were marked as AUSTEO.
Australian Government Information Security Manual	National security policy that aims to provide a common approach to ensure that the implementation of information security reduces both agency specific, and whole of government, security risks to an acceptable level.
Australian Government Protective Security Manual	National security policy that aims to provide a common approach to ensure that the implementation of protective security (mainly physical and personnel) reduces both agency specific, and whole of government, security risks to an acceptable level.
Authentication Header	A protocol used for authentication within IPSec.

baseline	A release of this manual including errata and interim policy releases.
blacklist	A set of inclusive non-accepted items that confirm the item being analysed is not acceptable. It is the opposite of a whitelist which confirms that items are acceptable.
cascaded connections	Cascaded connections occur when one network is connected to another, which has a connection to a third network, and so on.
caveat	A marking that indicates that the information has special requirements in addition to those indicated by the security classification. The term covers codewords, source codewords, releasability indicators and special-handling caveats.
certification	A procedure by which a formal assurance statement is given that a deliverable confirms to a specified standard.
certification authority	An official with the authority to assert that a system complies with prescribed controls within a standard.
certification report	A report generated by a certification body of a Common Criteria scheme that provides a summary of the findings of an evaluation.
chief information security officer	A senior executive who is responsible for coordinating communication between security and business functions as well as the overseeing the application of information security controls and security risk management processes within an agency.
Closed Internet Protocol network	An IPT network is considered closed if it only allows connections within an agency's infrastructure, and has no mechanism to connect to a public analog or data network. Closed IPT networks can traverse public analog or data networks providing appropriate data in transit encryption requirements are met.
coercivity	A property of magnetic material, used as a measure of the amount of coercive force required to reduce the magnetic induction to zero from its remnant state.
Common Criteria	An International Organization for Standardization standard (15408) for information security evaluations.
Common Criteria Recognition Arrangement	An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes, including the Australian and New Zealand certification scheme.
communications security	The measures and controls taken to deny unauthorised personnel information derived from telecommunications and to ensure the authenticity of such telecommunications.
compartmented mode	Not all system users are formally authorised to access all compartments of information processed by the system.
conduit	A tube, duct or pipe used to protect cables.
connection forwarding	The use of network address translation to allow a port on a network node inside a local area network to be accessed from outside the network. Alternatively, using a Secure Shell server to forward a Transmission Control Protocol connection to an arbitrary port on the local host.
consequence	The outcome of an event or change in circumstances affecting the achievement of objectives.
consumer guide	Product specific advice concerning evaluated products can consist of findings from mutually recognised information security evaluations (such as the Common Criteria), findings from DSD internal evaluations, any recommendations for use and references to relevant policy and standards.

content filtering	The most commonly used method to filter spam. Most antivirus methods are classified as content filters too, since they scan files, binary attachments of email and Hypertext Markup Language payload.
control	The measures to modify risk.
cryptographic hash	An algorithm (the hash function) which takes as input a string of any length (the message), and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest.
cryptographic protocol	An agreed standard for secure communication between two or more entities.
cryptographic system	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
cryptographic system material	Material that includes, but is not limited to, key, equipment, devices, documents and firmware or software that embodies or describes cryptographic logic.
data at rest	Information residing on media or a system that is not powered or is unauthenticated to.
data in transit	Information that is being communicated across a communication medium.
data in use	Information that has been decrypted for processing by a system.
data spill	An information security incident that occurs when information is transferred between two security domains by an unauthorised means. This can include from a security classified network to a less security classified network or between two areas with different need-to-know requirements.
declassification	A process whereby information is reduced to a non-security classified state and an administrative decision is made to formally authorise its release into the public domain.
dedicated mode	All system users have a need-to-know for all of the information processed by the system.
degausser	An electrical device or permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices.
degaussing	A process for reducing the magnetisation of a magnetic storage device to zero by applying a reverse (coercive) magnetic force, rendering any previously stored information as unreadable.
delegate	A person or group of people to whom the authority to authorise variations from requirements in this manual has been devolved by the agency head.
demilitarised zone	A small network with one or more servers that is kept separate from an agency's core network, either on the outside of the agency's firewall, or as a separate network protected by the agency's firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.
device access control software	Software that can be installed on a system to restricted access to communications ports on workstations. Device access control software can either block all access to a communications port or allow access using a whitelisting approach based on device types, manufacturer's identification, or even unique device identifiers.

Diffie-Hellman groups	A method used for specifying the modulus size used in the hashed message authentication code algorithms. Each DH group represents a specific modulus size. For example, group 2 represents a modulus size of 1024 bits.
diode	A device that allows data to flow in only one direction.
domain owner	A domain owner is responsible for the secure configuration of the security domain throughout its life-cycle, including all connections to/from the domain.
dual-stack device	A product that implements both the Internet Protocol version 4 and 6 protocol stacks.
electromagnetic radiation and coupling	All electrical/electronic equipment radiates electromagnetic signals. If the equipment processes information, these radiated signals can contain elements of the information that can be intercepted and analysed by an attacker. Such signals are known as compromising emanations, and can also couple to unprotected equipment, cabling or metalwork and consequently egress the secured space.
emanation security	The counter-measure employed to reduce security classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of RF energy, sound waves or optical signals.
emergency access	The process of a system user accessing a system that they do not hold appropriate security clearances for due to an immediate and critical emergency requirement.
emergency situation	A situation requiring the evacuation of a site. Examples include fires and bomb threats.
Encapsulating Security Payload	A protocol used for encryption and authentication within IPSec.
escort	A person who ensures that when maintenance or repairs are undertaken to hardware that uncleared personnel are not exposed to information.
Evaluation Assurance Level	A level of assurance in the security functionality of a product gained from undertaking a Common Criteria evaluation. Each EAL comprises a number of assurance components, covering aspects of a product's design, development and operation.
event	The occurrence or existence of a particular set of circumstances.
exposure	The susceptibility to gain or loss, usually quantified in terms of potential impact.
facility	An area that facilitates government business. For example, a facility can be building, a floor of a building or a designated space on the floor of a building.
fax machine	A device that allows copies of documents to be sent over a telephone network.
filter	A hardware or software device that controls the flow of data in accordance with a security policy.
firewall	A network protection device that filters incoming and outgoing network data, based on a series of rules.
firmware	Software embedded in a hardware device.
flash memory media	A specific type of EEPROM.
fly lead	A lead that connects equipment to the fixed infrastructure of the facility. For example, the lead that connects a workstation to a network wall socket.
foreign national	A person who is not an Australian citizen.
foreign system	A system that is not solely owned and managed by the Australian Government.

frequency	The number of occurrences of an event or outcome per defined period of time.
gateway/cross domain solution	Gateway/cross domain solutions connect two or more systems from different security domains to allow access to or transfer of information according to defined security polices. A gateway/CDS connection can be automated through a combination of physical or software mechanisms.
general user	A system user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
hardware	A generic term for any physical component of information and communication technology, including peripheral equipment and media used to process information.
hardware products	Hardware products include but are not limited to workstations, printers, photocopiers, scanners and multifunction devices.
hashed message authentication code algorithms	The SHA-1 hashing algorithm, combined with additional cryptographic functions, forms the HMAC algorithms of HMAC-SHA-1-96.
high grade cryptographic equipment	The equivalent to United States Type 1 cryptographic equipment.
high security risk locations	All locations outside Australia and TOP SECRET facilities within Australia.
host-based intrusion prevention system	A security device, resident on a specific host, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.
hybrid hard drives	Non-volatile magnetic media that use a cache to increase read and write speeds and reduce boot time. The cache is normally flash memory media or battery backed RAM.
incident response plan	A plan for responding to information security incidents as defined by the individual agency.
Information Security Incident Reporting scheme	A scheme established by DSD to collect information on information security incidents that affect government systems.
information security policy	A high-level document that describes how an agency protects its systems. The ISP is normally developed to cover all systems and can exist as a single document or as a set of related documents.
Information Security-Registered Assessor Program	A DSD initiative designed to register suitably qualified information security assessors to carry out specific types of information security assessments.
information technology security advisor	The ITSM within an agency that has overall responsibility for information technology security management across the agency.
information technology security manager	ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of ITSOs. The main responsibility of ITSMs is the administrative controls relating to information security within the agency.
information technology security officer	ITSOs are experts in administering and configuring a broad range of agency systems as well as analysing and reporting on information security issues. The main responsibility of ITSOs is the technical controls relating to information security within the agency.
infrared device	Devices such as mice, keyboards, pointing devices, PEDs and laptops that have an infrared communications capability.

Internet Key Exchange Extended Authentication	Internet Key Exchange Extended Authentication is used for providing an additional level of authentication by allowing IPSec gateways to request additional authentication information from remote users. As a result, users are forced to respond with credentials before being allowed access to the connection.
Internet Protocol Security	A suite of protocols for secure Internet Protocol communications through authentication or encryption of Internet Protocol packets as well as including protocols for cryptographic key establishment.
Internet Protocol telephony	The transport of telephone calls over Internet Protocol networks.
Internet Protocol version 6	A protocol used for communicating over a packet switched network. Version 6 is the successor to version 4 which is widely used on the Internet. The main change introduced in version 6 is a greater address space available, 2^{128} vs. 2^{32}, for identifying network devices, workstations and servers.
intrusion detection system	An automated system used to identify an infringement of security policy.
ISAKMP aggressive mode	An IPSec protocol that uses half the exchanges of main mode to establish an IPSec connection.
ISAKMP main mode	An IPSec protocol that offers optimal security using 6 packets to establish an IPSec connection.
ISAKMP quick mode	An IPSec protocol that is used for refreshing security association information.
key management	The use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.
key management plan	A plan that describes how cryptographic services are securely deployed within an agency. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys.
level of risk	The magnitude of a risk measured in terms of the combination of consequences and their likelihood.
likelihood	The chance of something happening.
limited higher access	The process of a system user accessing a system that they do not hold appropriate security clearances for, for a limited non-ongoing period of time.
lockable commercial cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
logging facility	A facility that includes the software component which generates the event and associated details, the transmission (if necessary) of these logs and how they are stored.
malicious code	Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms.
malicious code infection	An information security incident that occurs when malicious code is used to infect a system. Example methods of malicious code infection include viruses, worms and Trojans.
management traffic	Traffic generated by system administrators over a network in order to control a device. This traffic includes standard management protocols, but also includes traffic that contains information relating to the management of the network.

media	A generic term for the components of hardware that are used to store information.
media destruction	The process of physically damaging the media with the objective of making the data stored on it inaccessible. To destroy media effectively, only the actual material in which the data is stored needs to be destroyed.
media disposal	The process of relinquishing control of media when no longer required, in a manner that ensures that no data can be recovered from the media.
media sanitisation	The process of erasing or overwriting data stored on media.
multifunction devices	The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality within the one device. These devices are often designed to connect to computer and telephone networks simultaneously.
multilevel gateway/cross domain solution	A gateway/CDS that enables access, based on authorisation, to data at many security classification and releasability levels where each data unit is individually marked according to its domain.
multilevel mode	Information at two or more security classifications is processed and some of the system users with access are not cleared for some of the information processed by the system.
national security information	Information security classified as RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET.
national security systems	Systems that process, store or communicate information security classified as RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET.
need-to-know	The principle of telling a person only the information that they require to fulfil their role.
Network Access Control	Policies use to control access to a network and actions on a network, including authentication checks and authorisation controls.
network device	Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs.
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.
network protection device	A sub-class of network device used specifically to protect a network. For example, a firewall.
no-lone-zone	An area in which people are not permitted to be left alone such that all actions are witnessed by at least one other person.
non-national security information	Information security classified as X-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.
non-national security systems	Systems that process, store or communicate information security classified as X-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.
non-security classified information	Information produced by the Australian Government that is assessed as not requiring a security classification. Australian Government personnel are required to obtain authorisation prior to releasing such information to members of the public. Non-security classified information has an optional protective marking of UNCLASSIFIED.
non-security classified systems	Systems that process, store or communicate information produced by the Australian Government that does not require a security classification.

non-volatile media	A type of media which retains its information when power is removed.
off-hook audio protection	A method of mitigating the possibility of an active, but temporarily unattended handset inadvertently allowing discussions being undertaken in the vicinity of the handset to be heard by the remote party. This could be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent.
official information	The combination of non-security classified information and security classified information.
Open Internet Protocol network	An IPT network is open if it allows connections to a public analog or data network via an appropriate gateway/CDS.
OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
patch cable	A metallic (copper) or fibre optic cable used for routing signals between two components in an enclosed container or rack.
patch panel	A group of sockets or connectors that allow manual configuration changes, generally by means of connecting cables to the appropriate connector. Cables could be metallic (copper) or fibre optic.
Perfect Forward Security	Additional security for security associations in that if one security association is compromised subsequent security associations will not be compromised.
peripheral switch	A device used to share a set of peripherals between a number of computers.
portable electronic device	Portable devices that can process, store or communicate information electronically. PEDs include, but are not limited to: personal digital assistants, mobile phones and smartphones, two-way email devices, digital cameras, and digital audio players / recorders.
privacy marking	Privacy markings are used to indicate that official information has a special handling requirement or a distribution that is restricted to a particular audience. Privacy markings are integral to the X-IN-CONFIDENCE security classification but can also be used with any other protective markings.
privileged user	A system user who can alter or circumvent system security protections. This can also apply to system users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
protective marking	A marking that is applied to unofficial, non-security classified or security classified information to indicate the security measures, or lack thereof for unofficial information, that needs to be applied to the information to ensure that it is appropriately protected.
public domain information	Official information authorised for unlimited public access or circulation, such as agency publications and websites.
public switched telephone network	A public network where voice is communicated using analog communications.
push-to-talk	Handsets that have a button which must be pressed by the user before audio can be communicated, thus providing fail-safe off-hook audio protection.
quality of service	A process to prioritise network traffic based on availability requirements.

radio frequency device	Devices including mobile phones, wireless enabled PEDs and laptops.
reaccreditation	A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the continued operation of a system.
reclassification	An administrative decision to change the security measures afforded to information based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the security measures for media containing security classified information often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security measures protecting the information.
remote access	Access to a system from a location not within the physical control of the system owner.
removable media	Storage media that can be easily removed from a system and is designed for removal.
residual risk	The risk remaining after risk treatment.
risk	The effect of uncertainty on objectives.
risk acceptance	An informed decision to take a particular risk.
risk analysis	A systematic process to comprehend the nature of risk and to deduce the level of risk.
risk appetite	The amount and type of risk an organisation is prepared to pursue or take.
risk assessment	An overall process of risk identification, risk analysis and risk evaluation.
risk avoidance	The decision not be involved in, or to withdraw from, an activity based on the level of risk involved.
risk criteria	The terms of reference against which the significance of a risk is evaluated.
risk elimination	The reduction of the frequency of an unfavourable event or its severity to zero.
risk estimation	A process used to assign values to consequences, their likelihood and to the level of risk.
risk evaluation	A process of comparing the results of the risk analysis against risk criteria to determine the level of risk and whether it is tolerable or not.
risk identification	A process of finding, recognising and describing risks.
risk management	Coordinated activities to direct and control an organisation with regard to risk.
risk mitigation	Measures taken to reduce the effect of an undesired consequence.
risk owner	A person with the authority and accountability to make a decision to treat, or not to treat, a risk.
risk prevention	Measures taken to reduce the likelihood that an undesired event occurs.
risk reduction	A combination of risk prevention, risk repression or risk mitigation.
risk repression	Measures taken to reduce the likelihood that an undesired event leads to a consequence.
risk source	An object or activity which may cause a risk.
risk treatment	The development and implementation of measures to modify risk.

risk tolerance	An organisations readiness to accept a residual risk after risk treatment in order to achieve the organisations objectives.
rogue wireless access point	A WAP operating outside of the control of an agency.
threat	A potential cause of an event.
seconded foreign national	A representative of a foreign government on exchange or long-term posting to an agency.
secured space	An area that has been certified to physical security requirements as either an Secure Area, Partially Secure Area or Intruder Resistant Area to allow for the processing of security classified information.
Secure Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of Multipurpose Internet Mail Extension-encoded email messages including attachments.
Secure Shell	A network protocol that can be used to securely log into a remote workstation, executing commands on a remote workstation and securely transfer file(s) between workstations.
security association	A collection of connection-specific parameters containing information about a one-way connection within IPSec that is required for each protocol used.
security association lifetimes	The duration security association information is valid for.
security classified information	The combination of national security information and non-national security information.
security classified systems	Systems that process, store or communicate national security information or non-national security information.
Security Construction and Equipment Committee	A standing interdepartmental committee responsible for the evaluation and endorsement of security equipment for use by Australian Government agencies. The SCEC chaired by ASIO and reports to the Protective Security Policy Committee.
security domains	A security domain is a system or collection of systems operating under a security policy that defines the security classification and releasability of the information processed within the domain. It can be exhibited as one security classification (i.e. PROTECTED or RESTRICTED), a community of interest or releasability within a certain security classification.
Security Equipment Catalogue	A catalogue produced by the SCEC that lists equipment that has been tested and endorsed as meeting relevant SCEC standards. Copies of the can be obtained from ASIO.
security executive	A member of the Senior Executive Service who is responsible for overall security within an agency. The appointment of a person to this role is mandated within the PSM.
security risk management plan	A plan that identifies the risks and appropriate risk treatments including controls needed to meet agency policy.
security target	An artefact of Common Criteria evaluations. It contains the information security requirements of an identified target of evaluation and specifies the functional and assurance security measures offered by that target of evaluation to meet the stated requirements.
server	A computer (including mainframes) used to run programs that provide services to multiple users. For example, a file server, email server or database server.
severity	The extent of a loss, harm or damage.

softphone	A software application that allows a workstation to act as an Internet Protocol phone, using either a built-in or an externally connected microphone and speaker. It might also be known as a software Internet Protocol phone.
software component	An element of a system, including but not limited to, a database, operating system, network or Web application.
solid state drives	Non-volatile media that uses flash memory media to retain its information when power is removed and, unlike non-volatile magnetic media, contains no moving parts.
SSH-agent	An automated or script-based Secure Shell session.
standard operating environment	A standardised build of an operating system and associated software that is deployed on multiple devices. A SOE can be used for servers, workstations, laptops and mobile devices.
standard operating procedures	Instructions for complying with a SSP. For example, how to update virus signature files.
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.
system high mode	All system users have a need-to-know for some of the information processed by the system.
system owner	The person responsible for the information resource.
system security classification	The security classification of a system is the highest security classification of information for which the system is approved to store or process.
system security plan	A plan documenting the security controls for a system.
system user	A general user or a privileged user of a system.
target of evaluation	The functions of a product subject to evaluation under the Common Criteria.
technical surveillance counter-measures	The process of surveying facilitates to detect the presence of technical surveillance devices and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility.
telephone	A device that converts between sound waves and electronic signals that can be communicated over a distance.
telephone system	A system designed primarily for the transmission of voice traffic.
TEMPEST	A short name referring to investigations and studies of compromising emanations.
TEMPEST rated equipment	Hardware products that have been specifically designed to minimise TEMPEST emanations.
terminal	Hardware products including monitors, laptops, fax machines and computers.
TOP SECRET areas	Any area certified to operate at TOP SECRET, containing TOP SECRET servers, workstations or associated network infrastructure.
traffic flow filter	A device that has been configured to automatically filter and control the form of network data.
transfer gateway/cross domain solution	A gateway/CDS that facilitates the transfer of information, in one or multiple directions (i.e. low to high or high to low), between different security domains.

transport mode	An Internet Protocol mode that provides a secure connection between two endpoints by encapsulating an Internet Protocol payload.
trusted source	A person or system formally identified as being capable of reliably producing information meeting certain defined parameters, such as a maximum data security classification and reliably reviewing information produced by others to confirm compliance with certain defined parameters.
tunnel mode	An IPSec mode that provides a secure connection between two endpoints by encapsulating an entire Internet Protocol packet.
uncertainty	The state, even partial, of deficiency of information related to a future event, consequence or likelihood.
unsecured space	An area that has not been certified to physical security requirements to allow for the processing of security classified information.
virtual private network	The tunnelling of a network's traffic through another network, separating the VPN traffic from the underlying network. A VPN can encrypt traffic if necessary.
virtual private network split tunnelling	Functionality that allows personnel to access both a public network and a VPN connection at the same time, such as an agency system and the Internet.
volatile media	A type of media, such as RAM, which gradually loses its information when power is removed.
vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats.
wear levelling	A technique used in flash memory that is used to prolong the life of the media. Data can be written to and erased from an address on flash memory a finite number of times. The wear levelling algorithm helps to distribute writes evenly across each memory block, thereby decreasing the wear on the media and increasing its lifetime. The algorithm ensures that updated or new data is written to the first available free block with the least number of writes. This creates free blocks that previously contained data.
whitelist	A set of inclusive accepted items that confirm the item being analysed is acceptable. It is the opposite of a blacklist which confirms that items are not acceptable.
Wi-Fi Protected Access	Certifications of the implementations of protocols designed to replace WEP. They refer to components of the 802.11i security standard.
Wired Equivalent Privacy	A deprecated 802.11 security standard.
wireless access point	A device which enables communications between wireless clients. It is typically also the device which connects the wireless local area network to the wired local area network.
wireless communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium.
wireless local area network	A network based upon the 802.11 set of standards. Such networks are often referred to as wireless networks.
workstation	A stand-alone or networked single-user computer.
X11 Forwarding	X11, also known as the X Window System, is a basic method of video display used in a variety of operating systems. X11 forwarding allows the video display from one network node to be shown on another node.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

INFORMATION SECURITY
DEFENCE SIGNALS DIRECTORATE
www.dsd.gov.au