
Australian Government
Department of Defence
Intelligence and Security
2014
Australian Government
Information Security Manual
CONTROLS

2014

Australian Government Information Security Manual

CONTROLS

Contact us

Inquiries regarding the licence and any use of this document are welcome at:
Australian Signals Directorate
PO Box 5076
Kingston ACT 2604
1300 CYBER1 (1300 292 371)
asd.assist@defence.gov.au

Foreword

In recent years, the Australian Government has made great advances in bringing its business online. The benefits of government information and communications technology (ICT) systems and services becoming increasingly connected will continue as the government makes the most of new technologies. However, this new, connected way of doing business also creates opportunities for adversaries to gain an advantage by exploiting these technologies to access information of national importance.

As our intrusion detection, response, mitigation and threat assessment capabilities continue to improve, so too do the skills of cyber threat actors. This requires us to be vigilant, flexible and proactive in our approach to cyber and information security.

A strong security posture is not a trivial process—it requires ongoing vigilance and resources. By continually hardening our defences, we have a greater chance of protecting the information entrusted to us.

The *Australian Government Information Security Manual* (ISM) comprises three complementary documents designed to provide greater accessibility and understanding at all levels of government. This *Controls* document details the technical security controls which can be implemented to help mitigate security risks to agencies' information and systems.

I commend you on your agency's efforts to strengthen your cyber and information security and trust you'll continue to keep security as an agency priority.

Dr Paul Taloni

Director
Australian Signals Directorate

Contents

ABOUT INFORMATION SECURITY

About Information Security

Using This Manual

Objective

The *Australian Government Information Security Manual* (ISM) is used for the risk–based application of information security to information and systems.

Scope

This section describes how to interpret the content and layout of this manual.

Context

The Australian Signals Directorate

Under the *Defence White Paper 2013*, the Defence Signals Directorate (DSD) was renamed the Australian Signals Directorate (ASD). For legal and policy purposes, all references to ASD should be taken to be references to DSD.

Purpose of the Australian Government Information Security Manual

The purpose of this manual is to assist Australian government agencies in applying a risk–based approach to protecting their information and systems. While there are other standards and guidelines designed to protect information and systems, the advice in this manual is specifically based on ASD's experience in providing cyber and information security advice and assistance to the Australian government. The controls are therefore designed to mitigate the most likely threats to Australian government agencies.

Applicability

This manual applies to:

- Australian government agencies that are subject to the *Financial Management and Accountability Act 1997*, or post July 2014 the *Public Governance, Performance and Accountability Act 2013*
- bodies that are subject to the *Commonwealth Authorities and Companies Act 1997*, or post July 2014 the *Public Governance, Performance and Accountability Act*, and that have received notice in accordance with that Act that the ISM applies to them as a general policy of the 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 their Portfolio Minister that the ISM applies to them
- state and territory agencies that implement the *Australian Government Protective Security Policy Framework*
- organisations that have entered a Deed of Agreement with the Government to have access to sensitive or classified information.

ASD encourages Australian government agencies, whether Commonwealth, state or territory, which do not fall within this list to apply the considered advice contained within this manual when selecting security controls on a case–by–case basis.

Authority

The *Intelligence Services Act 2001* (the ISA) states that two functions of ASD, also known as 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
- to provide assistance to Commonwealth and state authorities in relation to cryptography, and communication and computer technologies.

This manual represents the considered advice of ASD provided in accordance with its designated functions under the ISA. Therefore agencies are not required as a matter of law to comply with this manual, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply with it.

Legislation and legal considerations

This manual does not override any obligations imposed by legislation or law. Furthermore, if this manual conflicts with legislation or law the latter takes precedence.

While this manual contains examples of when legislation or 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.

Public systems

Agencies deploying public systems can determine their own security measures based on their business needs, risk appetite and security risks to their systems. However, ASD encourages such agencies to use this manual, particularly the objectives, as a guide when determining security measures for their systems.

Public network infrastructure

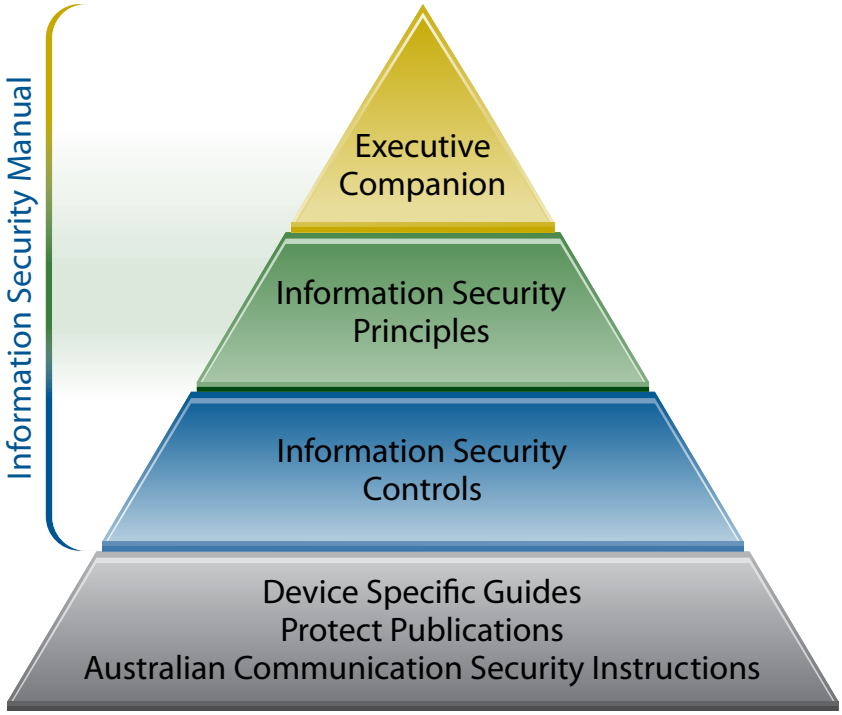
This manual uses the term 'public network infrastructure', defined as network infrastructure that an agency has no or limited control over (for example the Internet). Conversely, private network infrastructure is that which an agency controls exclusively.

However, there may be cases where a network does not precisely meet either of these definitions, a common example being the Intra Government Communications Network (ICON). Where a network's infrastructure and devices are not wholly controlled by your agency, it should be treated as if it is public network infrastructure in the context of relevant ISM controls.

Further information on ICON can be found at http://www.finance.gov.au/collaboration-services-skills/icon/.

Format of the Australian Government Information Security Manual

The three parts of the ISM are designed to complement each other and provide agencies with the necessary information to conduct informed risk–based decisions according to their own business requirements, specific circumstances and risk appetite.



The **Executive Companion** is aimed at the most senior executives in each agency, such as Secretaries, Chief Executive Officers and Deputy Secretaries, and comprises broader strategic messages about key cyber and information security issues.

The **Principles** document is aimed at Security Executives, Chief Information Security Officers, Chief Information Officers and other senior decision makers across government and focuses on providing them with a better understanding of the cyber threat environment. This document contains information to assist them in developing informed security policies within their agencies.

The **Controls** manual is aimed at Information Technology Security Advisors, Information Technology Security Managers, Information Security Registered Assessors and other security practitioners across government. This manual provides a set of detailed controls which, when implemented, will help agencies adhere to the higher level Principles document.

ASD provides further information security advice in the form of device–specific guides, Australian Communications Security Instructions (ACSIs) and Protect publications—such as the *Strategies to Mitigate Targeted Cyber Intrusions*. While these publications reflect the policy specified in this manual, not all requirements in this manual can be implemented on all devices or in all environments. In these cases, device–specific advice issued by ASD may take precedence over the controls in this manual.

Framework

This manual uses a framework to present information in a consistent manner. The framework consists of a number of headings in each section:

- **Objective—**the desired outcome of complying with the controls specified in the section, expressed as if the outcome has already been achieved
- **Scope and Context**—the scope and applicability of the section. It can also include definitions, legislative context, related ISM sections and background information
- **Controls—**procedures with associated compliance requirements for mitigating security risks to an agency's information and systems
- **References**—sources of information that can assist in interpreting or implementing controls.

System applicability

Each control in this manual has an applicability indicator that indicates the information and systems to which the control applies. The applicability indicator has up to five elements, indicating whether the control applies to:

- G: Baseline controls advised for Australian government systems holding information which requires some level of protection. Applicable to government systems containing unclassified but sensitive or official information not intended for public release, such as Dissemination Limiting Marker information (i.e. Unclassified (DLM) systems). Unclassified (DLM) and 'Government' are not classifications under the *Australian Government Security Classification System*, as mandated by the Attorney–General's Department
- P: PROTECTED information and systems
- C: CONFIDENTIAL information and systems
- S: SECRET information and systems
- TS: TOP SECRET information and systems.

ASD maintains a System Controls Checklist to facilitate the incorporation of ISM advice into agencies' risk assessments.

References

Nil.

Information Security Risk Management

Objective

Agencies select and implement information security controls from the ISM as part of a formal risk management process.

Scope

This section describes the expectations on Australian government agencies to include the controls contained in this manual in their wider agency risk management process.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Context

Taking a risk–based approach to Information Security

The ISM represents best practice in mitigating or minimising the threat to Australian government information and systems. However, due to the differences between government agencies, there is no one–size–fits–all model for information security. The ISM aims to encourage agencies to take a risk–based approach to information security. This approach enables the flexibility to allow agencies to conduct their business and develop resilience in the face of a changing threat environment.

It is a mandatory requirement of the *Australian Government Protective Security Policy Framework* that agencies adopt a risk management approach to cover all areas of protective security activity across their organisation. ASD recommends information security forms a part of an agency's broader risk management processes.

The ISM is developed as a tool to assist Australian government agencies to risk–manage the protection of their information and systems. It may not be possible or appropriate for an agency to implement all controls included in this manual. Agencies will have different security requirements, business needs and risk appetites from one another. The ISM aims to assist agencies in understanding the potential consequences of non–compliance—and whether such non–compliance presents an acceptable level of risk—as well as selecting appropriate risk mitigation strategies.

Applicability of controls

While this manual provides controls for various technologies, not all systems will use all of the technologies mentioned. When agencies develop systems they will need to determine the appropriate scope of the systems and which controls in this manual are applicable.

Not all ISM requirements can be implemented on all devices or in all environments. In these cases, device–specific advice issued by ASD may take precedence over the controls in this manual.

This section should be read in conjunction with the *Security Risk Management Plans* section of the *Information Security Documentation* chapter. Further information on vulnerability assessments and managing change can be found in the *Information Security Monitoring* chapter.

Controls

Identifying and analysing information security risks

Risk can be identified and analysed in terms of:

- What could happen? How could resources and activities central to the operation of an agency be affected?
- How would it happen? What weaknesses could be exploited to make this happen? What security controls are already in place? Are they adequate?
- How likely is it to happen? Is there opportunity and intent? How frequent is it likely to be?
- What would the consequence be? What possible effect could it have on an agency's operations, services or credibility?

Control: 1203; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must identify and analyse security risks to their information and systems.

Evaluating and treating information security risks

Once information security risks have been identified and analysed, agencies will need to determine whether they are acceptable or not. This decision can be made by balancing the risk against an agency's business needs and risk appetite, for example:

- What equipment and functionality is necessary for your agency to operate?
- Will the risk mitigation strategies affect your agency's ability to perform its core duties?
- What resource constraints are involved? (This can refer to financial or personnel limitations, for example.)
- Will the compromise of information, as a result of not treating this risk, breach your agency's obligation under law or damage national security in some way?

Treating a risk means that the consequences and/or likelihood of that risk is reduced. The controls included in this manual provide strategies to achieve this in different circumstances (in generic, agency and device non–specific terms).

Control: 1204; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Security risks deemed unacceptable must be treated.

Control: 1205; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must incorporate the controls contained in the *Australian Government Information Security Manual* in their security risk management processes.

Because an agency's risk owner—the agency head or their formal delegate—is accountable for an information or cyber security incident, they need to be made aware of any residual security risks to their information and systems through a formal approval process. Agency risk profiles will change over time as the threat environment, technology and agency business needs evolve, so it is important that any residual security risks are monitored.

Control: 1206; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Security risks deemed acceptable must be formally accepted by the responsible authority, as indicated for each control in this manual, and continually monitored by the agency.

Control: 1207; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should mitigate residual security risks through the implementation of alternative security measures.

System–specific security risks

While a baseline of controls is provided in this manual, agencies may have differing circumstances to those considered during the development of this manual. In such cases an agency needs to follow its own security risk management processes to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds.

Control: 0009; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should determine system specific security risks that could warrant additional controls to those specified in this manual.

Documentation

Documenting information security risk management activities can help an agency ensure security risks are managed in a coordinated and consistent manner. Documentation also provides a standard against which compliance can be measured.

Control: 1208; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document identified information security risks, as well as the evaluation of those risks and mitigation strategies, in their Security Risk Management Plan.

References

The *Australian Government Protective Security Policy Framework* can be found at http://www.protectivesecurity.gov.au.

For further guidance please refer to the *Australian Standard for Risk Management* AS/NZS ISO 31000:2009, the Australian Standards HB 167:2006 *Security risk management* and HB 327:2010 *Communicating and consulting about risk*.

The Protective Security Training College, managed by the Attorney–General's Department, provides formal training opportunities on the subject of security risk management: http://www.ag.gov.au/NationalSecurity/ProtectiveSecurityTraining/Pages/default.aspx.

Compliance and Non–compliance

Objective

Agencies comply with ISM controls where appropriate, in accordance with their business needs, threat environment and risk appetite. Non–compliance is formally accepted by the appropriate authority.

Scope

This section explains the compliance language used in this manual and the appropriate authorities for non–compliance with ISM controls.

Context

Authority to approve non–compliance

Each control specifies the authority that must provide approval for non–compliance with the control. The authority indicates one of the two possible approvers:

- ASD: Director ASD
- AA: Accreditation Authority

In most circumstances, the accreditation authority is the agency head or their formal delegate. For information on accreditation authorities, see the *Conducting Accreditations* section of the *System Accreditation* chapter.

Some controls will also require non–compliance notification to the relevant portfolio minister(s), the Attorney–General and the Auditor General as detailed in the *Australian Government Protective Security Policy Framework* (PSPF). These can be found in the *PSPF Mandatory Requirement INFOSEC 4 Explained* chapter.

Compliance language

There are two categories of compliance associated with the controls in this manual—'must' and 'should'. These compliance requirements are determined according to the degree of security risk an agency will be accepting by not implementing the associated control. ASD's assessment of whether a control is a 'must' or a 'should' is based on ASD's experience in providing cyber and information security advice and assistance to the Australian government and reflect what ASD assesses the risk level to be. Agencies may have differing risk environments and requirements, and may have other mitigations in place to reduce the residual risk to an acceptable level.

Non–compliance with multiple controls

When an agency is non–compliant with multiple controls, they may choose to logically group the areas of non–compliance when following the processes for non–compliance.

Compliance by smaller agencies

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

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

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 to formalise their security responsibilities.

Auditing of compliance by the Australian National Audit Office

All controls in this manual may be audited for compliance by the Australian National Audit Office (ANAO).

Controls

Complying with the Australian Government Information Security Manual

By using the latest release of this manual for system design activities, agencies will be taking steps to protect themselves from the current threats to Australian government systems.

Control: 0007; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies undertaking system design activities for in–house or out–sourced projects must use the latest release of this manual for security requirements.

ASD produces information security policies and guidance in addition to this manual, such as the ACSI suite, consumer guides, hardening guides and Protect publications. These may address device and scenario–specific security risks to information and systems, and accordingly may take precedence over the controls in this manual. Distinct time frames for compliance may also be specified.

Control: 0008; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with additional or alternative controls as stipulated in device and scenario–specific guidance issued by ASD.

Granting non–compliance

Non–compliance with 'must' and 'must not' controls are likely to represent a high security risk to information and systems. Non–compliance with 'should' and 'should not' controls are likely to represent a medium–to–low security risk to information and systems. The accreditation authority (the agency head or their formal delegate in most circumstances) is able to consider the justification for non–compliance and accept any associated residual security risk.

Non–compliance with controls where the authority is marked 'ASD' must be granted by the Director ASD.

Control: 0001; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
For any control where the authority field is 'ASD', system owners must seek and be granted approval for non–compliance from the Director ASD in consultation with their accreditation authority.

Control: 1061; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
System owners seeking approval for non–compliance with any control in this manual must be granted non–compliance from their accreditation authority.

If the agency head and accreditation authority form separate roles in an agency, the accreditation authority will need to ensure the agency head has appropriate oversight of the security risks being accepted on behalf of the agency. This helps to meet the PSPF's Protective Security Principles, which stipulate that agency heads need to understand, prioritise and manage security risks to prevent harm to official resources and disruption to business objectives. The authority for this control is listed as N/A as non–compliance approval cannot be sought under the ISM framework.

Control: 1379; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: N/A
In circumstances where the agency head and accreditation authority roles are separate, the accreditation authority must ensure the agency head has appropriate oversight of the security risks being accepted on behalf of the agency.

Justification for non–compliance

Without sufficient justification, and consideration of the security risks, the agency head or their authorised delegate will lack the appropriate information to make an informed decision on whether to accept the residual security risk and grant non–compliance to the system owner.

Control: 0710; Revision: 3; Updated: Sep–12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
System owners seeking approval for non–compliance with any control must document:

- the justification for non–compliance
- a security risk assessment
- the alternative mitigation measures to be implemented, if any.

Consultation on non–compliance

When an agency processes, stores or communicates information on their systems that belongs to another agency or foreign government they have an obligation to inform that third party when they desire to risk manage the controls specified in this manual. If the agency fails to do so, the third party will be unaware that their information has been placed at a heightened risk of compromise. The third party is thus denied the opportunity to consider additional security measures for their information.

The extent of consultation with other agencies and foreign governments may include:

- a notification of the intent to be non–compliant
- the justification for non–compliance
- any mitigation measures that may have been implemented
- an assessment of the security risks relating to the information they have been entrusted with.

Control: 0711; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If a system processes, stores or communicates information from another agency, that agency should be consulted as part of granting non–compliance with any control.

Notification of non–compliance

The purpose of notifying authorities of any decisions to grant non–compliance with controls is three–fold:

- to ensure that an accurate picture of the state of information security across government can be maintained
- to help inform incident response
- to use as feedback for the ongoing refinement of this manual.

Control: 0713; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should provide a copy of their non–compliance reports to ASD.

Reviewing non–compliance

When seeking approval for non–compliance, the system owner must provide a justification for non–compliance, outline any alternative mitigation measures to be implemented and conduct an assessment of the security risks. As the justification for non–compliance may change, and the risk environment will continue to evolve over time, it is important that the system owner update their approval for non–compliance at least every two years. This allows for the appropriate authority to have any decision to grant non–compliance either reaffirmed or, if necessary, rejected if the justification or residual security risk is no longer acceptable.

Control: 0876; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must review decisions to grant non–compliance with any control, including the justification, any mitigation measures and security risks, at least every two years or when significant changes occur to ensure its continuing relevance, adequacy and effectiveness.

Recording non–compliance

Without appropriate records of decisions to grant non–compliance with controls, agencies have no record of the status of their security posture. Furthermore, a lack of such records will hinder any auditing activities that may be conducted by the agency or by external parties such as the Australian National Audit Office (ANAO). Failing to maintain such records is also a breach of the *Archives Act 1983* (the Archives Act).

Control: 0003; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must retain a copy of decisions to grant non–compliance with any control from this manual.

References

ASD contact details can be found at http://www.asd.gov.au/contact.htm.

INFORMATION SECURITY GOVERNANCE

Information Security Governance

Information Security Engagement

Government Engagement

Objective

Security personnel are aware of and use security services offered in the Australian Government.

Scope

This section describes the agencies and bodies involved in providing information security advice.

Context

ASD

ASD is required under the *Intelligence Services Act 2001* (the ISA) 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.

ASD provides assistance to Commonwealth and State authorities in relation to cryptography, communications and computer technologies.

ASD works with industry to develop new cryptographic products. It has established the Australian Information Security Evaluation Program (AISEP) to deal with the increasing requirement to evaluate products with security functionality.

ASD can be contacted for advice and assistance on implementing this manual through agency Information Technology Security Managers (ITSMs) or Information Technology Security Advisors (ITSAs). ITSMs and ITSAs can send questions to ASD by email at asd.assist@defence.gov.au or phone on 1300 CYBER1 (1300 292 371).

ASD can be contacted for advice and assistance on cyber security incidents. ASD's response will be commensurate with the urgency of the cyber security incident. Urgent and operational enquiries can be submitted through ASD's OnSecure website or by phoning 1300 CYBER1 (1300 292 371) and selecting 1 at any time. Non–urgent and general enquiries can be submitted through the OnSecure website, by phoning 1300 CYBER1 (1300 292 371) and selecting 2 at any time or emailing the Cyber Security Operations Centre at asd.assist@defence.gov.au. ASD's incident response service is available 24 hours, 7 days a week.

ASD can be contacted by email at asd.assist@defence.gov.au for advice and assistance on the purchasing, provision, deployment, operation, disposal and COMSEC incidents relating to High Assurance products.

Other government agencies and bodies

The following table contains a brief description of the other government agencies and bodies that have a role in information security in government.

AGENCY OR BODY	SERVICES
Attorney–General's Department (AGD)	Responsible for information security policy and cyber security incident preparedness, response and recovery arrangements across government.
Attorney–General's Department—Protective Security Training College	Provides protective security training to government agencies and contractors.
Australian Federal Police (Australian High Tech Crime Centre)	Law enforcement in relation to electronic and other high tech crimes.
Australian Government Information Management Office (AGIMO)	Development, coordination and oversight of whole–of–government policy on electronic commerce, online services and the Internet.
Australian National Audit Office (ANAO)	Performance audits on information security.
Australian Security Intelligence Organisation (ASIO)—T4 Protective Security	ASIO is responsible for collecting, analysing and reporting intelligence on threats to security. ASIO—T4 Protective Security section provides advice and training, technical surveillance counter–measures, physical security certifications, protective security risk reviews and physical security equipment testing.
Computer Emergency Response Team (CERT) Australia	Provides the private sector with information and assistance to help them protect their Information and Communications Technology (ICT) infrastructure from cyber threats and vulnerabilities; coordination role during a serious cyber incident.
Cyber Security Operations Centre (CSOC)	The CSOC is responsible for improving government understanding of sophisticated cyber threats against Australian interests, and coordinating/providing operational responses to cyber security events of national importance. It is hosted by ASD but includes representatives from ASD, the Defence Intelligence Organisation (DIO), Australian Defence Force, ASIO, AFP and AGD.
Cyber Security Policy and Coordination Committee	Coordinates the development of cyber security policy for the Australian Government.

AGENCY OR BODY	SERVICES
Department of Communications	Responsible for initiatives to educate and protect home users, students and small business from electronic intrusions and fraud.
Department of Foreign Affairs and Trade	Policy and advice for security overseas.
Department of the Prime Minister and Cabinet	Coordination of cyber and information security policy and activities across government. Responsible for implementation of the National Security Information Environment Roadmap: 2020 Vision.
National Archives of Australia	Provides standards and advice on capturing and managing records to ensure their integrity as evidence is maintained; authorises the disposal of all Commonwealth records, including those relating to ICT and security processes and incidents.
Protective Security Policy Committee	Coordinates the development of protective security policy. Chairmanship and Secretariat support provided by the Attorney–General's Department.
Cyber Security Operations Board	Provides strategic direction and oversight of operational cyber security matters. Chairmanship and Secretariat support provided by the Attorney General's Department.
Security Construction and Equipment Committee	Oversees the evaluation of security equipment.

Controls

Organisations providing information security services

If security personnel are unaware of the roles government organisations play in the information security space, they could miss out on valuable insight and assistance in developing effective security measures.

Control: 0879; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Security personnel should familiarise themselves with the information security roles and services provided by Australian Government agencies and bodies.

References

The following websites can be used to obtain additional information about agencies and bodies involved in the security of government information and systems:

http://www.asd.gov.au/

http://www.protectivesecurity.gov.au/

http://www.ag.gov.au/cybersecurity

http://www.ag.gov.au/identitysecurity

http://www.ag.gov.au/NationalSecurity/ProtectiveSecurityTraining/Pages/default.aspx.

http://www.asd.gov.au/infosec/aisep.htm

http://www.afp.gov.au/

http://www.finance.gov.au/agimo/

http://www.anao.gov.au/

http://www.asio.gov.au/

http://www.cert.gov.au/

http://www.dfat.gov.au/

http://www.communications.gov.au/

http://www.pmc.gov.au/

http://www.naa.gov.au/records-management/

http://www.scec.gov.au/.

Industry Engagement and Outsourcing

Objective

Industry partners handle information appropriately and implement the same security measures as their sponsoring agency.

Scope

This section describes information on outsourcing information technology services and functions to industry as well as providing them with access to information in order to undertake their duties.

Context

Outsourced cloud computing

Cloud computing is a delivery model for information technology services. Where these services are provided by a third party (i.e. outsourced) cloud computing service provider, additional information security issues need to be considered. ASD's *Cloud Computing Security Considerations* document provides guidance for agencies considering using cloud computing services.

Additionally, the Attorney–General's Department's Australian Government *Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements* establishes whole–of–government guidelines for outsourcing agency ICT functions and offshoring unclassified government information.

For further information on the use of virtualisation technologies to achieve functional separation, see the *Standard Operating Environments* section of the *Software Security* chapter.

A public cloud arrangement involves infrastructure which is shared via the Internet with many other organisations and other members of the public.

Controls

Risks of outsourcing ICT services

Outsourcing can be a cost–effective option for providing information technology services and functions in an agency, as well as potentially delivering a superior service. However, it can also affect an agency's risk profile and control over its threat environment. Storing data in multiple disparate locations and allowing more people to access agency information can significantly increase the potential for network infection and information loss or compromise.

Outsourcing information technology services and functions outside of Australia, unless agencies are handling data considered publicly available, presents a high risk of unauthorised disclosure of agency information. Choosing a vendor (either locally or foreign owned) that is located in Australia and stores, processes and manages sensitive data only within Australian borders reduces this risk. An additional risk is that foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor.

The Attorney–General's Department's Australian Government *Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements* establishes a whole–of–government approach to how different categories of information are treated when considering offshore or outsourced ICT arrangements.

Control: 1376; Revision: 0; Updated: Feb-14; Applicability: G; Compliance: must not; Authority: AA
Unclassified information that is not considered publicly releasable must not be stored or processed in public cloud or offshore ICT arrangements unless it meets the requirements outlined in the Attorney–General's Department's Australian Government *Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements*.

Control: 1377; Revision: 0; Updated: Feb-14; Applicability: G; Compliance: must not; Authority: AA
Personal information as defined by the *Privacy Act 1988* must not be stored or processed in public cloud or offshore ICT arrangements unless it meets the requirements outlined in the Attorney–General's Department's Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements.

Control: 0873; Revision: 2; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Service providers' systems storing or processing Australian government information must be located in Australia.

Control: 1378; Revision: 0; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Security classified information must not be stored or processed in a public cloud arrangement, unless the handling requirements have been appropriately downgraded as per the *Cryptography* and other related chapters of the ISM.

When agency functions and services are outsourced, agencies can lose oversight of how their information is handled and stored. Ensuring service providers seek agency approval before transmitting, processing or storing information offshore will minimise the risk of agencies losing control of their information.

Control: 1073; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure service providers seek their approval before allowing information to leave or be accessed from outside Australian borders.

Accrediting service providers' systems

Service providers can be provided with information as long as their systems are accredited to process, store and communicate the information. This ensures that when they are provided with information that it receives an appropriate level of protection.

The principles and objectives set out in the ISM apply equally to agencies using cloud computing services. In some circumstances, agencies might need to seek non–compliance for controls that aren't applicable to a specific cloud computing implementation or usage scenario. The accreditation process should involve communication from the provider to the client agency on areas of non–compliance to inform their risk decision. This is no different to the expectations leveraged on government agencies when using this manual. If a service provider is changing its system architecture to meet ISM controls for certification purposes, which is in turn weakening security in other parts of the implementation scenario, then it is likely not meeting the intent of the ISM. In such circumstances, ASD should be contacted for ISM interpretation advice.

Further information on expected agency due diligence when connecting to a system not under their control or passing information to another party can be found in the *Accreditation Framework* section of the *System Accreditation* chapter.

Control: 0872; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Systems used by service providers for the provision of information technology services and functions must be accredited to the same minimum standard as the sponsoring agency's systems.

Cloud Computing

There are a variety of information security risks that need to be considered when engaging cloud computing providers. Data stored in outsourced cloud infrastructure is vulnerable to malicious cyber activity, due to the Internet–connected nature of outsourced cloud computing. Moreover, the physical data storage location—and the people responsible—will not necessarily be known to the agency. This diminishes agency control over threat mitigation and response and increases the threat from malicious insiders. Risks will vary depending on the sensitivity of agency data to be stored and processed and how the chosen cloud vendor has implemented their specific cloud services.

Control: 1210; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should assess the information security risks of using cloud computing services against ASD's *Cloud Computing Security Considerations* document.

Service providers' ITSM

When an agency engages a service provider for the provision of information technology services and functions, having a central point of contact for information security issues will greatly assist incident response and reporting procedures.

Control: 0744; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Service providers should provide a single point of contact who will act as an equivalent to an ITSM.

Developing an industry engagement plan

Developing an information security industry engagement plan will help ensure an agency has a clear and coordinated approach when engaging and using service providers for the outsourcing and provision of information technology services and functions.

Control: 1052; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop an information security industry engagement plan to manage service providers that have been approved for the provision of information technology services and functions.

References

Additional information regarding cloud computing security considerations can be found in the *Cloud Computing Security Considerations* document on the ASD website at http://www.asd.gov.au/infosec/cloudsecurity.htm.

Additional information on outsourcing and offshoring ICT services can be found in the Attorney–General's Department's *Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements.*

Additional whole–of–government policy and guidance on cloud computing can be found on the Australian Government Information Management Office website at http://www.finance.gov.au/cloud/.

Additional information on government expectation when outsourcing services and functions can be found in the Attorney–General's Department's *Protective Security Governance Guidelines—Security of Outsourced Services and Functions*.

Roles and Responsibilities

The Chief Information Security Officer

Objective

The Chief Information Security Officer (CISO) sets the strategic direction for information security for their agency.

Scope

This section describes the information security role of a CISO.

Context

The Security Executive and their CISO role

The requirement to appoint a member of the Senior Executive Service, or in an equivalent management position, to the role of CISO does not require a new dedicated position to be created in each agency. This role is intended to be performed by the Security Executive, which is a position in each agency mandated by the *Australian Government Protective Security Policy Framework*. The introduction of the CISO role is aimed at providing a more meaningful title for a subset of the Security Executive's responsibilities that relate to information security.

Controls

Requirement for a CISO

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. The CISO is typically responsible for:

- facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives
- providing strategic–level guidance for the agency security program
- ensuring compliance with national policy, standards, regulations and legislation.

Control: 0714; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

Agencies must appoint a senior executive, commonly referred to as the CISO, who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and security risk management processes.

References

Nil.

The Information Technology Security Advisor

Objective

The Information Technology Security Adivisor (ITSA) coordinates information technology security for their agency.

Scope

This section describes the information security role of an ITSM when designated as the ITSA.

Context

The ITSA

The ITSM who has 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, or equivalent, and external agencies on any information technology security management issues.

Information on the responsibilities of ITSMs can be found in the *Information Technology Security Managers* section of this chapter.

Controls

Requirement for an ITSA

An ITSM, when fulfilling the designation of ITSA, still maintains full responsibilities for their role as an ITSM in addition to ITSA responsibilities. An ITSA traditionally has the added responsibility of coordinating other ITSMs to ensure that security measures and efforts are undertaken in a coordinated manner.

Control: 0013; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must designate an ITSM as the ITSA, to have responsibility for information technology security management across the agency.

Contacting ITSAs

As security personnel in agencies need to communicate with security personnel from other agencies, often to provide warnings of threats to their systems, it is important that a consistent contact method is available across government to facilitate such communication.

Control: 0025; Revision: 3; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should maintain an email address for their ITSA in the form of ITSA@agency.

References

Nil.

Information Technology Security Managers

Objective

Information Technology Security Managers (ITSMs) provide information security leadership and management for their agency.

Scope

This section describes the information security role of ITSMs.

Context

ITSMs

ITSMs are executives that coordinate the strategic directions provided by the CISO and the technical efforts of Information Technology Security Officers (ITSOs). The main area of responsibility of an ITSM is that of the day–to–day management of information security within an agency.

Controls

Requirement for ITSMs

ITSMs are generally considered information security experts and are typically responsible for:

- managing the implementation of security measures
- monitoring information security for systems and responding to any cyber security incidents
- identifying and incorporating appropriate security measures in the development of ICT projects and the information security program
- establishing contracts and service–level agreements on behalf of the CISO, or equivalent
- assisting the CISO or equivalent to develop security budget projections and resource allocations
- providing regular reports on cyber security incidents and other areas of particular concern
- helping system owners to understand and respond to reported audit failures
- guiding the selection of appropriate strategies to achieve the direction set by the CISO or equivalent with respect to disaster recovery policies and standards
- delivering information security awareness and training programs to personnel.

Control: 0741; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

Agencies must appoint at least one executive, commonly referred to as an ITSM, to manage the day–to–day operations of information security within the agency, in line with the strategic directions provided by the CISO or equivalent.

References

Further information on the role of ITSAs is available in the Attorney–General's Department's *Protective Security Governance Guidelines*, available at http://www.protectivesecurity.gov.au.

Information Technology Security Officers

Objective

ITSOs provide information security operational support for their agency.

Scope

This section describes information security role of ITSOs.

Context

ITSOs

ITSOs implement technical solutions under the guidance of an ITSM to ensure that the strategic direction for information security within the agency is achieved.

Appointing ITSOs

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 security aspects of their role.

Controls

Requirement for ITSOs

Appointing a person whose responsibility is to ensure the technical security of systems is essential to manage compliance and non–compliance with the controls in this manual. The main responsibility of ITSOs is the implementation and monitoring of technical security measures for systems. Other responsibilities often include:

- conducting vulnerability assessments and taking actions to mitigate threats and remediate vulnerabilities
- working with ITSMs to respond to cyber security incidents
- assisting ITSMs with technical remediation activities required as a result of audits
- assisting in the selection of security measures to achieve the strategies selected by ITSMs with respect to disaster recovery
- raising awareness of information security issues with system owners and personnel.

Control: 0768; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

Agencies must appoint at least one expert, commonly referred to as an ITSO, in administering and configuring a broad range of systems as well as analysing and reporting on information security issues.

References

Nil.

System Owners

Objective

System owners obtain and maintain accreditation of their systems.

Scope

This section describes the information security role of system owners.

Context

The system owner is the person responsible for an information resource.

Controls

Requirement for system owners

While the system owner is responsible for the operation of the system, they will delegate the day–to–day management and operation of the system to a system manager or managers.

While it is strongly recommended that a system owner is a member of the Senior Executive Service, or in an equivalent management position, it does not imply that the system managers should also be at such a level.

Control: 1071; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Each system must have a system owner who is responsible for the operation of the system.

Control: 1072; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
System owners should be a member of the Senior Executive Service or in an equivalent management position.

Accreditation responsibilities

The system owner is responsible for the secure operation of their system and needs to ensure it is accredited. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken and documented in an appropriate manner, and that any necessary reaccreditation activities are completed.

Control: 0027; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
System owners must obtain and maintain accreditation for their systems.

References

Nil.

Information Security Documentation

Documentation Fundamentals

Objective

Information security documentation is produced for systems to support the accurate and consistent application of policy and procedures within an agency.

Scope

This section describes the information security documentation that government agencies should develop.

Context

The suite of documents outlined in this chapter forms the Information Security Management Framework, as mandated in the *Australian Government Information Security Management Protocol.*

Documentation is vital to any information security regime as it supports the accurate and consistent application of policy and procedures within an agency. Documentation also provides increased accountability and a standard against which compliance can be measured.

More detailed information about each document can be found in the relevant sections of this chapter.

Controls

Information Security Policy

The Information Security Policy (ISP) is a statement of high–level information security policies and is therefore an essential part of information security documentation.

Control: 0039; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have an ISP.

Security Risk Management Plan

The Security Risk Management Plan (SRMP) is 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.

Control: 0040; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that every system is covered by an SRMP.

System Security Plan

The System Security Plan (SSP) is derived from this manual and the SRMP and describes the implementation and operation of controls for a system. Depending on the documentation framework chosen, some details common to multiple systems could be consolidated in a higher level SSP.

Control: 0041; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that every system is covered by an SSP.

Standard Operating Procedures

Standard Operating Procedures (SOPs) provide a step–by–step guide to undertaking security related tasks. They provide assurance that tasks can be undertaken in a repeatable manner, even by users without strong knowledge of the system. Depending on the documentation framework chosen, some procedures common to multiple systems could be consolidated into a higher level SOP.

Control: 0042; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that SOPs are developed for systems.

Incident Response Plan

Having an Incident Response Plan (IRP) ensures that when a cyber security incident occurs, a plan is in place to respond appropriately to the situation. In most situations, the aim of the response will be to preserve any evidence relating to the cyber security incident and to prevent the incident escalating.

Control: 0043; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, maintain and implement an IRP and supporting procedures.

Developing content

It is likely that the most useful and accurate information security documentation will be developed by personnel who are knowledgeable about both information security issues and the business requirements.

Control: 0886; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that information security documentation is developed by personnel with a good understanding of both the subject matter and the business requirements.

Documentation content

As the SRMP, SSP, SOPs and IRP form a documentation suite for a system, it is essential that they are logically connected and consistent. Furthermore, each documentation suite developed for a system will need to be consistent with the ISP.

Control: 0044; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that their SRMP, SSP, SOPs and IRP are logically connected and consistent for each system and with the ISP.

Using a documentation framework

Having a documentation framework for information security documents ensures that they are accounted for and maintained appropriately. Furthermore, the framework can be used to describe relationships between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

Control: 0787; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should create and maintain a document framework including a hierarchical listing of all information security documentation and their relationships.

Control: 0885; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should adopt the naming conventions provided in this manual for their information security documentation.

Outsourcing development of content

Agencies outsourcing the development of information security documentation still need to review and control the contents to make sure it meets their requirements.

Control: 0046; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
When information security documentation development is outsourced, agencies should:

- review the documents for suitability
- retain control over the content
- ensure that all policy requirements are met.

Obtaining formal approval

If information security policy does not have formal approval, security personnel will have difficulty ensuring appropriate systems security procedures are in place. Having formal approval not only assists in the implementation of procedures, it also ensures senior managers are aware of information security issues and security risks.

Control: 0047; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
All information security documentation should be formally approved by a person with an appropriate level of seniority and authority.

Control: 0887; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that:

- all high–level information security documentation is approved by the agency head or their delegate
- all system–specific documentation is approved by the system owner and an ITSM.

Publication of documentation

If stakeholders are not made aware of new information security documentation, or changes to existing information security documentation, they will not know about any changes they may need to make to the security measures for their systems.

Control: 1153; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Once information security documentation has been approved it should be published and communicated to all stakeholders.

Documentation maintenance

The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation current to reflect the changing environment, their security measures and processes may cease to be effective. In that situation, resources could be devoted to areas that have reduced effectiveness, or are no longer relevant.

Control: 0888; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should review information security documentation:

- at least annually
- in response to significant changes in the environment, business or system.

Control: 1154; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should record the date of the most recent review on each information security document.

References

Nil.

Information Security Policy

Objective

The ISP sets the strategic direction for information security for an agency.

Scope

This section describes the development of an ISP.

Context

ISPs are a component of an agency's Information Security Management Framework, as mandated in the *Australian Government Information Security Management Protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of an ISP

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
- what performance measures will be established to ensure that the policy is being implemented effectively.

In developing the contents of the ISP, agencies may also consult any agency–specific directives that could be applicable to information security.

Agencies should avoid including controls for systems in their ISP. Instead, they should be documented in the SSP.

Control: 0049; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The ISP should describe information security policies, standards and responsibilities.

Control: 0890; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The ISP should cover topics such as:

- accreditation processes
- personnel responsibilities
- configuration control
- access control
- networking and connections with other systems
- physical security and media control
- emergency procedures and cyber security incident management
- change management
- information security awareness and training.

References

Nil.

Security Risk Management Plan

Objective

An SRMP identifies security risks and appropriate mitigation measures for systems.

Scope

This section describes the development of an SRMP, focusing on security risks related to the operation of systems.

Context

An SRMP is a component of an agency's *Information Security Management Framework*, as mandated in the *Australian Government Information Security Management Protocol*.

This section should be read in conjunction with the *Information Security Risk Management* section of the *About Information Security* chapter.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of an SRMP

Security risks cannot be managed if they are not known. Even if they are known, failing to deal with them is a failure of security risk management. For this reason an SRMP consists of two components, a security risk assessment and a corresponding risk treatment strategy.

Control: 0788; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The SRMP should contain a security risk assessment and a corresponding risk treatment strategy.

Agency risk management

If an agency fails to incorporate the SRMP for systems into their wider agency risk management plan then the agency will be unable to manage risks in a coordinated and consistent manner across the agency.

Control: 0893; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should incorporate their SRMP into their wider agency risk management plan.

Risk management standards

Security risk management is of most value to an agency when:

- it relates to the specific circumstances of an agency and its systems, and
- it is based on an industry–recognised approach to risk management, such as those produced by Standards Australia and the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC).

Standards Australia produces AS/NZS ISO 31000:2009, *Risk Management—Principles and guidelines* while the ISO/IEC has developed the risk management standard ISO/IEC 27005:2011, *Information technology—Security techniques—Information security risk management*, as part of the ISO/IEC 27000 family of standards.

Control: 0894; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop their SRMP in accordance with Australian or international standards for risk management.

References

For further guidance please refer to the *Australian Standard for Risk Management* AS/NZS ISO 31000:2009, the Australian Standards HB 167:2006 *Security risk management* and HB 327:2010 *Communicating and consulting about risk*.

Information on the development of SRMPs can be found in HB 231:2004, *Information security risk management guidelines*. In particular, section 5 discusses documentation. It is available from Standards Australia at http://www.standards.org.au/.

System Security Plan

Objective

An SSP specifies the security measures for systems.

Scope

This section describes the development of an SSP.

Context

An SSP is a component of an agency's Information Security Management Framework, as mandated in the *Australian Government Information Security Management Protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Further information to be included in an SSP about specific functionality or technologies that could be implemented for a system can be found in the applicable areas of this manual.

Stakeholders

There can be many stakeholders involved in defining an SSP, including representatives from the:

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

Controls

Contents of an SSP

This manual provides a list of controls that are potentially applicable to a system based on its classification, its functionality and the technology it is implementing. Agencies need to determine which controls are in scope of the system and translate those controls to the SSP. These controls will then be assessed on their implementation and effectiveness during the accreditation process for the system.

In performing accreditations against the latest release of this manual, agencies are ensuring that they are taking the most recent threat environment into consideration. ASD continually monitors the threat environment and conducts research into the security impact of emerging trends. With each release of this manual, controls can be added, rescinded or modified depending on changes in the threat environment.

Control: 0895; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must select controls from this manual 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.

Control: 0067; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the latest release of this manual when developing, and updating, their SSPs as part of accreditation and reaccreditation of their systems.

References

Further information on the *Australian Government Information Security Management Protocol* can be found at http://www.protectivesecurity.gov.au.

Standard Operating Procedures

Objective

SOPs ensure security procedures are followed in an appropriate and repeatable manner.

Scope

This section describes the development of security related SOPs.

Context

SOPs are a component of an agency's Information Security Management Framework, as mandated in the *Australian Government Information Security Management Protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Development of SOPs

To ensure that personnel undertake their duties appropriately, with a minimum of confusion, it is important that the roles of ITSMs, ITSOs, system administrators and users are covered by SOPs. Furthermore, ensuring that SOPs are consistent with SSPs reduces the potential for confusion resulting from conflicts in policy and procedures.

Control: 0051; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop SOPs for each of the following roles:

- ITSM
- ITSO
- system administrator
- user.

ITSM SOPs

The ITSM SOPs cover the management and leadership activities related to system operations.

Control: 0789; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The following procedures should be documented in the ITSM's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Cyber security incidents	Reporting and managing cyber security incidents

ITSO SOPs

The ITSO SOPs cover the operationally focused activities related to system operations.

Control: 0790; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
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 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
Cyber security incidents	Detecting potential cyber security incidents
	Establishing the cause of any cyber security incident, whether accidental or deliberate
	Actions to be taken to recover and minimise the exposure from a cyber security incident
Data transfers	Managing the review of media containing information that is to be transferred off–site
	Managing the review of incoming media for viruses or unapproved software
ICT equipment	Managing the destruction of unserviceable ICT equipment and media
System integrity audit	Reviewing user accounts, system parameters and access controls to ensure that the system is secure
	Checking the integrity of system software
	Testing access controls
	Inspecting ICT equipment and cables
System maintenance	Managing the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches/updates/ signatures, and applying appropriate hardening techniques
User account management	Authorising new users

System administrator SOPs

The system administrator SOPs support the ITSO SOPs; however, they focus on the administrative activities related to system operations.

Control: 0055; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
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 users
	Setting user privileges
	Cleaning up directories and files when a user departs or changes roles

User SOPs

The user SOPs focus on day–to–day activities that users need to know about, and comply with, when using systems.

Control: 0056; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The following procedures should be documented in the user's SOPs.

TOPIC	PROCEDURES TO BE INCLUDED
Cyber security incidents	What to do in the case of a suspected or actual cyber security incident
End of day	How to secure systems at the end of the day
Media control	Procedures for handling and using media
Passphrases	Choosing and protecting passphrases
Temporary absence	How to secure systems when temporarily absent

Agreement to abide by SOPs

When SOPs are produced the intended audience needs to be made aware of their existence and acknowledge that they have read, understood and agree to abide by their contents. Additionally, the intended audience needs to be made aware of any consequences for deviating from the agreed SOP.

Control: 0057; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
ITSMs, ITSOs, system administrators and users should sign a statement that they have read and agree to abide by their respective SOPs.

References

Nil.

Incident Response Plan

Objective

An IRP outlines actions to take in response to a cyber security incident.

Scope

This section describes the development of an IRP to address cyber security incidents. It does not cover physical security incidents.

Context

An IRP is a component of an agency's Information Security Management Framework, as mandated in the *Australian Government Information Security Management Protocol*.

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Contents of an IRP

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

Control: 0058; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

Agencies must include, as a minimum, the following content in their IRP:

- broad guidelines on what constitutes a cyber security incident
- the minimum level of cyber security incident response and investigation training for users and system administrators
- the authority responsible for initiating investigations of a cyber security incident
- the steps necessary to ensure the integrity of evidence supporting a cyber security incident
- the steps necessary to ensure that critical systems remain operational
- how to formally report cyber security incidents.

Control: 0059; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA

Agencies should include the following content in their IRP:

- clear definitions of the types of cyber security incidents that are likely to be encountered
- the expected response to each cyber security incident type
- the authority responsible for responding to cyber security incidents
- the criteria by which the responsible authority would initiate or request formal, police or Australian Security Intelligence Organisation investigations of a cyber security incident
- other authorities which need to be informed in the event of an investigation being undertaken
- the details of the system contingency measures or a reference to these details if they are located in a separate document.

References

Nil.

Emergency Procedures

Objective

Information and systems are secured before personnel evacuate a facility in the event of an emergency.

Scope

This section describes the requirements for securing information and systems as part of the procedures for evacuating a facility in the event of an emergency.

Context

Emergency procedures are a component of an agency's Information Security Management Framework, as mandated in the *Australian Government Information Security Management Protocol.*

Information about other mandatory documentation can be found in the *Documentation Fundamentals* section of this chapter.

Controls

Evacuating facilities

During the evacuation of a facility it is important that personnel secure information and systems as they would at the end of operational hours. This includes, but is not limited to, securing media and logging off workstations. This is important as malicious actor could use such an opportunity to gain access to applications or databases that a user had already authenticated to, or use another user's credentials, for a malicious purpose.

Control: 0062; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must include in evacuation procedures the requirement to secure information and systems before the evacuation; unless the chief warden, to avoid serious injury or loss of life, authorises personnel to evacuate immediately without securing information and systems.

Preparing for the evacuation of facilities

The warning phase before the evacuation of a facility alerts personnel that they may be required to evacuate the facility. This warning phase is the ideal time for personnel to begin securing information and systems to ensure that if they need to evacuate the facility they can do so immediately.

Control: 1159; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should include in evacuation procedures the requirement to secure information and systems during the warning phase before the evacuation.

References

Nil.

Business Continuity and Disaster Recovery Plans

Objective

Business continuity and disaster recovery plans help minimise the disruption to the availability of information and systems after an event or disaster.

Scope

This section describes the role of business continuity and disaster recovery plans in ensuring continuing operation of agencies' critical systems.

Context

Business continuity and disaster recovery plans work to maintain security in the face of unexpected events and changes.

Additional information relating to business continuity can be found in the *Ensuring Service Continuity* section of the *Network Security* chapter.

Controls

Availability requirements

As availability requirements will vary based on business requirements they cannot be stipulated in this manual. Agencies will need to determine their own availability requirements and implement appropriate security measures to achieve them.

Control: 0118; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must determine availability requirements for their systems and implement appropriate security measures to support these requirements.

Backup strategy

Having a backup strategy in place is an important part of business continuity planning. The backup strategy ensures that critical business information is not accidentally lost.

Control: 0119; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

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

Business continuity plans

Developing a business continuity plan can help ensure that critical functions of systems continue to operate when the system is in a degraded state. For example, when limited bandwidth is available on networks, agencies may choose to strip all large attachments from emails.

Control: 0913; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop a business continuity plan.

Disaster recovery plans

Developing a disaster recovery plan will reduce the time between a disaster occurring and critical functions of systems being restored.

Control: 0914; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop a disaster recovery plan.

References

Additional information relating to business continuity is contained in HB 221:2004, *Business Continuity Management.*

System Accreditation

Accreditation Framework

Objective

Accreditation formalises the acceptance of security risks relating to the operation of a system.

Scope

This section describes the accreditation framework for systems and agencies' responsibilities.

This chapter details the ICT system accreditation process, where a system is defined as a related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates. This chapter does not discuss physical security certifications. Further information on TOP SECRET physical security certifications can be provided by ASD on request.

Context

Accreditation is the process by which the accreditation authority formally recognises and accepts the residual security risk to a system and the information it processes, stores and communicates.

The accreditation framework comprises three layers:

- audit:
  - reviewing the information security documentation
  - assessing the appropriateness of the controls applied to the system
  - assessing the effectiveness of the implementation of the controls.
- certification:
  - providing independent assurance and acceptance of the audit
  - determining the residual security risk relating to the operation of the system.
- accreditation:
  - formally accepting the residual security risk
  - awarding approval to operate the system.

Detailed information about the processes and the requirements for conducting accreditations, certification and audits is given in the *Conducting Accreditations*, *Conducting Certifications* and *Conducting Audits* sections of this chapter.

Controls

Accreditation framework

Developing an accreditation framework ensures that accreditation activities are conducted in a repeatable and consistent manner across the agency.

Control: 0791; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop an accreditation framework.

Accreditation

Accreditation of a system ensures that either sufficient security measures have been put in place or that deficiencies in such measures have been accepted by an appropriate authority. When systems are awarded accreditation the accreditation authority accepts that the residual security risks are appropriate for the sensitivity or classification of the information that the system processes, stores or communicates.

Monitoring the accredited systems will assist in assessing changes to the environment and operation and to determine the implications for the security risk profile and accreditation status of the system.

Control: 0064; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that their system is awarded accreditation before they are used to process, store or communicate sensitive or classified information.

Control: 0065; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all systems are awarded accreditation before connecting them via a gateway.

Control: 0086; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure information security monitoring activities are conducted on accredited systems.

Determining authorities

For multinational and multi–agency systems, determining the certification and accreditation authorities through a formal agreement between the parties ensures that the system owner has appropriate points of contact and does not receive conflicting advice from different authorities.

Control: 0793; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
For multinational and multi–agency systems, the certification and accreditation authorities should be determined by a formal agreement between the parties involved.

Notifying authorities

In advising the certification and accreditation authorities of their intent to seek certification and accreditation for a system, the system owner can seek information on the latest processes and requirements for their system.

The list of accreditation and certification authorities is given in the *Conducting Accreditations* and *Conducting Certifications* sections of this chapter.

Control: 0082; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Before beginning the accreditation process, the system owner should advise the certification and accreditation authorities of their intent to seek certification and accreditation for their system.

Due diligence

When an agency is connecting to a system not under their control or passing information to another party, the agency needs to be aware of the security measures that have been implemented to protect the agency's information. More importantly, the agency needs to accept the security risks associated with non–compliance with controls in this manual by the other party before connecting or passing information to them. The security risks include the system potentially being used as a platform to launch an intrusion on the agency's system or spilling information onto a system not under their control and requiring subsequent clean up of the spilled information.

Methods that an agency may use to ensure compliance with security requirements, and to assist in security risks being identified and accepted by the agency, include:

- conducting an accreditation of the non–agency system
- having an information security review performed by an Information Security Registered Assessor on the non–agency system
- reviewing a copy of an existing certification report for the non–agency system in order to make an accreditation decision on the non–agency system.

Control: 0071; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
If information is processed, stored or communicated by a system not under an agency's control, the agency must ensure that the non–agency system has appropriate security measures in place to protect the agency's information.

Control: 0900; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should review an accreditation report when determining whether the non–agency system has appropriate security measures in place to protect the agency's information.

Control: 0072; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that security requirements are documented in either:

- contract provisions
- a memorandum of understanding.

Control: 0073; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that a process is in place to provide assurance to its management that a non–agency system meets, and will continue to meet, the agency's security requirements.

Processing restrictions

When security is applied to systems, security measures are put in place based on the sensitivity or classification of information that will be processed, stored or communicated by the system. If information is placed on a system, and its sensitivity or classification is higher than the level of accreditation for the system, the information will be inadequately protected and will be exposed to a greater risk of compromise.

Control: 0076; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow a system to process, store or communicate information above the sensitivity or classification for which the system has received accreditation.

Accrediting systems bearing a caveat or compartment

When processing caveated or compartmented information on a system, agencies need to ensure that the system has received accreditation for the caveated or compartmented information.

It should be noted that for Special Compartmented Information Facilities (SCIFs), ICT security is only one part of the requirements for gaining accreditation. Further information on gaining SCIF accreditation can be provided upon request from ASD.

Control: 0077; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
A system that processes, stores or communicates caveated or compartmented information must be accredited for such caveated or compartmented information.

Requirement for Australian control

Due to sensitivities associated with Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) systems, it is essential that control of such systems is maintained by Australian citizens working for the government of Australia.

Control: 0078; Revision: 2; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that systems processing, storing or communicating AUSTEO or AGAO information remain at all times under the control of an Australian national working for the government.

Reaccreditation

Agencies' threat environment and business needs are dynamic. Agencies should reaccredit their systems every two years to ensure their security measures are appropriate in the current environment, as security measures and processes may cease to be effective over time.

Agencies may have an additional year's grace if they follow the procedures defined in this manual for non–compliance with 'should' requirements: that is, providing a suitable justification, conducting a security risk assessment and obtaining formal approval from the accreditation authority.

Once three years has elapsed since the last accreditation, the agency needs to either reaccredit the system or seek approval for non–compliance from their agency head.

Other reasons an agency could seek reaccreditation include:

- changes in information security policies
- detection of new or emerging threats to systems
- the discovery that controls are not operating as effectively as planned
- a major cyber security incident
- changes to the system or the security risk profile.

Control: 0069; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that the period between accreditations of systems does not exceed two years.

Control: 0070; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the period between accreditations of systems does not exceed three years.

References

For agencies wishing to gain a physical security certification for SCIF areas in addition to their ICT certification, a SCIF Support Pack is available from ASD on request.

Conducting Accreditations

Objective

Systems are accredited before they are used operationally.

Scope

This section describes conducting an accreditation for a system.

Context

Accreditation aim

The aim of accreditation is to formally recognise and accept the residual security risk to a system and the information it processes, stores or communicates.

Accreditation authorities

For standard systems the accreditation authority is the agency head or their formal delegate, which is strongly recommended to be the CISO or equivalent.

For TOP SECRET systems the accreditation authority is ASD.

For systems that process, store or communicate caveated or compartmented information there may be a mandated accreditation authority external to the agency operating the system.

For multinational and multi–agency systems the accreditation authority is determined by a formal agreement between the parties involved.

For gateway services of commercial providers the accreditation authority is the agency head or their delegate, which is strongly recommended to be the CISO or equivalent.

For commercial providers supporting agencies the accreditation authority is the head of the supported agency or their authorised delegate, which is strongly recommended to be the CISO or equivalent.

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.

Depending on the circumstances and practices of an agency, the agency head can choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions; for example the CISO or equivalent.

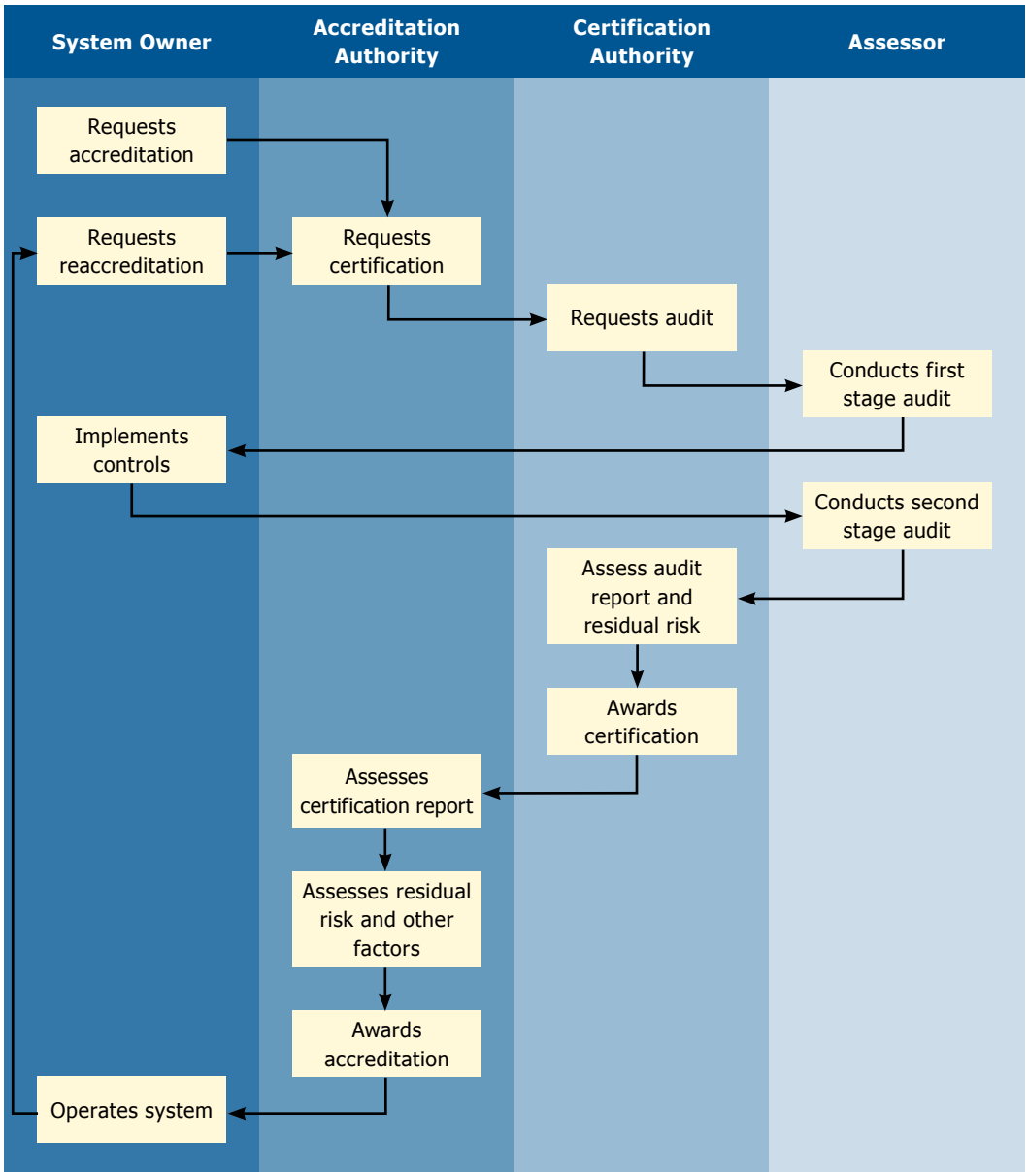
Accreditation outcomes

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 is predominantly due to security risks being insufficiently considered and documented in the SRMP, resulting in security measures being inaccurately scoped in the SSP. In such cases the accreditation authority may request that the SRMP and SSP be amended and security measures reassessed before reconsidering the system for accreditation.

In awarding accreditation for a system, the accreditation authority may specify a shorter period before reaccreditation than that specified in this manual. The accreditation authority may also place restrictions on the use of the system which must be enforced until reaccreditation takes place or until required changes are made to the system.

Accreditation process

The following diagram shows, at a high level, the process of accreditation.



Controls

Certification

Certification (described in the *Conducting Certifications* section of this chapter) provides the accreditation authority with information on the security posture of a system. This allows the accreditation authority to make an informed decision on whether the residual security risk of allowing the system to operate is acceptable.

Control: 0795; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All systems must be certified as part of the accreditation process; unless the accreditation authority is satisfied that if the system is not immediately operational it would have a devastating and potentially long–lasting effect on operations.

Accreditation decision

The purpose of conducting an accreditation of a system is to determine the security posture of the system and the security risk that it poses to information. In giving approval for the system to operate, the accreditation authority is accepting the residual security risk to information that is processed, stored or communicated by the system.

To assist in making an accreditation decision, the accreditation authority may review:

- the SRMP for the system
- the report of compliance from the audit
- the certification report from the certification authority
- any decisions to be non–compliant with any controls specified in this manual
- any additional security risk reduction strategies that have been implemented.

To assist in making an informed accreditation decision, the accreditation authority may also seek advice from technical experts on the technical components of information presented to them during the accreditation process.

Control: 0808; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The accreditation authority must accept the residual security risk relating to the operation of a system in order to award accreditation.

Control: 1229; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S; Compliance: must; Authority: AA
An agency's accreditation authority must be at least a senior executive with an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

Control: 1230; Revision: 1; Updated: Feb-14; Applicability: TS; Compliance: must; Authority: ASD
For TOP SECRET systems, the accreditation authority must be ASD.

References

Nil.

Conducting Certifications

Objective

Formal acceptance is given that a system has been audited appropriately and security controls implemented effectively.

Scope

This section describes conducting a certification as part of the accreditation process for a system.

Context

Certification aim

The aim of certification is to ensure the audit for a system was conducted in an appropriate manner and to a sufficiently high standard.

Certification outcome

The outcome of certification is a certificate to the system owner acknowledging that the system has been appropriately audited and that the controls identified by the system owner have been implemented effectively.

Certification authorities

For TOP SECRET systems the certification authority is ASD.

For SECRET or below systems the certification authority is the agency ITSA.

For systems that process, store or communicate caveated or compartmented information there may be a mandated certification authority external to the agency operating the system.

For multinational and multi–agency systems the certification authority is determined by a formal agreement between the parties involved.

For commercial providers of gateway services intended for use by multiple agencies across government, ASD performs the role of the certification authority as an independent third party.

For commercial providers supporting agencies the certification authority is the ITSA of the agency sponsoring the organisation.

Controls

Audit

The aim of an audit is to assess the actual implementation and effectiveness of controls for a system.

The process of conducting an audit is described in the *Conducting Audits* section of this chapter.

Control: 1141; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All systems must undergo an audit as part of the certification process.

Certification decision

To award certification for a system the certification authority needs to be satisfied that the controls identified by the system owner have been implemented and are operating effectively. However, certification only acknowledges that the identified controls were implemented and are operating effectively and not that the residual security risk is acceptable or an approval to operate has been awarded.

Control: 1142; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The certification authority must accept the effectiveness of controls for the system in order to award certification.

Assessment of residual security risks

Before the certification authority can make a recommendation to the accreditation authority, an assessment of the residual security risk must be done. The purpose of the assessment is to assess the residual security risk relating to the operation of a system following the audit.

Even if, after the audit, the system does not conform, the certification authority may be able to recommend to the accreditation authority that accreditation be awarded. For example, since the audit, the system owner may have taken corrective actions to address areas of non–compliance, or the residual security risk may not be great enough to preclude accreditation.

Control: 0807; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Following the audit, the certification authority should produce a certification report for the accreditation authority containing an assessment of the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not.

Certification of gateway services

Agencies may provide their own gateway services, or outsource this function to a commercial provider. In either case, agencies must ensure gateway services intended for use by multiple agencies have undergone an audit conducted by an Information Security Registered Assessor and received certification from ASD. Even though ASD may certify a gateway service from a commercial provider, agencies using the service still need to decide whether accreditation should be awarded or not.

Control: 0100; Revision: 5; Updated: Feb-14; Applicability: G, P; Compliance: must; Authority: AA
Agencies must ensure that commercial or government–provided gateway services intended for use by multiple agencies, have undergone an Information Security Registered Assessor Program Audit and ASD Gateway Certification annually.

References

Nil.

Conducting Audits

Objective

The effectiveness of security measures for systems is assessed.

Scope

This section describes conducting an audit as part of the certification process for a system.

Context

Audit aim

The aim of an audit is to review the system architecture (including the information security documentation) and assess the actual implementation and effectiveness of controls for a system.

Audit outcome

The outcome of an audit is a report to the certification authority describing areas of compliance and non–compliance for a system and any suggested remediation actions.

Who can conduct an audit

Audits for TOP SECRET systems can only be undertaken by ASD and Information Security Registered Assessors.

Audits for SECRET and below systems can be undertaken by agency ITSMs and Information Security Registered Assessors.

Who can assist with an audit

A number of agencies and personnel are often consulted during an audit.

Agencies or personnel who can be consulted on physical security aspects of information security include:

- the Australian Security Intelligence Organisation for TOP SECRET sites
- the Department of Foreign Affairs and Trade for systems located at overseas posts and missions
- the Agency Security Advisor (ASA) for all other systems.

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

An ITSM or communications security officer can be consulted on communications security aspects of information security.

Independent audits

An audit can be conducted by agency assessors; however, the agency may choose to add an extra level of objectivity by engaging the services of an Information Security Registered Assessor to undertake the audit.

Connections to certain inter–agency systems could require an independent audit from an Information Security Registered Assessor as a prerequisite to certification of the system. Such requirements can be obtained from the inter–agency system owners.

Controls

Independence of assessors

As there can be a perceived conflict of interest in the system owner assessing the security of their own system, the assessor should be independent of the system owner and certification authority. This does not preclude an appropriately qualified system owner from assessing the security of a system that they are not responsible for.

Control: 0902; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that assessors conducting audits are not also the system owner or certification authority.

Audit preparation

Ensuring that the system owner has approved the system architecture and associated information security documentation assists assessors in understanding the scope of work for the first stage of the audit.

Control: 0797; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Before undertaking the audit, the system owner must approve the system architecture and associated information security documentation.

Audit (first stage)

The purpose of the first stage of the audit is to determine that the system architecture (including information security documentation) is based on sound security principles and has addressed all applicable controls from this manual. During this stage, the statement of applicability for the system will also be assessed along with any justification for non–compliance with applicable controls from this manual.

Control: 0798; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The system architecture should be reviewed by the assessor to ensure that it is based on sound security principles and meets security requirements.

Control: 0799; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The ISP should be reviewed by the assessor to ensure that policies have been developed or identified to protect information that is processed, stored or communicated by systems.

Control: 0800; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The SRMP, SSP, SOPs and IRP must be reviewed by the assessor to ensure that they are comprehensive and appropriate for the environment the system is to operate in.

Control: 0802; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The SSP must be reviewed by the assessor to ensure that all relevant controls specified in this manual are addressed.

Control: 0904; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The system owner should provide a statement of applicability for the system which includes the following topics:

- the version of this manual used for determining controls
- controls that are, and are not, applicable to the system
- controls that are applicable but are not being complied with
- any additional controls implemented as a result of the SRMP.

Implementing controls

Without implementing the controls for a system, their effectiveness cannot be assessed during the second stage of the audit.

Control: 0084; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Before undertaking the second stage of the audit the system owner must implement the controls for the system.

Audit (second stage)

The purpose of the second stage of the audit is to determine whether the controls, as approved by the system owner and reviewed during the first stage of the audit, have been implemented and are operating effectively.

Control: 0805; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The implementation of controls must be assessed to determine whether they have been implemented and are operating effectively.

Control: 0806; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The assessor must ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.

Control: 0905; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The physical security certification should be less than 5 years old at the time of the audit.

Report of compliance

The report of compliance helps the certification authority assess the residual security risk relating to the operation of a system following the audit and any remediation activities the system owner may have undertaken.

Control: 1140; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The assessor must produce a report of compliance for the certification authority outlining areas of non–compliance for a system and any suggested remediation actions.

References

Policy and Procedures for the Information Security Registered Assessors Program contains a definition of the range of activities Information Security Registered Assessors are authorised to perform. It can be obtained from ASD's website at http://www.asd.gov.au/infosec/irap.htm.

Information Security Monitoring

Vulnerability Management

Objective

Vulnerability management activities contribute to the security of systems.

Scope

This section describes agencies' requirements for conducting vulnerability management activities for their systems.

Context

Information security monitoring practices can help ensure that new vulnerabilities are addressed and security is maintained through unforeseen events and changes, whether internal to the system or in the system's operating environment. Such practices allow agencies to be proactive in identifying, prioritising and responding to security risks. Measures to monitor and manage vulnerabilities in, and changes to, a system can provide an agency with a wealth of valuable information about its level of exposure to threats, as well as assisting agencies in keeping up to date with industry and product advances.

Vulnerability management activities will feed into an agency's wider risk management processes. Further information on risk management can be found in the *About Information Security* chapter and the *Security Risk Management Plans* section of the *Information Security Documentation* chapter.

Controls

Vulnerability management strategy

Undertaking vulnerability management activities such as regular vulnerability assessments, analysis and mitigation are important as threat environments change over time. Vulnerability assessments allow agencies to identify security weaknesses caused by misconfigurations, bugs or flaws.

Control: 1163; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA

Agencies should implement a vulnerability management strategy by:

- conducting vulnerability assessments on systems throughout their life cycle to identify vulnerabilities
- analysing identified vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls
- using a risk–based approach to prioritise the implementation of identified mitigations or treatments
- monitoring new information on new or updated vulnerabilities in operating systems, software and devices as well as other elements which may adversely impact on the security of a system.

Conducting vulnerability assessments

Conducting vulnerability assessments prior to systems being used, and after significant changes, can allow the agency to establish a baseline for further information security monitoring activities.

Conducting vulnerability assessments annually can help ensure that the latest threat environment is being addressed and that systems are configured in accordance with associated information security documentation.

It is recommended that vulnerability assessments are conducted by suitably skilled personnel independent of the target of the assessment. Such personnel can be internal to an agency, such as an IT security team, or a third party such as an Information Security Registered Assessor. Where possible, it is advisable that system managers do not conduct vulnerability assessments themselves. This ensures that there is no conflict of interest, perceived or otherwise, and that the assessment is undertaken in an objective manner.

Control: 0909; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should have vulnerability assessments conducted by suitably skilled personnel independent to the target of the assessment or by an independent third party.

An agency may choose to undertake a vulnerability assessment either:

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

Agencies will find it useful to gather appropriate information before they start a vulnerability assessment. This will help to ensure that the assessment is undertaken to a degree that is commensurate with the threat environment, and if applicable, the sensitivity or classification of information that is involved.

Depending on the scope and subject of the vulnerability assessment, agencies may gather information on areas such as:

- agency priorities, risk appetite and business requirements
- system functional and security requirements
- risk assessments, including threat data, likelihood and consequence estimates, and existing controls in place
- effectiveness of existing controls
- other possible controls
- vendor and other security best practices.

Vulnerability assessments can consist of:

- conducting documentation–based security reviews of systems' designs before they are implemented
- detailed manual testing to provide a detailed, in–depth assessment of a system once implemented
- supplementing manual testing with automated tools to perform routine, repeatable security testing. These tools should be from a reputable and trusted source.

Control: 0911; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should conduct vulnerability assessments on systems:

- before the system is deployed, this includes conducting assessments during the system design and development stages
- after a significant change to the system
- after significant changes to the threats or risks faced by a system, for example, a software vendor announces a critical vulnerability in a product used by the agency
- at least annually, or as specified by an ITSM or the system owner.

Analysing and mitigating vulnerabilities

Agencies are encouraged to monitor information about new vulnerabilities that could affect their systems. However, if no vulnerabilities are disclosed in specific products used in their systems it is important agencies are not complacent.

Vulnerabilities can be introduced as a result of poor security practices, implementations or accidental activities. Therefore, even if no new vulnerabilities in deployed products have been disclosed there is still value to be gained from conducting regular vulnerability analyses.

Furthermore, by monitoring vulnerability sources/alerts, conducting vulnerability analyses, keeping up to date with industry and product advances, and keeping up to date with changes to this manual, agencies will become aware of factors which may adversely impact the security risk profile of their systems.

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

To determine the potential impact and possible mitigations to a system, comprehensive documentation and an understanding of the system are required. External sources that can be monitored for information on new vulnerabilities are vendor published vulnerability information, other open sources and subscription services.

Mitigation efforts are best prioritised using a risk–based approach in order to address the most significant vulnerabilities first. Where two or more vulnerabilities are of similar importance, the mitigations with lower cost (in time, staff and capital) can be implemented first.

Control: 0112; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must analyse any vulnerabilities to determine their potential impact on the agency and determine appropriate mitigations or other treatments.

Control: 0113; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must mitigate or otherwise treat identified vulnerabilities as soon as possible.

References

A high–level summary of vulnerability assessment, analysis and management can be found in ASD's Protect publication *Know and minimise your vulnerabilities before they are used against you*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Change Management

Objective

Information security is an integral part of change management policy and process.

Scope

This section describes the importance of maintaining the security of systems when implementing routine and urgent changes.

Context

Identifying the need for change

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

- identification of security vulnerabilities, new threats and associated mitigations
- users identifying problems or need for enhancements
- vendors notifying upgrades to software or ICT equipment
- vendors notifying the end of life for software or ICT equipment
- 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
- other incidents or continuous improvement activities.

Types of system change

A proposed change to a system could involve either:

- an upgrade to, or introduction of, ICT equipment
- an upgrade to, or introduction of, software
- major changes to security controls.

Controls

Change management process

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

The change management process ensures that changes to systems are made in an accountable manner with due consideration and with appropriate approval. Furthermore, the change management process provides an opportunity for the security impact of the change to be considered and, if necessary, reaccreditation processes initiated.

The most likely scenario for bypassing change management processes is when an urgent change needs to be made to a system. Before and after an urgent change is implemented, it is essential that the change management process strongly enforces appropriate actions to be taken.

Control: 1211; Revision 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a formal change management process in place.

Control: 0912; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure their change management process includes:

- a policy which identifies which changes need to go through the formal change management process
- documenting the changes to be implemented
- formal approval of the change request
- maintaining and auditing logs of all changes
- conducting vulnerability management activities when significant changes have been made to the system
- testing and implementing the approved changes
- updating the relevant information security documentation including the SRMP, SSP and SOPs
- notifying and educating users of the changes that have been implemented as close as possible to the time the change is applied
- continually educating users in regard to changes.

Control: 0115; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that for routine and urgent changes:

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

Control: 0117; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The change management process must define appropriate actions to be followed before and after urgent changes are implemented.

Changes impacting the security of a system

The accreditation for a system is the acceptance of the residual security risk relating to the operation of the system. It is important therefore that, when a change occurs that impacts the overall security risk for the system, the accreditation authority is consulted on whether that residual security risk is still acceptable.

Control: 0809; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
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 system must undergo reaccreditation.

References

Nil.

Cyber Security Incidents

Detecting Cyber Security Incidents

Objective

Tools and appropriate procedures are in place to detect cyber security incidents.

Scope

This section describes controls aimed at detecting cyber security incidents. It does not cover detecting physical and personnel security incidents.

Context

A cyber security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be relevant to security.

A cyber security incident is a single or series of unwanted or unexpected cyber security events that have a significant probability of compromising business operations and threatening information security.

Additional information relating to detecting cyber security incidents can be found in the following chapters and sections:

- *Information Security Monitoring: Vulnerability Management*
- *Personnel Security for Systems: Information Security Awareness and Training*
- *Access Control: Event Logging and Auditing*
- *Network Security: Intrusion Detection and Prevention.*

Controls

Preventing and detecting cyber security incidents

The activities listed for assisting in detecting cyber security incidents will assist in mitigating the most common methods used to exploit systems.

Many potential cyber security incidents are noticed by personnel rather than software tools. However, this can only occur if personnel are well trained and aware of information security issues and know how to recognise possible cyber security incidents.

Automated tools are only as good as the quality of the analysis they provide. If tools are not adequately configured to assess potential security risks, 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.

Agencies may consider some of the tools described in the following table for detecting potential cyber security incidents.

TOOL	DESCRIPTION
Anomaly detection systems	Monitor network and host activities that do not conform to normal system activity.
Intrusion Detection Systems	Some Intrusion Detection Systems (IDSs) are combined with functionality to repel detected intrusions. Caution and assessment of the potential impact need to be exercised if this capability is to be used.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities.
Network and host IDSs	Monitor and analyse network and host activity, usually relying on a list of known malicious signatures to recognise potential cyber security incidents.
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 intrusion on the system and inadvertent system changes that render the system vulnerable to intrusion.

Control: 0120; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, implement and maintain tools and procedures covering the detection of potential cyber security incidents, incorporating:

- counter–measures against malicious code
- intrusion detection strategies
- audit analysis
- system integrity checking
- vulnerability assessments.

Control: 0121; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention as opposed to detection of cyber security incidents.

References

Nil.

Reporting Cyber Security Incidents

Objective

Reported cyber security incidents assist in maintaining an accurate threat environment picture for government systems.

Scope

This section describes agencies' responsibilities for reporting cyber security incidents. It does not cover reporting physical or personnel security incidents.

Context

Cyber security incidents and outsourcing

The requirement to lodge a cyber security incident report applies even when an agency has outsourced some or all of its information technology functions and services.

Categories of cyber security incidents

The Cyber Security Incident Reporting (CSIR) scheme defines cyber security incidents that are reportable to ASD.

Controls

Reporting cyber security incidents

Reporting cyber security incidents to an ITSM as soon as possible after it occurs provides management with a means to assess the overall damage to a system and to take remedial action, including seeking advice from ASD if necessary.

Control: 0123; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must direct personnel to report cyber security incidents to an ITSM as soon as possible after the cyber security incident is discovered.

Control: 0124; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

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

Reporting cyber security incidents to ASD

ASD uses cyber security incident reports as the basis for identifying and responding to cyber security events across government. Cyber security incident reports can also be used for developing new policies, procedures, techniques and training measures to prevent the recurrence of similar cyber security incidents across government. Agencies are recommended to coordinate their reporting of cyber security incidents to ASD e.g. through their ITSA.

Where agencies have outsourced information technology services and functions, they may request that the service provider report cyber security incidents directly to ASD. This could be specified in either a memorandum of understanding or as part of the contract of services. In such cases it is recommended that the agency's ITSA be made aware of all reporting of cyber security incidents to ASD by the service provider.

Control: 0139; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must report cyber security incidents to ASD.

Reporting cyber security incidents to ASD through the appropriate channels ensures that appropriate and timely assistance can be provided. In addition, it allows ASD to maintain an accurate threat environment picture for government systems through the CSIR scheme.

Control: 0140; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should formally report cyber security incidents using the CSIR scheme.

Outsourcing and cyber security incidents

When an agency outsources information technology services and functions, they are still responsible for the reporting of cyber security incidents. It is up to the agency to ensure the service provider informs them of all cyber security incidents to allow them to formally report these to ASD.

Control: 0141; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies that outsource their information technology services and functions must ensure that the service provider consults with the agency when a cyber security incident occurs.

Cryptographic keying material

Reporting any cyber security incident involving the loss or misuse of cryptographic keying material is particularly important, as the confidentiality and integrity of secure communications relies on the secure use of keying material.

Control: 0142; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must notify all communications security custodians of any suspected loss or compromise of keying material.

High Assurance cryptographic keying material

ACSI 107 applies to all agencies including contractors. Its requirements cover all High Assurance products used to process classified information.

For security incidents involving the suspected loss or compromise of keying material for High Assurance products, ASD will investigate the possibility of compromise and, where possible, initiate action to reduce the impact of the compromise.

Control: 0143; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must notify ASD of any suspected loss or compromise of High Assurance products or keying material associated with High Assurance products in accordance with ACSI 107.

References

Further information on reporting cyber security incidents is located on the ASD website at http://www.asd.gov.au/infosec/reportincident.htm.

The cyber security incident reporting form can be found at http://www.asd.gov.au/publications/Cyber_Security_Incident_Report.pdf.

Managing Cyber Security Incidents

Objective

Appropriate remedies assist in preventing future cyber security incidents.

Scope

This section describes agencies' responsibilities for managing cyber security incidents.

Context

The management of physical and personnel security incidents is not covered in this section unless it directly impacts on the protection of systems (for example, breaching physical protection for a server room).

Controls

Cyber security incident management documentation

Documenting responsibilities and procedures for cyber security incidents in relevant SSPs, SOPs and the IRP ensures that when a cyber security incident does occur, personnel can respond in an appropriate manner. In addition, ensuring that users are aware of reporting procedures assists in capturing any cyber security incidents that an ITSM, ITSO or system owner fail to notice.

Control: 0122; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must detail cyber security incident responsibilities and procedures for each system in the relevant SSP, SOPs and IRP.

Recording cyber security incidents

The purpose of recording cyber security incidents in a register is to highlight the nature and frequency of the cyber 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.

Control: 0125; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that all cyber security incidents are recorded in a register.

Control: 0126; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should include, at a minimum, the following information in their register:

- the date the cyber security incident was discovered
- the date the cyber security incident occurred
- a description of the cyber security incident, including the personnel and locations involved
- the action taken
- to whom the cyber security incident was reported
- the file reference.

Control: 0916; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use their register as a reference for future security risk assessments.

Handling data spills

Assuming that information is compromised as a result of a cyber security incident allows an agency to apply procedures in response to a worst case scenario.

Control: 0129; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When a data spill occurs agencies must assume that the information has been compromised.

Control: 0130; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
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.

Control: 0131; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for dealing with data spills in their IRP.

Control: 0132; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must treat any data spill as a cyber security incident and follow the IRP to deal with it.

Control: 0133; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When a data spill occurs, agencies must report the details of the data spill to the information owner.

Containing data spills

The spillage of information onto a system not accredited to handle it is considered a cyber security incident under the ASD CSIR scheme.

An affected system can be segregated by powering off the system, removing network connectivity to the device or applying access controls on information associated with the data spill to prevent access. However, it should be noted that powering off the system could destroy information that would be useful for forensics activities at a later date.

Control: 0134; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
When information is introduced onto a system not accredited to handle the information, personnel must not delete the information until advice is sought from an ITSM.

Control: 0135; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
When information is introduced onto a system not accredited to handle the information, personnel should not copy, print or email the information.

Control: 0136; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
When information is introduced onto a system not accredited to handle the information, agencies should segregate the affected system from the network.

Handling malicious code infection

The guidance for handling malicious code infections is provided to help prevent the spread of the infection and to prevent reinfecting the system. An important consideration is the infection date of the machine. However, when determining the infection date, it is important to bear in mind that the record could be inaccurate as a result of the infection.

A complete operating system reinstallation, or an extensive comparison of characterisation information, is the only reliable way to ensure that malicious code is eradicated.

Taking immediate steps after the discovery of a malicious code infection can minimise the time and cost spent eradicating and recovering from the incident.

Control: 0917; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should follow the steps described below when malicious code is detected:

- isolate the infected system
- decide whether to request assistance from ASD, and if such assistance is requested and agreed to, delay any further action until advised by ASD to continue
- scan all previously connected systems, and any media used in a set period leading up to the cyber security incident, for malicious code
- isolate all infected systems and media to prevent reinfecting the system
- change all passwords and key material stored or potentially accessed from compromised systems
- advise users of any relevant aspects of the compromise, including changing all passphrases on the compromised systems and any other system that uses the same passphrase
- use current antivirus or other Internet security software to remove the infection from the systems or media
- report the cyber security incident and perform any other activities specified in the IRP
- where possible, restore a compromised system from a known good backup or rebuild the affected machine.

Upon reporting the incident to ASD, agencies are likely to be asked to provide information to ASD regarding the incident that will assist ASD investigations and response. If agencies have an understanding of the types of information that ASD might request then this can significantly shorten incident investigation and response times.

ASD might request:

- event logs
- application whitelisting logs
- antivirus logs
- proxy logs
- VPN Logs
- DNS logs
- DHCP logs
- mail server logs.

For more information on event logging, including required retention periods, see the *Event Logging and Auditing* section of the *Access Control* chapter.

Allowing continued intrusions for the purpose of scoping the incident

Agencies may wish to allow an intrusion to continue against their system for a short period of time in order to allow time for the agency to fully understand the scope of the incident.

Control: 1212; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies considering allowing intrusion activity to continue under controlled conditions for the purpose of scoping the intrusion should inform their accreditation authority.

Allowing continued intrusions for the purpose of gathering information

Agencies allowing an intrusion to continue against a system in order to seek further information or evidence will need to establish with their legal advisors whether the actions are breaching the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

Control: 0137; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies considering allowing intrusion activity to continue under controlled conditions for the purpose of seeking further information or evidence must seek legal advice.

Integrity of evidence

While gathering evidence it is important to maintain the integrity of the information, this includes maintaining metadata about the information, who used it, and how it was used. 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.

When storing raw audit trails onto media it is important that it is done in accordance with relevant retention requirements as documented in the National Archives of Australia's (NAA) *Administrative Functions Disposal Authority.*

Control: 0138; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- transfer a copy of raw audit trails onto media for secure archiving, as well as securing manual log records for retention
- ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

Seeking assistance

If the integrity of evidence of a cyber security incident is compromised, it reduces ASD's ability to assist agencies. ASD therefore requests that no actions which could affect the integrity of the evidence be carried out before ASD's involvement.

Control: 0915; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that any requests for ASD assistance are made as soon as possible after the cyber security incident is detected and that no actions, which could affect the integrity of the evidence, are carried out before ASD's involvement.

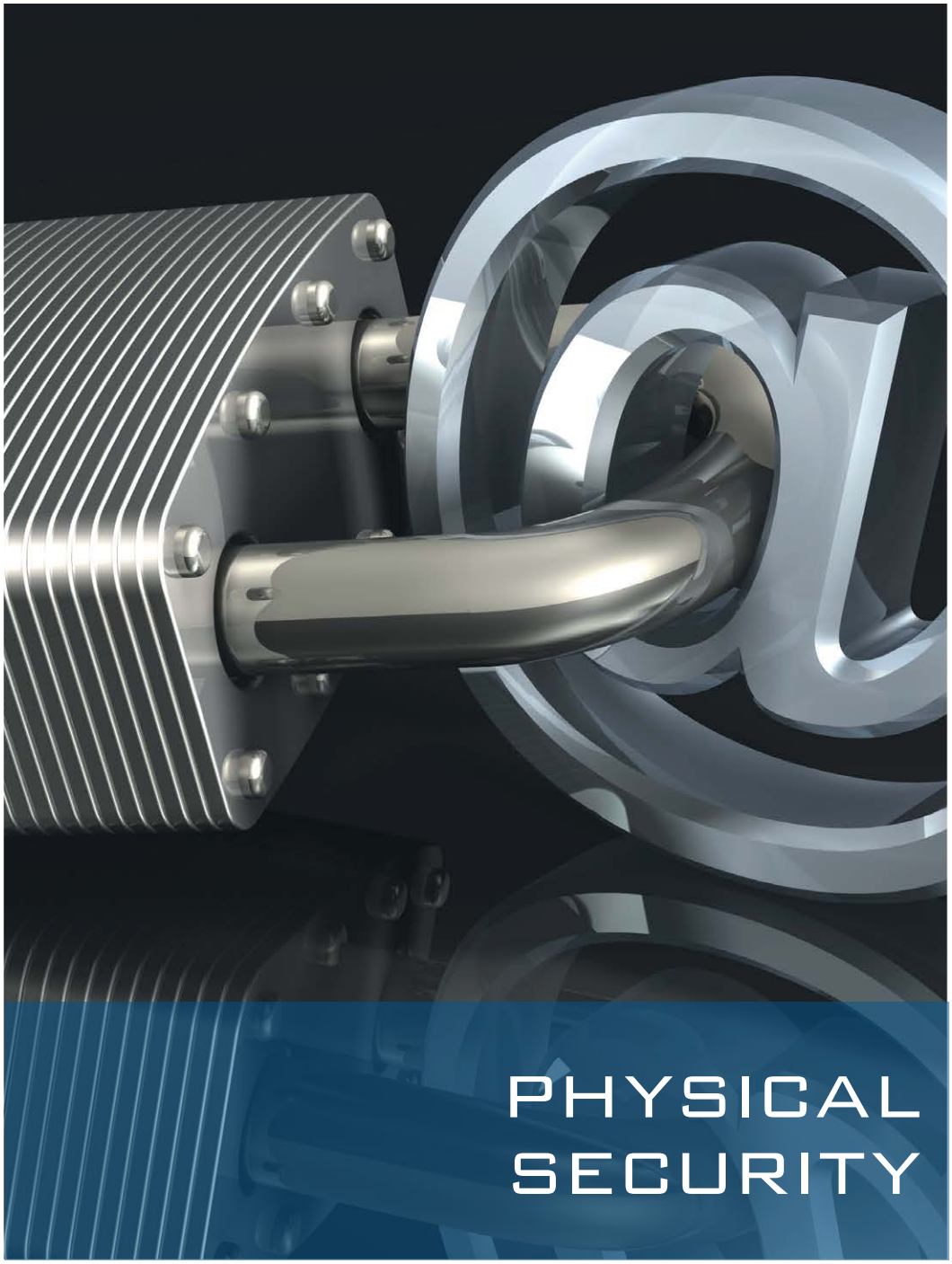
Post–incident analysis

System analysis after a successful intrusion helps to ensure the incident has been contained and removed from the system. After an incident has occurred, agencies may wish to perform post–incident analysis on their system by conducting a full network traffic capture. Agencies will be able to identify anomalous behaviour that may indicate an intruder persisting on the system, perform post–incident analysis and ensure mitigations put in place are effective.

Control: 1213; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform a post–incident analysis of successful intrusions, storing network traffic for at least seven days after the incident.

References

Further information relating to the management of ICT evidence is contained in HB 171:2003, *Guidelines for the management of information technology evidence*.



PHYSICAL SECURITY

Physical Security

Physical Security for Systems

Facilities and Network Infrastructure

Objective

Physical security measures are applied to facilities and network infrastructure to protect systems.

Scope

This section describes the requirements for the physical security of facilities and network infrastructure.

Context

Information on servers, network devices, ICT equipment and media can be found in other sections of this chapter. Information on encryption requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Facilities

In the context of this manual a facility is an area that facilitates government business. For example, a facility can be a building, a floor of a building or a designated space on the floor of a building.

Physical security certification authorities

The certification of physical security measures is undertaken by:

- the ASA for Zone Two to Zone Four security areas
- ASIO for Zone Five security areas.

For facilities that process or store caveated or compartmented information there may be a certification authority external to the agency operating the facility.

For multinational and multi–agency facilities the certification authority is determined by a formal agreement between the parties involved.

For commercial providers of gateway services intended for use by multiple agencies across government, ASIO performs the role of the certification authority as an independent third party.

For commercial providers supporting agencies the certification authority is the ASA of the agency sponsoring the organisation.

Physical security accreditation authorities

The accreditation of physical security measures for Zone Two to Zone Five security areas is undertaken by the ASA.

For facilities that process or store caveated or compartmented information there may be an accreditation authority external to the agency operating the facility.

For multinational and multi–agency facilities the accreditation authority is determined by a formal agreement between the parties involved.

For gateway services of commercial providers the accreditation authority is the ASA.

For commercial providers supporting agencies the accreditation authority is the ASA.

Controls

Facilities located outside of Australia

Control: 1214; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies operating sites in posts or missions located outside of Australia should contact the Department of Foreign Affairs and Trade to determine requirements.

Facility and network infrastructure physical security

The application of defence–in–depth to the protection of systems is enhanced through the use of successive layers of physical security. The first layer of security is the use of Security Zones for the facility, the second layer is the use of a higher Security Zone or security room for the server room 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.

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 security personnel should contact their appropriate physical security certification authority to seek guidance.

In the case of deployable platforms, physical security requirements may also include perimeter controls, building standards and manning levels.

Control: 0810; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that any facility containing a system, including deployable systems, is certified and accredited against the requirements in the *Australian Government Physical Security Management Protocol.*

Network infrastructure in unsecured spaces

Agencies do not have control over sensitive or classified information when it is communicated over public network infrastructure or over infrastructure in unsecured spaces (Zone One security areas). For this reason, it is imperative information is encrypted to a sufficient level that if it was captured it would not be cost–effective to retrieve the original information.

The PSPF's *Physical Security Management Guidelines—Security Zones and Risk Mitigation Control Measures* states a Zone Five security area is required for the storage of codeword and TOP SECRET information. Secure transmission of this information is also a key consideration. Transmission of TOP SECRET or codeword information through lower security zone areas without encryption could allow a malicious actor to successfully access and exploit TOP SECRET infrastructure with relative ease. The only way to mitigate this threat is to apply strong encryption through the use of High Assurance products.

Control: 0157; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S; Compliance: must; Authority: AA
Agencies communicating sensitive or classified information over public network infrastructure or over infrastructure in unsecured spaces (Zone One security areas) must use encryption approved for communicating such information over public network infrastructure.

Control: 1358; Revision: 0; Updated: Feb-14; Applicability: TS; Compliance: must; Authority: AA
Agencies communicating TOP SECRET or codeword information outside a Zone Five security area boundary must encrypt information using a High Assurance product.

Preventing observation by unauthorised people

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. This can be achieved by using blinds or drapes on the inside of the windows.

Control: 0164; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should prevent unauthorised people from observing systems, in particular, displays and keyboards.

References

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.* This document can be found at http://www.protectivesecurity.gov.au.

Servers and Network Devices

Objective

Server and communication rooms protect servers and network devices.

Scope

This section describes the requirements for the physical security of servers and network devices.

Context

Information relating to the physical security of facilities, network infrastructure and ICT equipment and media can be found in other sections of this chapter.

Server and communications rooms

Agencies must certify and accredit the physical security of a facility and server or communications room against the requirements in the *Australian Government Physical Security Management Protocol*. In such cases, because of the additional layer of security described in this manual, the requirements for physical storage of server and communications equipment in the *Australian Government Physical Security Management Protocol* can be lowered according to the *Physical security of ICT equipment systems and facilities* guideline.

Controls

Controlling physical access to network devices

Adequate physical protection must be provided to network devices, especially those in public areas, to prevent a malicious actor physically damaging a network device in order to cause a denial of service to a network.

Physical access to network devices can allow an intruder to reset devices to factory default settings by pressing a physical reset button, using a serial interface on a device or connecting directly to a device to bypass any access controls. Resetting a network device back to factory default settings may disable security settings on the device including authentication and encryption functions as well as resetting administrator accounts and passwords to known defaults. Even if access to a network device is not gained by resetting it, it is highly likely a denial of service will occur.

Physical access to network devices can be restricted through methods such as physical enclosures that prevent access to console ports and factory reset buttons, mounting devices on ceilings or behind walls, or placing devices in locked rooms or cabinets.

Control: 1296; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Adequate physical protection must be provided to network devices, especially those in public areas.

Securing server rooms, communications rooms and security containers

If personnel leave server rooms, communications rooms and security containers or rooms unlocked, with keys in the locks or with security functions disabled, it negates the purpose of providing security. Such activities will compromise the security efforts and must not be permitted.

Control: 1053; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that servers and network devices are secured in either security containers or rooms as specified in the *Australian Government Physical Security Management Protocol.*

Control: 0813; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not leave server rooms, communications rooms and security containers or rooms in an unsecured state.

Control: 1074; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers or rooms are appropriately controlled.

No–lone zones

Areas containing particularly sensitive materials or ICT equipment can be provided with additional security through the use of a designated no–lone zone. The aim of this designation is to enforce two–person integrity, where all actions are witnessed by at least one other qualified or knowledgeable person.

Control: 0150; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies operating no–lone zones must suitably signpost the area and have all entry and exit points appropriately secured.

References

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.* This document can be found at http://www.protectivesecurity.gov.au.

ICT Equipment and Media

Objective

ICT equipment and media is physically secured during operational and non–operational hours.

Scope

This section describes the physical security of ICT equipment and media. This includes but is not limited to workstations, printers, photocopiers, scanners, Multifunction Devices (MFDs), optical media, flash drives, portable hard drives and memory cards.

Context

Additional information relating to ICT equipment and media can be found in the *Fax Machines and Multifunction Devices* section of the *Communications Systems and Devices* chapter as well as in the *Product Security* and *Media Security* chapters. Information on the encryption of media can be found in the *Cryptography* chapter.

Controls

Accounting for ICT equipment and media

Control: 0159; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must account for all sensitive and classified ICT equipment and media.

Control: 0336; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must register all ICT equipment and media with a unique identifier in an appropriate register.

Securing ICT equipment and media

During operational and non–operational hours, ICT equipment and media needs to be stored in accordance with the *Australian Government Physical Security Management Protocol*.

The physical security requirements of the *Australian Government Physical Security Management Protocol* can be achieved by:

- ensuring ICT equipment and media always resides in an appropriate security zone
- storing ICT equipment and media during non–operational hours in an appropriate security container or room
- using ICT equipment with a removable hard drive which is stored during non–operational hours in an appropriate security container or room as well as sanitising the ICT equipment's Random Access Memory (RAM)
- using ICT equipment without a hard drive as well as sanitising the ICT equipment's RAM
- using an encryption product to reduce the physical storage requirements of the hard drive in ICT equipment to an unclassified level as well as sanitising the ICT equipment's RAM.

Control: 0161; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that ICT equipment and media with sensitive or classified information is secured in accordance with the requirements for storing sensitive or classified information in the *Australian Government Physical Security Management Protocol*.

Reducing the physical storage requirements for ICT equipment

In some circumstances it may not be feasible to secure ICT equipment during non–operational hours by storing it in a security container or room, using a removable hard drive, using ICT equipment without a hard drive or using approved encryption. In such cases the *Australian Government Physical Security Management Protocol* allows for the reduction of physical storage requirements for ICT equipment if appropriate logical controls are applied. This can be achieved by configuring systems to prevent the storage of sensitive or classified information on the hard drive (e.g. storing profiles and work documents on network shares) and enforcing scrubbing of the operating system swap file and other temporary data at logoff or shutdown in addition to the standard practice of sanitising the ICT equipment's RAM.

The security measures described in the previous paragraph do not constitute sanitisation of the hard drive in the ICT equipment. Therefore, the hard drive retains its classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal as specified in this manual.

As hybrid hard drives and solid state drives cannot be sanitised in the same manner as standard magnetic hard drives, refer to the *Media Sanitisation* section of the *Media Security* chapter, the logical controls described above are not approved as a method of lowering the physical storage requirements of the ICT equipment.

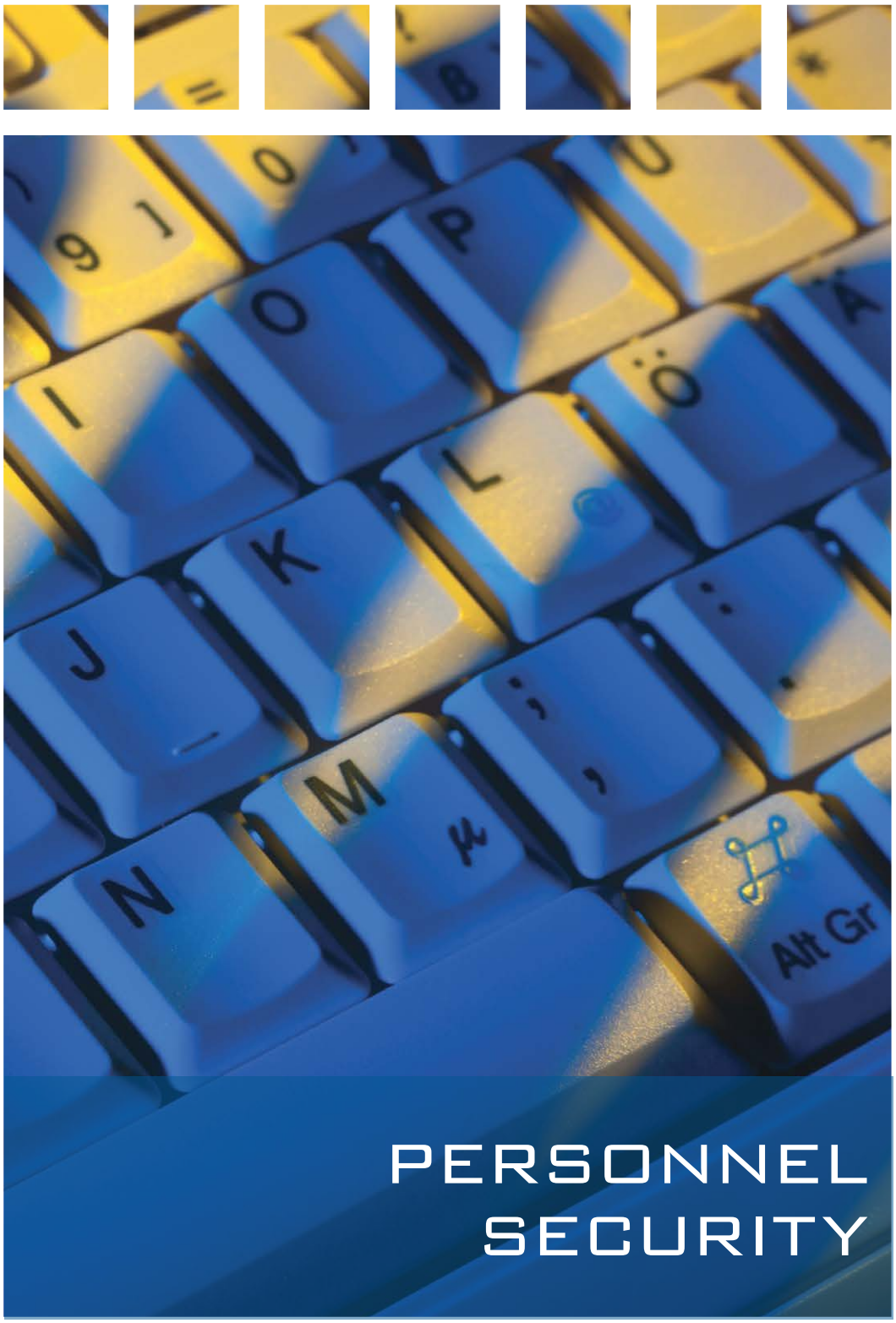
There is no guarantee that techniques such as preventing the storage of sensitive or classified information on hard drives and scrubbing the operating system swap file and other temporary data at logoff or shutdown will always work effectively or will not be bypassed due to unexpected circumstances such as an unexpected loss of power to the workstation. As such these security risks need to be considered when implementing such a solution and documented in the SSP.

Control: 0162; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies preventing the storage of sensitive or classified information on hard drives and enforcing scrubbing of the operating systems swap files and other temporary data at logoff or shutdown should:

- assess the security risks associated with such a practice
- in the SSP specify the processes and conditions for their application.

References

For further information on physical security and media security see the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol.* These documents can be found at http://www.protectivesecurity.gov.au.


PERSONNEL
SECURITY

Personnel Security

Personnel Security for Systems

Information Security Awareness and Training

Objective

A security culture is fostered through continual information security awareness and training tailored to roles and responsibilities.

Scope

This section describes information security awareness and training that should be provided to personnel.

Context

The following sections of this chapter contain information on areas that specifically need to be covered by the training provided.

Additional information that should be included in information security awareness and training is provided in the *Web Content and Connections* of the *Software Security* chapter, *Email Applications* section of the *Email Security* chapter, the *Video Conferencing and Internet Protocol Telephony* section of the *Network Security* chapter and the *Using the Internet* section of this chapter.

Controls

Information security awareness and training

Tailored education plays a major role in protecting agency systems and information from intrusion or compromise by fostering an effective security culture and sound decision–making practices.

Information security awareness and training programs are designed to help personnel to:

- become familiar with their roles and responsibilities
- understand and support security requirements
- learn how to fulfil their security responsibilities.

Control: 0252; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must provide ongoing information security awareness and training for personnel on information security policies including topics such as responsibilities, consequences of non–compliance, and potential security risks and counter–measures.

Information security awareness and training responsibility

Agencies are responsible for ensuring that an appropriate information security awareness and training program is provided to personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

Personnel will naturally lose awareness or forget training over time. Providing ongoing information security awareness and training helps keep personnel aware of issues and their responsibilities.

Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins or memoranda.

Control: 0251; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all personnel who have access to a system have sufficient information security awareness and training.

Degree and content of information security awareness and training

The exact degree and content of information security awareness and training depends on the objectives of the agency. Personnel with responsibilities beyond that of a general user will require tailored training to meet their needs.

When providing guidance to personnel it is important to emphasise which activities are not allowed on systems. The minimum list of content given below ensures that personnel are sufficiently exposed to issues that, if they are ignorant of them, could cause a cyber security incident.

Control: 0253; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should align the exact degree and content of information security awareness and training to a person's roles and responsibilities.

Control: 0922; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that information security awareness and training includes:

- the purpose of the training or awareness program
- security appointments and contacts
- the legitimate use of system accounts, software and information
- the security of accounts, including shared passphrases
- security risks associated with unnecessarily exposing email addresses and other personal details
- authorisation requirements for applications, databases and data
- the security risks associated with non–agency systems, particularly the Internet
- reporting any suspected compromises or anomalies
- reporting requirements for cyber security incidents, suspected compromises or anomalies
- classifying, marking, controlling, storing and sanitising media
- protecting workstations from unauthorised access
- informing the support section when access to a system is no longer needed
- observing rules and regulations governing the secure operation and authorised use of systems.

Control: 0255; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that information security awareness and training includes advice to personnel not to attempt to:

- physically damage systems
- bypass, strain or test security measures
- introduce or use unauthorised ICT equipment or software on a system
- assume the roles and privileges of others
- attempt to gain access to information for which they have no authorisation
- relocate ICT equipment without proper authorisation.

System familiarisation training

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, provides them with specific knowledge relating to these types of systems.

Control: 0256; Revision: 2; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Agencies must provide all 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.

References

Nil.

Authorisations, Security Clearances and Briefings

Objective

Only appropriately authorised, cleared and briefed personnel are allowed access to systems.

Scope

This section describes the authorisations, 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 *System Access* section of the *Access Control* chapter.

Context

Security clearances—Australian and foreign

Where this manual refers to security clearances, the reference applies to Australian security clearances or security clearances from a foreign government which are recognised by Australia under a security of information arrangement.

Controls

Documenting authorisations, security clearance and briefing requirements

Ensuring that the requirements for access to a system are documented and agreed upon helps determine if personnel have the appropriate authorisations, security clearances and need–to–know to access the system.

Types of system accounts for which access requirements need to be documented include general users, privileged users, contractors and visitors.

Control: 0432; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must specify in the SSP any authorisations, security clearances and briefings necessary for system access.

Authorisation and system access

Personnel seeking access to a system need to have a genuine business requirement to access the system as verified by their manager. Once a requirement to access a system is established, giving personnel only the privileges that they need to undertake their duties is imperative. Providing all personnel with privileged access when there is no requirement for privileged access can be a significant threat to a system.

Control: 0405; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must:

- limit system access on a need–to–know basis
- have any requests for access to a system authorised by the person's manager
- provide personnel with the least amount of privileges needed to undertake their duties
- review system access and privileges at least annually and when personnel change roles
- when reviewing access, ensure a response from the person's manager confirming the need to access the system is still valid, otherwise access will be removed.

Recording authorisation for personnel to access systems

Retaining records of completed system account request forms signed by each user's manager will assist with maintaining user accountability. This is required to ensure there is a record of all personnel authorised to access a system, their user identification, who provided the authorisation, when the authorisation was granted and when the access was reviewed.

Control: 0407; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- maintain a secure record of:
  - all personnel authorised to a system
  - their user identification
  - who provided the authorisation to access the system
  - when the authorisation was granted
  - when the access was reviewed
  - when the access was removed.
- maintain the record for the life of the system to which access is granted.

Security clearance for system access

A security clearance provides assurance that personnel can be trusted with access to sensitive or classified information that is processed, stored or communicated by a system.

Control: 0434; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that personnel hold an appropriate security clearance according to the requirements in the *Australian Government Personnel Security Management Protocol* before being granted access to a system.

System access briefings

Some systems may contain caveated or compartmented information. There may be unique briefings that personnel need before being granted access to such systems.

Control: 0435; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All personnel must have received any necessary briefings before being granted access to a system.

Access by foreign nationals to particularly sensitive systems

AUSTEO information is restricted to Australian nationals.

AGAO information is restricted to Australian nationals, with the exception of seconded foreign nationals, who may access such information to undertake their assigned duties.

Control: 0409; Revision: 2; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow foreign nationals, including seconded foreign nationals, to have access to systems that process, store or communicate AUSTEO information unless effective controls and procedures are in place to ensure AUSTEO information is not passed to, or made accessible by, foreign nationals, including seconded foreign nationals.

Control: 0411; Revision: 2; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow foreign nationals, excluding seconded foreign nationals, to have access to systems that process, store or communicate AGAO information unless effective controls and procedures are in place to ensure AGAO information is not passed to, or made accessible by, foreign nationals, excluding seconded foreign nationals.

Access by foreign nationals to Australian systems

When information from foreign nations is entrusted to the Australian Government, care needs to be taken to ensure that foreign nationals do not have access to such information unless it has also been released to their country.

Control: 0816; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Where systems process, store or communicate information with nationality releasability markings, agencies must not allow foreign nationals, including seconded foreign nationals, to have access to such information that is not marked as releasable to their nation.

Temporary access to classified information

Under strict circumstances access to systems may be granted to personnel who lack the appropriate security clearance.

Control: 0440; Revision: 3; Updated: Sep-11; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must follow the Temporary access to classified information requirements in the *Australian Government Personnel Security Management Protocol* before granting personnel temporary access to a system.

Controlling temporary access

When personnel are granted access to a system under the provisions of temporary access they need to be closely supervised or have their access controlled in such a way that they only have access to information they require to undertake their duties.

Control: 0441; Revision: 4; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies granting personnel temporary access to a system must ensure that either:

- effective controls are in place to restrict access to only information that is necessary to undertake their duties
- they are continually supervised by another user who has the appropriate security clearances to access the system.

Granting emergency access

Emergency access to a system may be granted where there is an immediate and critical need to access information for which personnel do not have the appropriate security clearance.

Control: 0442; Revision: 3; Updated: Sep-11; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must follow the Temporary access to classified information requirements in the *Australian Government Personnel Security Management Protocol* before granting personnel emergency access to a system.

Accessing systems without necessary security clearances and briefings

Temporary or emergency access to systems processing, storing or communicating caveated or compartmented information is not permitted.

Control: 0443; Revision: 2; Updated: Sep-11; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not grant personnel temporary access or emergency access to systems that process, store or communicate caveated or compartmented information.

References

The *Australian Government Personnel Security Management Protocol* contains Australian government policy on security clearances.

Using the Internet

Objective

Personnel use Internet services in a responsible and security conscious manner.

Scope

This section describes the policy and awareness considerations that personnel using Internet services need to know and why personnel should not use web–based email and peer–to–peer applications over the Internet.

Context

This section applies to services utilising the Internet such as web browsing, Instant Messaging (IM), Internet Relay Chat (IRC), Internet Protocol (IP) telephony, video conferencing and peer–to–peer applications. Agencies need to be aware and educate personnel that unless applications using these communications methods are evaluated and approved by ASD they must not be used for communicating sensitive or classified information over the Internet.

Additional technical information and controls are in the *Web Content and Connections* section of the *Software Security* chapter, the *Email Applications* section of the *Email Security* chapter and the *Video Conferencing and Internet Protocol Telephony* section of the *Network Security* chapter.

Controls

Using the Internet

Agencies need to determine what constitutes suspicious contact in their own work environment such as being contacted by an unknown source and ensure personnel know how to report these events. Suspicious contact may relate to questions regarding the work duties of personnel or the specifics of projects being undertaken by personnel.

Control: 0817; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure personnel know how to report any suspicious contact and what suspicious contact is, especially contact from external sources using Internet services.

Awareness of web usage policies

There is little value in having web usage policies if personnel are not made aware of their existence.

Control: 0818; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must make personnel aware of their web usage policies.

Monitoring web usage

Monitoring breaches of web usage policies—for example attempts to access blocked websites such as pornographic and gambling websites—as well as compiling a list of personnel who excessively download or upload data without a legitimate business requirement will assist agencies in enforcing their web usage policies.

Control: 0819; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement measures to monitor their personnel's compliance with their web usage policies.

Posting official information on websites

Personnel need to take special care not to accidentally post sensitive or classified information on public websites, especially in forums, blogs and social networking sites. Even unclassified information that appears to be benign in isolation, such as the Global Positioning System information in a picture, could, along with other information, have a considerable security impact on the government.

To ensure that personal opinions of personnel are not interpreted as official policy, personnel will need to maintain separate professional and personal accounts when using websites, especially when using online social networks.

Control: 0820; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure personnel are instructed to take special care not to post sensitive or classified information on public websites and how to report cases where such information is posted.

Control: 1146; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure personnel posting information on websites maintain separate professional accounts from any personal accounts they have for websites.

Control: 1147; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure personnel are aware of the approved websites on which personnel can post information authorised for release into the public domain.

Posting personal information on websites

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 sensitive or classified information from them or implant malicious software on systems by having them, for example, open emails or visit websites with malicious content.

Encouraging personnel to use the privacy settings on websites to restrict who can view their information and not allow public access will minimise who can view their interactions on websites. The privacy settings should be regularly reviewed for changes to the website policy and ensure the settings maintain privacy.

Control: 0821; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
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.

Control: 0924; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Personnel should avoid posting personal information, such as the following, on websites:

- past and present employment details
- personal details
- schools/institutions
- clubs/hobbies
- educational qualifications
- current work duties
- work contact details.

Control: 1148; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Personnel should use the privacy settings on websites to restrict access to personal information they post to only those they authorise to view it.

Peer–to–peer applications

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, eMule and uTorrent.

Some peer–to–peer IP telephony applications, such as Skype, use proprietary protocols and make heavy use of encrypted tunnels to bypass firewalls. Because of this their use cannot be regulated or monitored. It is important that agencies implementing an IP telephony solution over the Internet choose applications that use protocols that are open to inspection by IDSs.

Control: 0823; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow personnel to use peer–to–peer applications over the Internet.

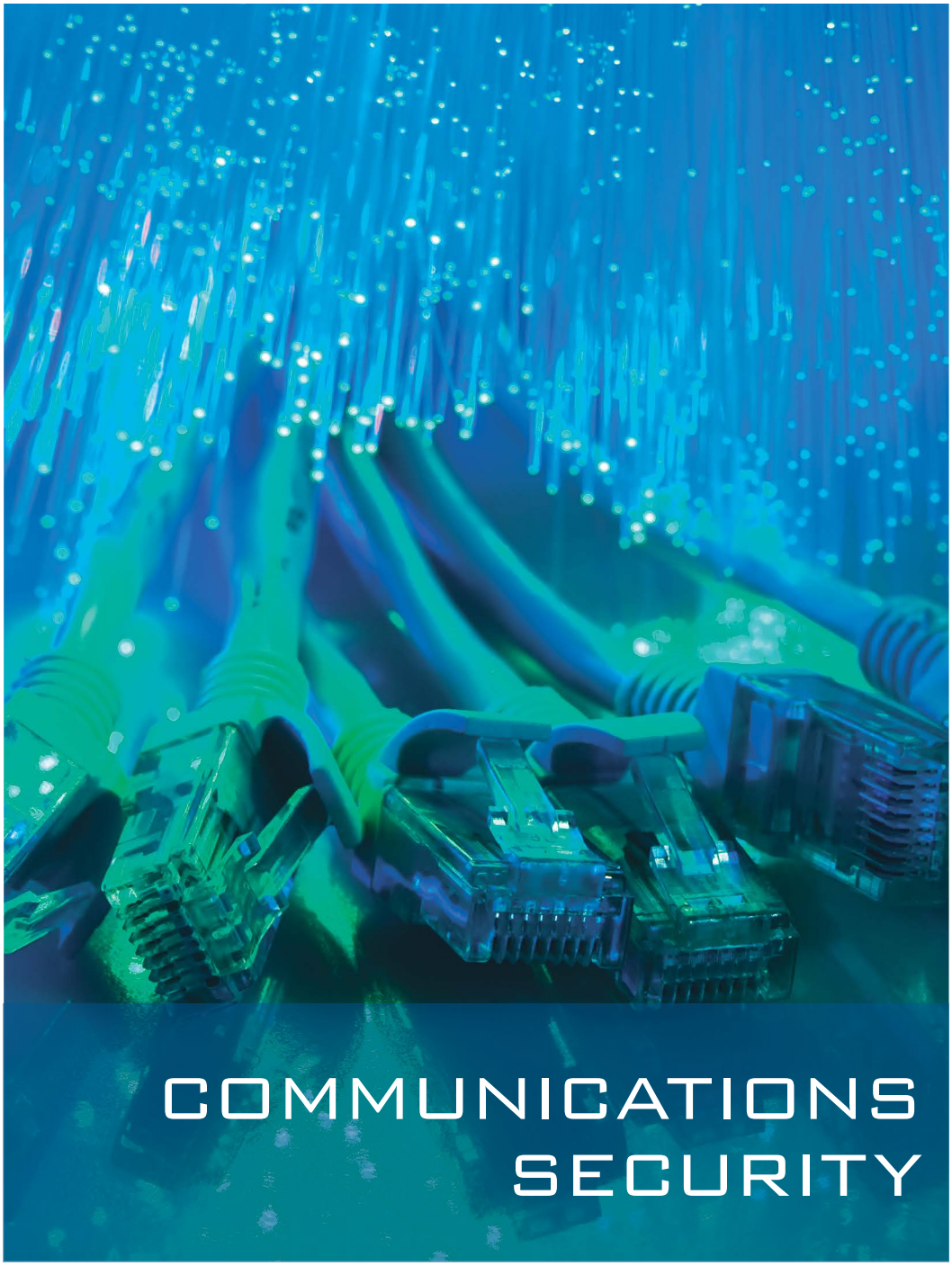
Sending and receiving files via peer–to–peer applications

When personnel send or receive files via peer–to–peer file sharing, including IM and IRC applications, they bypass security measures put in place to detect and quarantine malicious code. Encouraging personnel to send and receive files via agency established methods such as email will ensure they are appropriately marked and scanned for malicious code.

Control: 0824; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow personnel to send or receive files via peer–to–peer applications.

References

Nil.



COMMUNICATIONS SECURITY

Communications Security

Communications Infrastructure

Cable Management Fundamentals

Objective

Cable management systems are implemented to allow easy integration of systems across government.

Scope

This section describes cable distribution systems used in facilities in Australia.

Context

Applicability of controls in this section

The controls in this section only apply to new cable installations or upgrades. When designing cable management systems, the *Cable Labelling and Registration* and *Cable Patching* sections of this chapter also apply. Agencies are not required to retro fit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Common implementation scenarios

This section provides common requirements for non–shared government facilities, shared government facilities and shared non–government facilities. Further specific requirements for each scenario can be found in the other sections of this chapter.

Cables

The cable's protective sheath is not considered to be a conduit. For fibre optic cables with subunits, the cable's outer protective sheath is considered to be a conduit.

Unclassified (DLM) and Government system controls

All references to 'Unclassified (DLM)' systems in the tables here relate to systems containing unclassified but sensitive information not intended for public release, such as Dissemination Limiting Marker (DLM) information. ASD advises that government system (G) controls in the ISM are applied as a baseline to ICT equipment storing or processing Unclassified (DLM) information. Unclassified, Unclassified (DLM) and 'Government' are not classifications under the *Australian Government Security Classification System* as mandated by the Attorney–General's Department.

Controls

Cable standards

All cables must be installed by an endorsed cable installer to the relevant Australian Standards to ensure personnel safety and system availability.

Control: 0181; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must install all cables in accordance with the relevant Australian Standards as directed by the Australian Communications and Media Authority.

Cable colours

The use of defined cable colours provides an easily recognisable cable management system.

Control: 0926; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should comply with the cable colours specified in the following table.

SYSTEM	CABLE COLOUR
SECRET	Pink
CONFIDENTIAL	Green
PROTECTED	Blue
Unclassified (DLM)	Black or grey

Control: 0186; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, agencies must comply with the cable colours specified in the following table.

SYSTEM	CABLE COLOUR
TOP SECRET	Red
SECRET	Pink
CONFIDENTIAL	Green
PROTECTED	Blue
Unclassified (DLM)	Black or grey

Cable colours for foreign systems in Australian facilities

Different cable colours for foreign systems in Australian facilities helps prevent unintended patching of Australian and foreign systems.

Control: 0825; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S; Compliance: should not; Authority: AA
Agencies should not allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

Control: 0827; Revision: 0; Updated: Sep-09; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not allow cable colours for foreign systems installed in Australian facilities to be the same colour as cables used for Australian systems.

Control: 0826; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S; Compliance: should; Authority: AA
The cable colour to be used for foreign systems should be agreed between the host agency, the foreign system owner and the accreditation authority.

Control: 0828; Revision: 0; Updated: Sep-09; Applicability: TS; Compliance: must; Authority: AA
The cable colour to be used for foreign systems must be agreed between the host agency, the foreign system owner and the accreditation authority.

Cable colour non–compliance

In certain circumstances it is not possible to use the correct cable colours to match the classification. Where the accreditation authority has approved non–compliance, cables are still required to be associated with their classification. Under these circumstances agencies are to band the cables with the appropriate colour for its classification. The banding of cables is to comply with the inspection points for the cables. The size of the cable bands must be easily visible from the inspection point. For large bundles on cable reticulation systems, band and label the entire bundle. It is important bands are robust and stand the test of time. Examples of appropriate cable bands include stick–on coloured labels, colour heat shrink, coloured ferrules or short lengths of banded conduit.

Control: 1215; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S; Compliance: must; Authority: AA
Agencies that are non–compliant with cable colouring must band cables with the classification colour at the inspection points.

Control: 1216; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, no matter the classification of the system, agencies that are non–compliant with cable colouring must band and label the cables with the classification at the inspection points.

Cable groupings

Grouping cables provides a method of sharing conduits and cable reticulation systems in the most efficient manner.

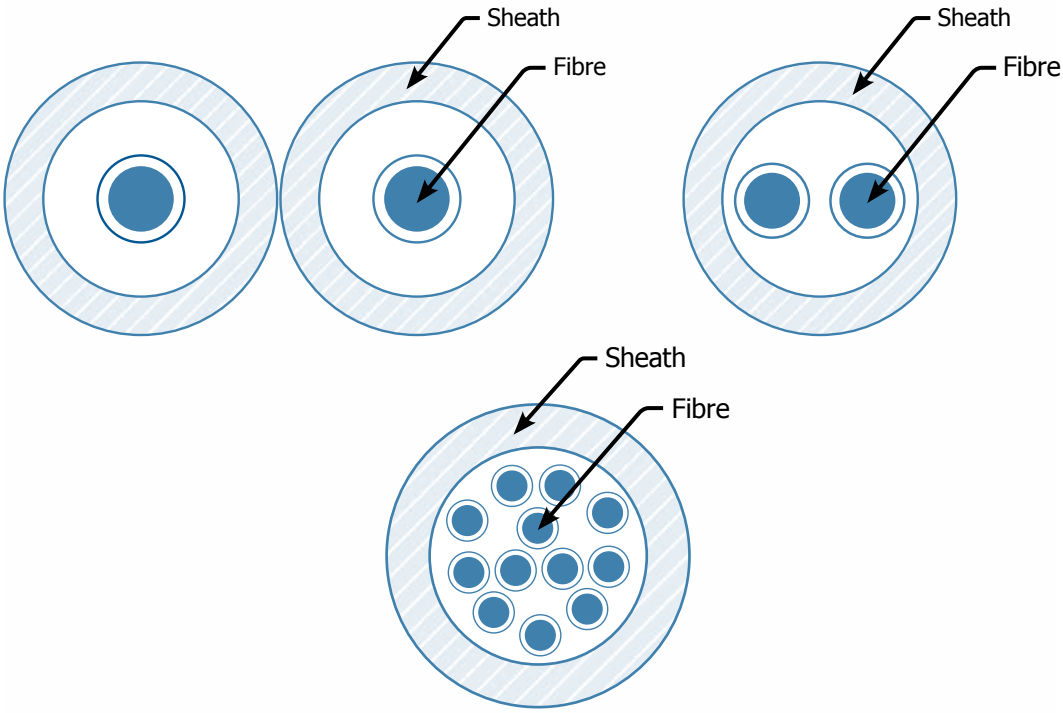
Control: 0187; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not deviate from the approved group combinations for cables as indicated below.

GROUP	APPROVED COMBINATION
1	Unclassified (DLM)
	PROTECTED
2	CONFIDENTIAL
	SECRET
3	TOP SECRET

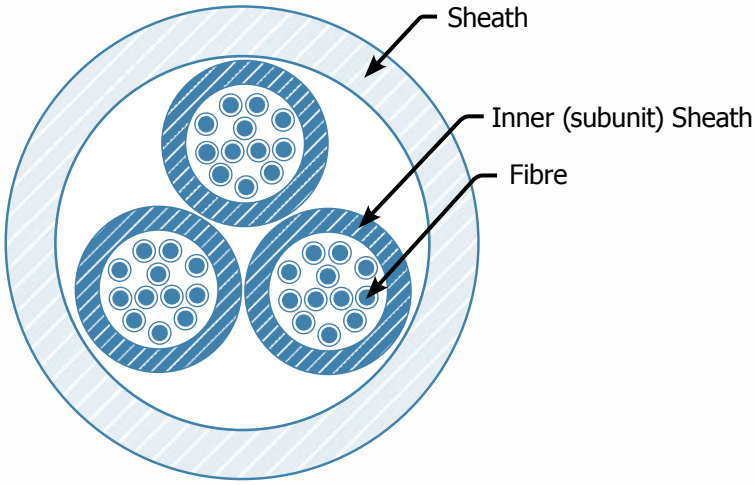
Fibre optic cables sharing a common conduit

Fibre optic cables of various cable groups can share a common conduit to reduce installation costs.

Control: 0189; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
With fibre optic cables the fibres in the sheath, as shown below, must only carry a single group.



Control: 0190; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
If a fibre optic cable contains subunits, as shown below, each subunit must only carry a single group; however, each subunit in the cable can carry a different group.



Terminating cables in cabinets

Having individual or divided cabinets for each classification prevents accidental or deliberate cross patching and makes visual inspection of cables and patching easier.

Control: 1098; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Cables should terminate in either:

- individual cabinets
- one cabinet with a division plate to delineate classifications for small systems.

Control: 1099; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: must; Authority: AA
In TOP SECRET areas, cables must terminate in either:

- individual cabinets
- one cabinet with a division plate to delineate classifications for small systems.

Control: 1100; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
TOP SECRET cables must terminate in an individual TOP SECRET cabinet.

Connecting cable reticulation systems to cabinets

Strictly controlling the routing from cable management systems to cabinets prevents unauthorised modifications and tampering and provides easy inspection of cables.

Control: 1101; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Reticulation systems leading into cabinets in secured communications and server rooms should terminate as close as possible to the cabinet.

Control: 1102; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Reticulation systems leading into cabinets not in a secure communications or server room should terminate as close as possible to the cabinet.

Control: 1103; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, reticulation systems leading into cabinets not in a secure communications or server room must terminate at the boundary of the cabinet.

Audio secure spaces

Audio secure spaces are designed to prevent audio conversations from being heard outside the walls. Penetrating an audio secure space in an unapproved manner can degrade this. Consultation with ASIO needs to be undertaken before any modifications are made to audio secure spaces. For physical security measures regarding Security Zone requirements, refer to the *Australian Government Physical Security Management Protocol.*

Control: 0198; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
When penetrating an audio secured space, agencies must consult with ASIO and comply with all directions provided.

Wall outlet terminations

Wall outlet boxes are the main method of connecting cable infrastructure to workstations. They allow the management of cables and the type of connectors allocated to various systems.

Control: 1104; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: must; Authority: AA
Cable groups sharing a wall outlet must:

- use fibre optic cables
- use different connectors on opposite sides of the wall outlet for each group.

Control: 1105; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
TOP SECRET cables must not share a wall outlet with another classification.

Control: 1106; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
In areas containing outlets for both TOP SECRET systems and systems of other classifications, agencies must ensure that the connectors for the TOP SECRET systems are different from those of the other systems.

Wall outlet colours

The colouring of wall outlets makes it easy to identify TOP SECRET infrastructure.

Control: 1107; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: must not; Authority: AA
Wall outlets must not be coloured red.

Control: 1108; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Wall outlets must be coloured red.

Wall outlet covers

Transparent covers on wall outlets allows for inspection of cables for cross patching and tampering.

Control: 1109; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Faceplates on wall outlets should be clear plastic.

Control: 1110; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, faceplates on wall outlets must be clear plastic.

References

Australian Standards for cables can be obtained from
http://www.acma.gov.au/Industry/Telco/Infrastructure/Cabling-rules.

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*

Cable Management for Non–Shared Government Facilities

Objective

Cable management systems are implemented in non–shared government facilities.

Scope

This section describes cables installed in facilities where the entire facility and personnel are cleared to the highest level of information processed in the facility.

Context

Applicability of controls in this section

This section is to be applied in addition to common requirements for cables as outlined in the *Cable Management Fundamentals* section of this chapter. The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retro fit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre optic cables

Fibre optic cables do not produce, and are not influenced by, electromagnetic emanations, and therefore offer the highest degree of protection from electromagnetic emanation effects.

Fibre cables are more difficult to tap than copper cables.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre cable is the best method to future proof cable infrastructure—it protects against unforeseen threats and facilitates upgrading secure cables to higher classifications in the future.

Control: 1111; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use fibre optic cables.

Inspecting cables

Regular inspections of cable installations are necessary to detect any illicit tampering or degradation.

Control: 1112; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agency cables should be inspectable at a minimum of five–metre intervals.

Cables sharing a common reticulation system

Laying cables in a neat and controlled manner that allows for inspections reduces the need for individual cable trays for each classification.

Control: 1114; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the differing cable groups.

Cables in walls

Cables run correctly in walls allows for neater installations while maintaining separation and inspection requirements.

Control: 1115; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use flexible or plastic conduit in walls to run cables from cable trays to wall outlets.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cables or cross patching.

Control: 1116; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: should; Authority: AA
Agencies should ensure there is a visible gap between TOP SECRET cabinets and cabinets of a lower classification.

References

Nil.

Cable Management for Shared Government Facilities

Objective

Cable management systems are implemented in shared government facilities.

Scope

This section describes cables installed in facilities where the facility and personnel are cleared at different levels.

Context

Applicability of controls in this section

This section is to be applied in addition to common requirements for cables as outlined in the *Cable Management Fundamentals* section of this chapter. The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retro fit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre optic cables

Fibre optic cables do not produce, and are not influenced by, electromagnetic emanations, and therefore offer the highest degree of protection from electromagnetic emanation effects.

Fibre optic cables are more difficult to tap than copper cables.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre optic cable is the best method to future proof cable infrastructure—it protects against unforeseen threats and facilitates upgrading secure cables to higher classifications in the future.

Control: 1117; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use fibre optic cables.

Inspecting cables

In a shared government facility it is important that cable systems be inspected for illicit tampering and damage on a regular basis and that they have tighter controls than in a non–shared government facility.

Control: 1118; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Cables should be inspectable at a minimum of five–metre intervals.

Control: 1119; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
In TOP SECRET areas, cables should be fully inspectable for their entire length.

Cables sharing a common reticulation system

In a shared government facility, tighter controls are placed on sharing reticulation systems.

Control: 1120; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the individual cable groups.

Cables in walls

In a shared government facility, cables run correctly in walls allow for neater installations while maintaining separation and requirements for inspecting cables.

Control: 1121; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Cables from cable trays to wall outlets should run in flexible or plastic conduit.

Wall penetrations

Penetrating a wall into a lesser–classified space by cables requires the integrity of the classified space to be maintained. All cables are encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure space. For physical security measures regarding Security Zone requirements refer to the *Australian Government Physical Security Management Protocol.*

Control: 1122; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: should; Authority: AA
For wall penetrations that exit into a lower classified space, cables should be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

In a shared government facility with lesser–classified systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

Control: 1123; Revision: 1; Updated: Sep-12; Applicability: TS; Compliance: should; Authority: AA
TOP SECRET facilities should have a power distribution board located in the TOP SECRET area with a feed from an Uninterruptible Power Supply (UPS) to power all ICT equipment.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cables or cross patching.

Control: 1124; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: should; Authority: AA
Agencies should ensure there is a visible gap between TOP SECRET cabinets and cabinets of a lower classification.

References

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*

Cable Management for Shared Non–Government Facilities

Objective

Cable management systems are implemented in shared non–government facilities.

Scope

This section describes cables installed in facilities shared by agencies and non–government organisations.

Context

Applicability of controls in this section

This section is to be applied in addition to common requirements for cables as outlined in the *Cable Management Fundamentals* section of this chapter. The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retro fit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Use of fibre optic cables

Due to the higher degree of associated risk, greater consideration should be applied to the use of fibre optic cables in shared non–government facilities. Fibre optic cables do not produce, and are not influenced by, electromagnetic emanations, and therefore offer the highest degree of protection from electromagnetic emanation effects.

Fibre optic cables are more difficult to tap than copper cables.

Many more fibres can be run per cable diameter than wired cables, reducing cable infrastructure costs.

Fibre optic cable is the best method to future proof cable infrastructure—it protects against unforeseen threats and facilitates upgrading secure cables to higher classifications in the future.

Control: 1125; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should use fibre optic cables.

Control: 0182; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, agencies must use fibre optic cables.

Inspecting cables,

In a shared non–government facility it is imperative that cable systems be inspected for illicit tampering and damage on a regular basis and that they have tighter controls where the threats are closer and unknown.

Control: 1126; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Cables should be inspectable at a minimum of five–metre intervals.

Control: 0184; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, cables must be fully inspectable for their entire length.

Cables sharing a common reticulation system

In a shared non–government facility, tighter controls are placed on sharing reticulation systems as the threats to tampering and damage are increased.

Control: 1127; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Approved cable groups can share a common reticulation system but should have either a dividing partition or a visible gap between the differing cable groups.

Control: 1128; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: must; Authority: AA
In TOP SECRET areas, approved cable groups can share a common reticulation system but must have either a dividing partition or a visible gap between the differing cable groups.

Control: 1129; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: must not; Authority: AA
TOP SECRET cables must not share a common reticulation system unless it is in an enclosed reticulation system and has dividing partitions or visible gaps between the differing cable groups.

Enclosed cable reticulation systems

In a shared non–government facility, TOP SECRET cables are enclosed in a sealed reticulation system to prevent access and enhance cable management.

Control: 1130; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S; Compliance: should; Authority: AA
Cables should be run in an enclosed cable reticulation system.

Control: 1131; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, cables must be run in an enclosed cable reticulation system.

Covers for enclosed cable reticulation systems

Clear covers on enclosed reticulation systems are a convenient method of maintaining inspection and control requirements. Having clear covers face inwards increases their inspection.

Control: 1164; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S; Compliance: should; Authority: AA
Conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings should be clear plastic.

Control: 1165; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
In TOP SECRET areas, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings must be clear plastic.

Cables in walls

In a shared non–government facility, cables run correctly in walls allows for neater installations while maintaining separation and inspection requirements. Controls are more stringent than in a non–shared government facility or a shared government facility.

Control: 1132; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Cables from cable trays to wall outlets must run in flexible or plastic conduit.

Cables in party walls

In a shared non–government facility, cables are not allowed in a party wall. A party wall is a wall shared with an unsecured space where there is no control over access. An inner wall can be used to run cables where the space is sufficient for inspection of the cables.

Control: 1133; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Cables must not run in a party wall.

Sealing conduits

In a shared non–government facility, where the threat of access to cables is increased, all conduits are sealed with a visible smear of glue to prevent access to cables.

Control: 0194; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must use a visible smear of conduit glue to seal:

- all plastic conduit joints
- conduit runs connected by threaded lock nuts.

Sealing reticulation systems

In a shared non–government facility, where the threats of access to cable reticulation systems is increased, Security Construction and Equipment Committee (SCEC) endorsed seals are required to provide evidence of any tampering or illicit access.

Control: 0195; Revision: 2; Updated: Sep-11; Applicability: TS; Compliance: must; Authority: AA
Agencies must use SCEC endorsed tamper evident seals to seal all removable covers on reticulation systems, including:

- box section front covers
- conduit inspection boxes
- outlet and junction boxes
- T–pieces.

Control: 0196; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Tamper evident seals must be uniquely identifiable.

Wall penetrations

Penetrating a wall to a lesser–classified space by cables requires the integrity of the classified space be maintained. All cables are encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure space. For physical security measures regarding Security Zone requirements refer to the *Australian Government Physical Security Management Protocol.*

Control: 1134; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
For wall penetrations that exit into a lower classified space, cables must be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Power reticulation

In a shared non–government facility, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means. The addition of a UPS is required to maintain availability of the TOP SECRET systems.

Control: 1135; Revision: 0; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
TOP SECRET facilities must have a power distribution board located in the TOP SECRET area with a feed from a UPS to power all ICT equipment.

Cabinet separation

Having a definite gap between cabinets allows for ease of inspections for any illicit cables or cross patching.

Control: 1136; Revision: 1; Updated: Sep-11; Applicability: TS; Compliance: must; Authority: AA
Agencies must ensure there is a visible gap between TOP SECRET cabinets and cabinets of a lower classification.

References

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 SCEC at http://www.scec.gov.au/.

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*

Cable Labelling and Registration

Objective

Cable registers are used to record cables and labels.

Scope

This section describes the labelling of cable infrastructure installed in secured spaces.

Context

Applicability of controls in this section

The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Conduit label specifications

Conduit labels must be a specific size and colour to allow easy identification of secure conduits carrying cables.

Control: 0201; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Labels for TOP SECRET conduits must be:

- a minimum size of 2.5cm x 1cm
- attached at 5m intervals
- marked as 'TS RUN'.

Control: 0202; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Conduit labels in areas where uncleared personnel could frequently visit must have red text on a clear background.

Control: 0203; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Conduit labels in areas that are not clearly observable must have red text on a white background.

Installing conduit labelling

Conduit labelling in public or reception areas could draw unwanted attention to the level of classified processing and lead to a disclosure of capabilities.

Control: 0204; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Conduit labels installed in public or visitor areas should not draw undue attention from people who do not have a need–to–know of the existence of such cables.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment of a lesser classification to the wrong outlet.

Control: 1095; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Wall outlet boxes should denote the classification, cable number and outlet number.

Control: 0205; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Wall outlet boxes must denote the classification, cable number and outlet number.

SOPs

Documenting labelling conventions in SOPs makes cable and fault finding easier.

Control: 0206; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Site conventions for labelling and registration should be documented in an agency's SOPs.

Labelling cables

Labelling cables with the correct source and destination information minimises the likelihood of cross patching and aids in fault finding and configuration management.

Control: 1096; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should label cables at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable.

Control: 0207; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must label cables at each end, with sufficient source and destination details to enable the physical identification and inspection of the cable.

Cable register

Cable registers provide a source of information that assessors can view to verify compliance.

Control: 0208; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should maintain a register of cables.

Control: 0210; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must maintain a register of cables.

Cable register contents

Cable registers allow installers and assessors to trace cable for inspections, malice or accidental damage. Cable registers track all cable management changes through the life of the system.

Control: 0209; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
The cable register should record at least the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers if applicable.

Control: 1097; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
For cables in TOP SECRET areas, the cable register must record at least the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers if applicable.

Cable inspections

Cable inspections, at predefined periods, are a method of checking the cable management system with the cable register.

Control: 0211; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SSP.

References

Nil.

Cable Patching

Objective

Communications systems are designed to prevent patching between different classifications and security domains.

Scope

This section describes the configuration and installation of patch panels, patch cables and fly leads associated with communications systems.

Context

Applicability of controls in this section

The controls in this section only apply to new cable installations or upgrades. Agencies are not required to retro fit existing cable infrastructure to align with changes to controls in this manual. The controls are applicable to all facilities that process sensitive or classified information. For deployable platforms or facilities outside of Australia, consult the *Emanation Security Threat Assessments* section of this chapter.

Controls

Terminations to patch panels

Connecting a system to another system of a lesser classification will result in a data spill, possibly resulting in the following issues:

- inadvertent or deliberate access by non–cleared personnel
- the lesser system not meeting the appropriate requirements to secure the classified information from unauthorised access or tampering.

Control: 0213; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that only approved cable groups terminate on a patch panel.

Patch cable and fly lead connectors

Ensuring that cables are equipped with connectors of a different configuration to all other cables prevents inadvertent connection to systems of lower classifications.

Control: 1093; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
In areas containing cables for systems of different classifications, agencies should ensure that the connectors for each system are different from those of the other systems; unless the length of the higher classified patch cables is less than the distance between the higher classified patch panel and any patch panel of a lower classification.

Control: 0214; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
In areas containing cables for both TOP SECRET systems and systems of other classifications, agencies must ensure that the connectors for the TOP SECRET systems are different from those of the other systems.

Control: 1094; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S; Compliance: should; Authority: AA
In areas containing cables for systems of different classifications, agencies should document the selection of connector types.

Control: 0215; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
In areas containing cables for both TOP SECRET systems and systems of other classifications, agencies must document the selection of connector types for TOP SECRET systems.

Physical separation of patch panels

Appropriate physical separation between a TOP SECRET system and a system of a lesser classification:

- reduces or eliminates the chances of cross patching between the systems
- reduces or eliminates the possibility of unauthorised personnel gaining access to TOP SECRET system elements.

Control: 0216; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should; Authority: AA
Agencies should physically separate TOP SECRET and non–TOP SECRET patch panels by installing them in separate cabinets.

Control: 0217; Revision: 3; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Where spatial constraints demand patch panels of a lower classification than TOP SECRET be located in the same cabinet, agencies must:

- provide a physical barrier in the cabinet to separate patch panels
- ensure that only personnel holding a TOP SECRET security clearance have access to the cabinet
- obtain approval from the relevant accreditation authority prior to installation.

Fly lead installation

Keeping the lengths of fly leads to a minimum prevents clutter around desks, prevents damage to fibre optic cables and reduces the chance of cross patching and tampering. If lengths become excessive, cable needs to be treated as infrastructure and run in conduit or fixed infrastructure such as desk partitioning.

Control: 0218; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: should; Authority: AA
Agencies should ensure that the fibre optic fly leads used to connect wall outlets to ICT equipment either:

- do not exceed 5m in length
- if they exceed 5m in length:
  - are run in the facility's fixed infrastructure in a protective and easily inspected pathway
  - are clearly labelled at the equipment end with the wall outlet designator
  - are approved by the accreditation authority.

References

Nil.

Emanation Security Threat Assessments

Objective

A valid threat assessment is used to determine the appropriate counter–measures to minimise compromising emanations.

Scope

This section describes emanation security threat assessment advice so agencies can implement appropriate counter–measures to minimise the loss of sensitive or classified information through compromising emanations.

Context

This section is only applicable to:

- agencies located outside of Australia
- facilities in Australia that have transmitters
- facilities that are shared with non–Australian government entities
- mobile platforms and deployable assets that process sensitive or classified information.

Controls

Emanation security threat assessments in Australia

Obtaining the current threat advice from ASD on potential adversaries and applying the appropriate counter–measures is vital in protecting the confidentiality of sensitive and classified systems from emanation security threats.

Implementing required counter–measures against emanation security threats can prevent 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 expensive and time consuming to retro fit.

Control: 0247; Revision: 2; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA

Agencies designing and installing systems with Radio Frequency (RF) transmitters inside or co–located with their facility must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 0248; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S; Compliance: must; Authority: AA

Agencies designing and installing systems with RF transmitters that co–locate with systems of a higher classification must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 1137; Revision: 1; Updated: Feb-14; Applicability: TS; Compliance: must; Authority: AA
Agencies designing and installing systems in shared facilities with non–Australian government entities must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Emanation security threat assessments outside Australia

Fixed sites outside Australia and deployed military platforms are more vulnerable to emanation security threats and require a current threat assessment and counter–measure implementation. Failing to implement recommended counter–measures and SOPs to reduce threats could result in the platform emanating compromising signals, which if intercepted and analysed, could lead to platform compromise with serious consequences.

Control: 0932; Revision: 4; Updated: Feb-14; Applicability: G, P; Compliance: should; Authority: AA
Agencies deploying systems overseas should:

- contact ASD for emanation security threat advice
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Control: 0249; Revision: 2; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies deploying systems overseas in military and fixed locations must:

- contact ASD for an emanation security threat assessment in accordance with the latest version of ACSI 71
- install cables and ICT equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Early identification of emanation security issues

It is important to identify the need for emanation security controls for a system early in the project life cycle as this can reduce costs for the project. Costs are much greater if changes have to be made once the system has been designed and deployed.

Control: 0246; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies needing an emanation security threat assessment should do so as early as possible in project life cycles as emanation security controls can have significant cost implications.

ICT equipment in highly sensitive areas

While ICT equipment in a TOP SECRET area in Australia may not need certification to TEMPEST standards, the equipment still needs to meet applicable industry and government standards.

Control: 0250; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must ensure that ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

References

Additional information on cables and separation standards, as well as the potential dangers of operating RF transmitters near systems is documented in the latest version of ACSI 61.

Additional information on conducting an emanation security threat assessment is found in the latest version of ACSI 71.

Communications Systems and Devices

Radio Frequency, Infrared and Bluetooth Devices

Objective

Only approved RF, infrared and Bluetooth devices are brought into secured areas.

Scope

This section describes the use of RF, infrared and Bluetooth devices in secured spaces. Information on the use of RF devices outside secured spaces can be found in the *Working Off–Site* chapter.

Context

Exemptions for the use of infrared devices

An infrared device can be used in a secured space provided it does not communicate sensitive or classified information.

Exemptions for the use of RF devices

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
- car lock/alarm keypads
- medical and exercise equipment that uses RF to communicate between sub–components
- communications radios that are secured by approved cryptography.

Controls

Pointing devices

Since wireless RF pointing devices can pose an emanation security risk they are not to be used in TOP SECRET areas unless in an RF screened building.

Control: 0221; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Wireless RF pointing devices must not be used in TOP SECRET areas unless used in an RF screened building.

Infrared keyboards

When using infrared keyboards with CONFIDENTIAL or SECRET systems, drawn curtains that block infrared transmissions are an acceptable method of protection.

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.

Control: 0222; Revision: 1; Updated: Sep-09; Applicability: G, P; Compliance: should; Authority: AA
Agencies using infrared keyboards should ensure that infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.

Control: 0223; Revision: 3; Updated: Sep-11; Applicability: C, S; Compliance: must not; Authority: AA
Agencies using infrared keyboards must not allow:
- line of sight and reflected communications travelling into an unsecured space
- multiple infrared keyboards for different systems in the same area
- other infrared devices in the same area
- infrared keyboards to be operated in areas with unprotected windows.

Control: 0224; Revision: 3; Updated: Sep-11; Applicability: TS; Compliance: must not; Authority: AA
Agencies using infrared keyboards must not allow:
- line of sight and reflected communications travelling into an unsecured space
- multiple infrared keyboards for different systems in the same area
- other infrared devices in the same area
- infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

Bluetooth and wireless keyboards

Bluetooth has a number of known weaknesses in the protocol that potentially enable exploitation. While there have been a number of revisions to the protocol that have made incremental improvements to security, there have been trade–offs that have limited the improvements. These include maintaining backward compatibility to earlier versions of the protocol and limits to the capabilities of some devices.

Though newer revisions of the Bluetooth protocol have addressed many of the historical security concerns, it is still very important that agencies consider the security risks posed by enabling Bluetooth technology.

As part of an agency's security risk assessment, things to consider are:
- using the strongest security modes available
- educating users of the known weaknesses of the technology and their responsibilities in complying with policy in the absence of strong technical controls
- man–in–the–middle pairing
- maintaining an inventory of all Bluetooth devices addresses (BD_ADDRs).

Bluetooth version 2.1 and subsequent versions introduced secure simple pairing and extended inquiry response. Secure simple pairing improves the pairing experience for Bluetooth devices, while increasing the strength as it uses a form of public key cryptography. Extended inquiry response provides more information during the inquiry procedure to allow better filtering of devices before connecting.

The device class can be used to restrict the range that the Bluetooth communications will operate over. Typically Bluetooth class 1 devices can communicate up to 100 metres, class 2 devices can communicate up to 10 metres and class 3 devices can communicate up to 5 metres.

Control: 1058; Revision: 0; Updated: Nov-10; Applicability: G, P; Compliance: should not; Authority: AA
Agencies should not use Bluetooth and wireless keyboards unless in an RF screened building.

Control: 1155; Revision: 0; Updated: Nov-10; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not use Bluetooth and wireless keyboards unless in an RF screened building.

Control: 1166; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: must; Authority: AA
Agencies must use Bluetooth version 2.1 or later if Bluetooth keyboards are used.

Control: 1167; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: should; Authority: AA
Agencies should restrict the range of Bluetooth keyboards to less than 10 metres by only using class 2 or class 3 devices.

RF devices in secured spaces

RF devices with voice capability pose an audio security threat to secured spaces as they are capable of picking up and transmitting sensitive or classified background conversations. Furthermore, many RF devices can connect to ICT equipment and act as unauthorised data storage devices.

Control: 0830; Revision: 0; Updated: Sep-09; Applicability: P, C, S; Compliance: should; Authority: AA
Agencies should prevent RF devices from being brought into secured spaces unless authorised by the accreditation authority.

Control: 0225; Revision: 1; Updated: Sep-09; Applicability: TS; Compliance: must; Authority: AA
Agencies must prevent RF devices from being brought into TOP SECRET areas unless authorised by the accreditation authority.

Detecting RF devices in secured spaces

As RF devices are prohibited in highly classified environments, agencies are encouraged to deploy security measures that detect and respond to the unauthorised use of such devices.

Control: 0829; Revision: 2; Updated: Sep-11; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should deploy security measures to detect and respond to active RF devices in secured spaces.

RF controls

Minimising the output power of wireless devices and using RF shielding on facilities will assist in limiting the wireless communications to areas under the control of the agency.

Control: 0929; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should limit the effective range of communications outside their area of control by either:

- minimising the output power level of wireless devices
- RF shielding.

References

Further information on Bluetooth security can be found in the NIST SP 800–121 *Guide to Bluetooth Security* at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911133.

Fax Machines and Multifunction Devices

Objective

Fax machines and Multifunction Devices (MFDs) are used in a secure manner.

Scope

This section describes fax machines and MFDs connected to the Public Switched Telephone Network (PSTN), High Assurance product or computer networks.

Context

Further information on MFDs communicating via network gateways can be found in the *Cross Domain Security* chapter.

Controls

Fax machine and MFD usage policy

As fax machines and MFDs are capable of communicating sensitive or classified information, and are a potential source of cyber security incidents, it is important that agencies develop a policy governing their use.

Control: 0588; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a policy governing the use of fax machines and MFDs.

Sending fax messages

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a sensitive or classified fax message, it can no longer be trusted when connected directly to unsecured telecommunications infrastructure or the PSTN. For example, if a fax machine fails to send a sensitive or classified fax message the device will continue attempting to send the fax message even if it has been disconnected from the cryptographic device and connected directly to the PSTN. In such cases, the fax machine could then send the sensitive or classified fax message in the clear, causing a data spill.

Control: 1092; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have separate fax machines or MFDs for sending sensitive or classified and unclassified fax messages.

Control: 0241; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies sending sensitive or classified fax messages must ensure that the fax message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the PSTN.

Sending fax messages using High Assurance products

Using the correct procedure for sending a classified fax message will ensure that it is sent securely to the correct recipient.

Using the correct memory erase procedure will prevent a classified fax message being sent in the clear.

Implementing the correct procedure for establishing a secure call will prevent sending a classified fax message in the clear.

Witnessing the receipt of a fax message and powering down the receiving machine or clearing the memory after transmission will prevent someone without a need–to–know from accessing the fax message.

Ensuring fax machines and MFDs are not connected to unsecured phone lines will prevent accidentally sending classified messages stored in memory.

Control: 0242; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies intending to use fax machines or MFDs to send classified information must comply with additional requirements in ACSI 129 and ACSI 131.

Receiving fax messages

While the communications path between fax machines and MFDs may be appropriately protected, personnel need to be aware of the need–to–know of the information that is being communicated. It is therefore important that fax messages are collected from the receiving fax machine or MFD as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

Control: 1075; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The sender of a fax message should make arrangements for the receiver to:

- collect the fax message as soon as possible after it is received
- notify the sender if the fax message does not arrive in an agreed amount of time.

Connecting MFDs to telephone networks

When an MFD is connected to a computer network and a digital telephone network the device can act as a bridge between the two. The telephone network therefore needs to be accredited to the same level as the computer network.

Control: 0244; Revision: 3; Updated: Sep-11; Applicability: G; Compliance: should not; Authority: AA
Agencies should not enable a direct connection from a MFD to a digital telephone network unless the telephone network is accredited to at least the same level as the computer network to which the device is connected.

Control: 0245; Revision: 3; Updated: Sep-11; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not enable a direct connection from a MFD to a digital telephone network unless the telephone network is accredited to at least the same level as the computer network to which the device is connected.

Connecting MFDs to computer networks

As network connected MFDs are considered to be devices that reside on a computer network, they need to have the same security measures as other devices on the computer network.

Control: 0590; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies must ensure that:

- each MFD applies user identification, authentication and audit functions for all information communicated by that device
- these mechanisms are of similar strength to those specified for workstations on that network
- each gateway can identify and filter the information in accordance with the requirements for the export of data via a gateway.

Copying documents on MFDs

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 level higher than that of the network the device is connected to, it will cause a data spill.

Control: 0589; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not permit MFDs connected to computer networks to be used to copy documents above the sensitivity or classification of the connected network.

Observing fax machine and MFD use

Placing fax machines and MFDs in public areas can help reduce the likelihood of any suspicious use going unnoticed.

Control: 1036; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that fax machines and MFDs are located in an area where their use can be observed.

References

Specific information regarding the procedures for fax machines and MFDs attached to either a SECTERA Wireline Terminal or OMNI Terminal is found in ACSI 129 and ACSI 131.

Telephones and Telephone Systems

Objective

Telephone systems are prevented from communicating unauthorised information.

Scope

This section describes the secure use of fixed telephones, including cordless telephones, as well as the systems they use to communicate information.

Context

Information regarding mobile phones is covered in the *Mobile Devices* section of the *Working Off–Site* chapter while information regarding IP telephony, including Voice over Internet Protocol (VoIP), and encryption of data in transit is covered in the *Video Conferencing and Internet Protocol Telephony* section of the *Network Security* chapter and the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Telephones and telephone systems usage policy

All non–secure telephone networks are subject to interception. Accidentally or maliciously revealing sensitive or classified information over a public telephone network can lead to interception.

Control: 1078; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a policy governing the use of telephones and telephone systems.

Personnel awareness

As there is a high risk of unintended disclosure of sensitive or classified information when using telephones, it is important that personnel are made aware of what they can discuss on particular telephone systems, as well as the audio security risk associated with the use of telephones.

Control: 0229; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must advise personnel of the permitted sensitive or classified information that can be discussed on both internal and external telephone connections.

Control: 0230; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should advise personnel of the audio security risk posed by using telephones in areas where sensitive or classified conversations can occur.

Visual indication

When single telephone systems are approved to hold conversations at different levels, alerting the user to the sensitive or classified information that can be discussed will assist in reducing the risk of unintended disclosure of sensitive or classified information.

Control: 0231; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
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.

Use of telephone systems

When sensitive or classified conversations are to be held using telephone systems, the conversation needs to be appropriately protected through the use of encryption measures.

Control: 0232; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies intending to use telephone systems for the transmission of sensitive or classified information must ensure that:

- the system has been accredited for the purpose
- all sensitive or classified traffic that passes over external systems is appropriately encrypted.

Cordless telephones

Cordless telephones have minimal transmission security and are susceptible to interception. Using cordless telephones for sensitive or classified communications can result in disclosure of information to an unauthorised party through interception.

Control: 0233; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use cordless telephones for sensitive or classified conversations.

Cordless telephones with secure telephony devices

As the data between cordless handsets and base stations is not appropriately secured, using cordless telephones for sensitive or classified communications can result in unauthorised disclosure of the information, even if the device is connected to a secure telephony device.

Control: 0234; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use cordless telephones in conjunction with secure telephony devices.

Speakerphones

As speakerphones are designed to pick up and transmit conversations in the vicinity of the device, using speakerphones in TOP SECRET areas presents a high audio security risk. However, if the agency is able to reduce the audio security risk through the use of an audio secure room that is secured during conversations, then they may be used. For physical security measures regarding Security Zone requirements refer to the *Australian Government Physical Security Management Protocol.*

Control: 0235; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not use speakerphones on telephones in TOP SECRET areas unless:

- it is located in a room rated as audio secure
- the room is audio secure during any conversations
- only personnel involved in discussions are present in the room.

Off–hook audio protection

Providing off–hook security minimises the chance of sensitive and classified conversations being accidentally coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat.

Simply providing an off–hook audio protection feature is not sufficient to meet the requirement for its use. To ensure that the protection feature is used appropriately, personnel need to be made aware of the protection feature and trained in its proper use.

Control: 0236; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should ensure that off–hook audio protection features are used on all telephones that are not accredited for the transmission of sensitive or classified information in areas where such information could be discussed.

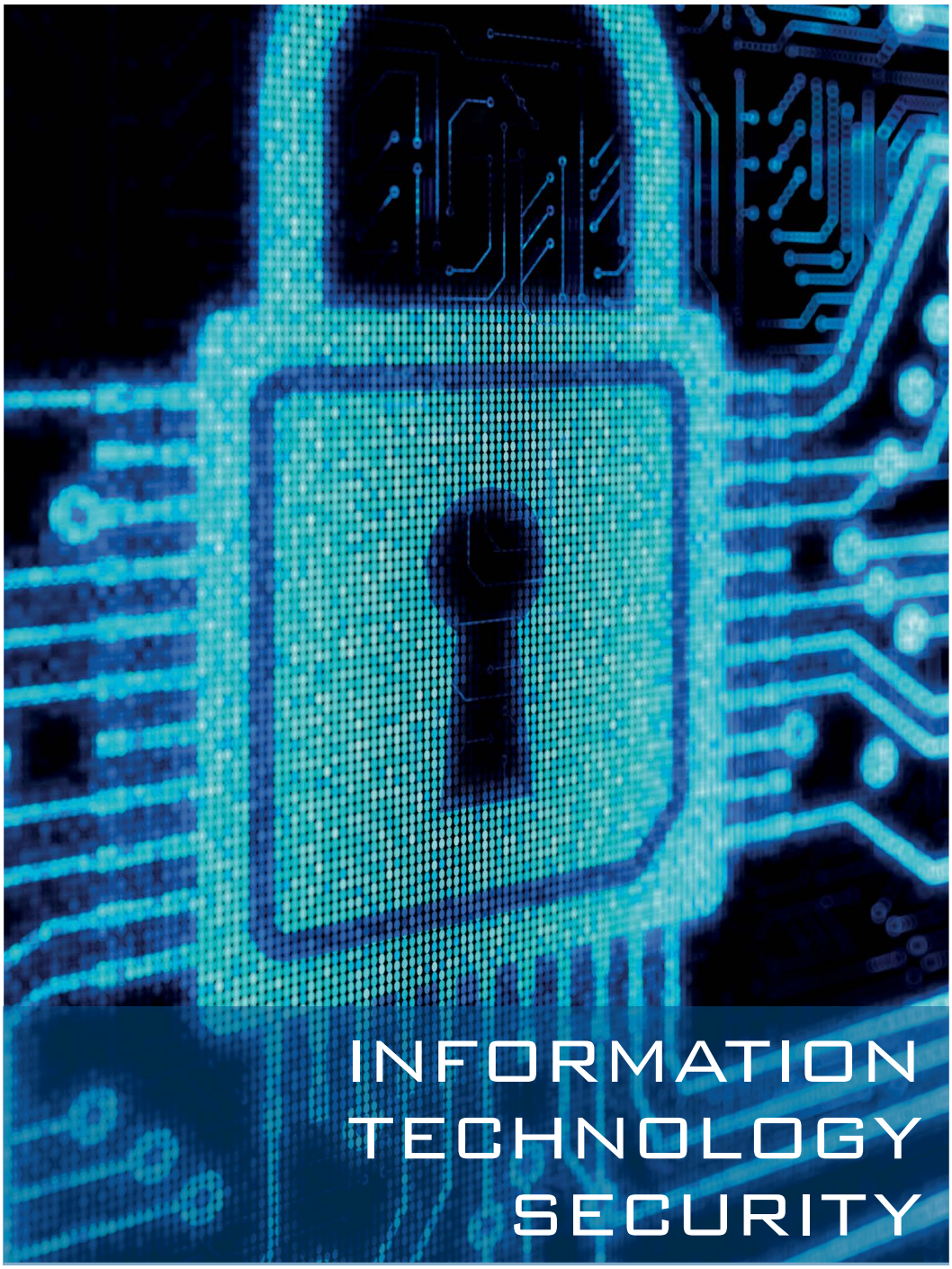
Control: 0931; Revision: 3; Updated: Sep-11; Applicability: S; Compliance: should; Authority: AA
Agencies should use push–to–talk handsets in open areas, and where telephones are shared.

Control: 0237; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must; Authority: AA
Agencies must ensure that off–hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

Control: 0238; Revision: 0; Updated: Sep-08; Applicability: TS; Compliance: should; Authority: AA
Agencies should use push–to–talk handsets to meet the requirement for off–hook audio protection.

References

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*


INFORMATION
TECHNOLOGY
SECURITY

Information Technology Security

PSPF Mandatory Requirement INFOSEC 4 Explained

Objective

Key technical measures are in place to prevent targeted cyber intrusions.

Scope

This section outlines the ISM controls for which compliance is required by the *Australian Government Protective Security Policy Framework* (PSPF). It provides agencies with a guide to determining the applicability of the mandatory requirement based on the specific risks agencies are trying to mitigate.

Context

PSPF mandatory requirement INFOSEC 4 requires agencies to implement the *Strategies to Mitigate Targeted Cyber Intrusions* (the Strategies) as outlined in this manual. To satisfy INFOSEC 4, agencies are required to implement the Top 4 Strategies. The implementation of the remaining Strategies is also strongly recommended, however agencies can prioritise these depending on business requirements and the risk profile of each system.

The Top 4 Strategies are:

1. application whitelisting
2. patch applications
3. patch operating systems
4. minimise administrative privileges.

Compliance reporting against PSPF mandatory requirements must be provided to relevant Ministers annually in accordance with PSPF requirements.

Applicability and implementation priority

The applicability of ASD's Top 4 Strategies should be determined by the specific risks agencies are trying to mitigate. The Strategies are directed at the most common cyber threat being faced by Australian government agencies at this point in time: targeted cyber intrusions from the Internet to the workstation. These intrusions purposefully target specific government agencies, seeking to gain access to sensitive information through content–based intrusions (i.e. email and web pages). These intrusions easily bypass perimeter defences, because they look like legitimate business traffic, to gain access to the workstation. From the workstation they spread, gaining access to other computing and network resources and the data they contain.

The Strategies are designed with this scenario in mind. They form part of a layered defence primarily designed to protect the workstation, and by extension the corporate network.

Priority for implementing the Top 4 Strategies should therefore be placed on Australian government systems that are able to receive emails or browse web content originating from a different security domain, particularly from the Internet.

Other systems will benefit from implementing the Top 4, and the Top 35 Strategies more broadly, however there may be circumstances where the risks or business impact of implementing the Strategies outweighs the benefit, and other security controls may have greater relevance. In such circumstances, agencies should apply appropriate risk management practices as outlined in this manual.

Further information on risk management can be found in the *Information Security Risk Management* chapter.

Controls

The Top 4 mandatory controls

Existing ISM controls satisfy the mandatory requirement to implement ASD's Top 4 Strategies.

Note: Some controls are duplicated between 'patch applications' and 'patch operating systems' as they satisfy both strategies.

Implementation of the Top 4 controls is mandatory for all systems able to receive emails or browse web content originating in a different security domain. Under the PSPF, non–compliance with any mandatory requirements must be reported to an agency's relevant portfolio Minister, and also to ASD for matters relating to the ISM.

Control: 1353; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies, at a minimum, must implement the controls indicated in the following table on all systems able to receive emails or browse web content originating in a different security domain.

TOP 4 CONTROLS		
Mitigation strategy	**Chapter and section of ISM**	**Control numbers**
Application whitelisting	Software Security—Application Whitelisting	0843, 0845, 0846, 0848, 0849
Patch applications	Software Security—Standard Operating Environments	0300, 0303, 0304, 0940, 0941 1143, 1144, 1348, 1349
Patch operating systems	Software Security—Standard Operating Environments	0300, 0303, 0304, 0940, 0941, 1143, 1144, 1348, 1350, 1351
Minimise administrative privileges	Access Control—Privileged Access	0445, 1175
	Personnel Security for Systems—Authorisations, Security Clearances and Briefings	0405

However, some technologies and systems may lack functionality or available products to feasibly implement the mandatory controls as specified in this manual. For example, implementing the Top 4 on mobile devices can be achieved using platform–specific controls which meet the general principles behind the Top 4 (described in ASD publication *Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)*. In circumstances where the Top 4 mandatory controls cannot be implemented, and no product–specific guidance exists, agencies should apply appropriate risk management practices as outlined in this manual.

Control: 1354; Revision: 0; Updated: Apr-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must adopt a risk–management approach and implement alternative security controls for:

- technologies which lack available software to enforce the mandatory controls
- scenarios or circumstances which prevent enforcement of the mandatory controls.

Other applicable controls

The following controls relate to the Top 4 Strategies. Although not considered mandatory under the PSPF requirement INFOSEC 4, these controls are best–practice for a Top 4 implementation and complement the mandatory controls listed above. Agencies may take a risk–based approach to these controls, as is the norm for the ISM. See each control for compliance and authority information.

OTHER APPLICABLE CONTROLS		
Mitigation strategy	**Chapter and section of ISM**	**Control numbers**
Application whitelisting	Software Security—Application Whitelisting	0851, 0955, 0956, 0957
Patch applications	Software Security—Standard Operating Environments	0297, 0298
Patch operating systems	Software Security—Standard Operating Environments	0297, 0298
Minimise administrative privileges	Access Control—Privileged Access	0446, 0447, 0448
	Access Control—Remote Access	0985, 0709
	Personnel Security for Systems—Authorisations, Security Clearances and Briefings	0407

Compliance reporting

Under the PSPF, non–compliance with any mandatory requirements must be reported to an agency's relevant portfolio Minister, and also to ASD for matters relating to the ISM. Compliance reporting to the relevant portfolio Minister is not designed to be an extra step in the system accreditation process, nor is it assumed compliance must be gained before authority to operate can be granted to a system.

ASD, along with the Attorney–General's Department, is responsible for assessing and reporting on Australian government agency implementation of the Top 4 controls and their overarching strategies. ASD intends to conduct an annual survey to collate more detailed information from agencies to help meet new reporting requirements.

Control: 1355; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must provide information relating to implementation of the mandatory ISM controls upon request from ASD.

References

Further information on the Strategies can be found in the following ASD Protect publications available through the OnSecure portal and the ASD website at: http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

- *Strategies to Mitigate Targeted Cyber Intrusions*
- *Strategies to Mitigate Targeted Cyber Intrusions—Mitigation Details*
- *Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained*
- *The Top 4 in a Linux Environment*
- *Application Whitelisting Explained*
- *Assessing Vulnerabilities and Patches*
- *Minimising Administrative Privileges Explained.*

Further guidance on protective security policy and the *Australian Government Protective Security Policy Framework* is available at http://www.protectivesecurity.gov.au.

Product Security

Product Selection and Acquisition

Objective

Products providing security functions for the protection of information are formally evaluated.

Scope

This section describes product evaluation and its role in the selection and acquisition of products that provide security functionality. It does not describe selecting or acquiring physical security products.

Agencies selecting products that do not provide a security function, or selecting products whose security functions will not be used and are disabled, do not need to comply with these requirements.

Context

Agencies need confidence that products perform as claimed by the vendor and provide the security necessary to mitigate contemporary threats. This confidence is best achieved through a formal, and impartial, evaluation of the product by an independent entity. ASD manages and operates a number of evaluation programs and the results are listed on the Evaluated Products List (EPL).

ASD Evaluation Programs

This security evaluation is performed by several means:

- The Common Criteria scheme through the Australasian Information Security Evaluation Program (AISEP) using licensed commercial facilities to perform evaluation of products.
- Cryptographic product evaluations called an ASD Cryptographic Evaluation (ACE) for products which contain cryptographic functions.
- The High Assurance evaluation program for assessment of products protecting highly classified information.

These programs have been established to manage the different characteristics of families of security enforcing technologies.

The Evaluated Products List

ASD maintains a list of products that have been formally and independently evaluated on the EPL, which can be found via the ASD website at http://www.asd.gov.au/infosec/epl.

Through the AISEP, ASD recognises evaluations from foreign Common Criteria schemes with equal standing. These products are listed on the Common Criteria portal can be found at http://www.commoncriteriaportal.org.

The product listing on the EPL will also include important evaluation documentation that will provide specific requirements and guidance on the secure use of the product.

In cases where an agency finds that a product they wish to use is not evaluated, agencies can recommend to ASD that the product be evaluated through a letter of recommendation. In the case of a Common Criteria evaluation, this will be either against an approved Protection Profile, where one exists, or up to maximum of an EAL 2.

Protection Profiles

To assist agencies in selecting appropriate security products, ASD has introduced approved Protection Profiles for specific technologies. A Protection Profile is a document that stipulates the security functionality that must be included in a Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be taken to assess the security function of a product. Agencies can have confidence that a product evaluated against a ASD approved Protection Profile does address the defined threats in the required manner. ASD approved Protection Profiles are published on the ASD web site.

Products entered into the AISEP for evaluation against a ASD approved Protection Profile will be given the highest priority for evaluation. The aim is for these evaluations to take less time than those against the traditional criteria, which will enable the AISEP to keep pace with evaluating current security products and updates.

Cryptographic security functionality is also included in the scope of products evaluated against a ASD approved Protection Profile. ASD is currently establishing cryptographic testing as part of the AISEP Common Criteria evaluations. When this is established, evaluations against a ASD approved Protection Profile may undergo a simplified ACE process. This will assist in reducing the completion time taken to perform the evaluation.

To facilitate the transition to ASD approved Protection Profiles, a cap of Evaluation Assurance Level (EAL) 2 applies for all traditional EAL based evaluations performed in the AISEP, including those technologies with no existing ASD approved Protection Profile. EAL 2 represents the best balance between completion time and meaningful security assurance gains. Evaluations conducted in other nations' Common Criteria schemes will still be recognised by ASD.

Controls

Product selection

Agencies can determine that an evaluated product from the EPL or the Common Criteria portal is suitable by reviewing its evaluation documentation. This documentation includes the Protection Profile or Security Target, Certification Report and Consumer Guide. In particular, agencies need to determine if the scope or target of evaluation (including security functionality and the operational environment) is suitable for their needs.

When selecting a product with security functionality, whether it has or has not been evaluated, it is imperative that agencies implement best practice security measures. New vulnerabilities are regularly discovered in products. For this reason, even evaluated products from the EPL will need to have a program of continuous security management.

For Protection Profile evaluated products, the scope of the evaluation has been predefined to meet minimum security requirements for the given technology area.

Products that are in evaluation will not yet have published evaluation documentation. For a Common Criteria evaluation, a draft Security Target can be obtained from ASD for products that are in evaluation through the AISEP. For products that are in evaluation through a foreign scheme, the product vendor can be contacted directly for further information.

Control: 0279; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should select products that have their desired security functionality in the scope of the product's evaluation and are applicable to the intended environment.

Product selection preference order

A Common Criteria evaluation is traditionally conducted at a specified EAL. However, ASD approved Protection Profiles evaluations exist outside of this scale.

While products evaluated against an ASD approved Protection Profile will fulfil the Common Criteria EAL requirements, the EAL number will not be published on the EPL. This is intended to facilitate the transition from EAL numbering to ASD approved Protection Profiles.

Control: 0280; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must select a product with the required security functionality that has completed an ASD approved Protection Profile evaluation in preference to one that has completed an EAL–based evaluation.

If agencies select a product that has not completed an evaluation, documenting this decision, assessing the security risks and accepting these risks ensures the decision is appropriate for an agency's business requirements and risk profile.

Control: 0282; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must not use unevaluated products, unless the risks have been appropriately accepted and documented.

Product specific requirements and evaluation documentation

As products move toward greater convergence and inter–connectivity, more require third party hardware or software to operate, which may introduce new vulnerabilities which are outside evaluation scope. Documentation associated with each evaluation can assist agencies in determining exactly what the evaluation covered and any recommendations for the product's secure use.

Evaluation documentation, provided on the EPL, gives specific guidance on evaluated product use. Documentation may also contain specific requirements for the evaluated product which take precedence over those in this manual.

Product specific requirements may also be produced for cross domain solutions and High Assurance products.

Control: 0463; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must check product evaluation documentation, where available, to determine any product specific requirements.

Control: 0464; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with all product specific requirements outlined in product evaluation documentation.

Control: 0283; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies selecting cross domain solutions or High Assurance products must contact ASD and comply with any product specific requirements.

Control: 1342; Revision: 1; Updated: Apr-13; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must comply with specific guidance on cross domain solutions and High Assurance products for handling information classified CONFIDENTIAL and above.

Technology convergence

Convergence is the integration of a number of discrete technologies into one product, such as mobile devices that integrate voice and data services. Converged solutions can include the advantages of each technology but can also present the vulnerabilities of each discrete technology at the same time. Furthermore, some vulnerabilities may be unique to converged products due to the combination of technologies present in the product and their interaction with each other. When products have converged elements, the relevant areas of this manual for each of the discrete elements are applicable.

Control: 1343; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When using products with converged elements, agencies must apply the relevant sections of this manual for each discrete element.

Delivery of products

It is important that agencies ensure that the product that is intended for use is the actual product that is received. For evaluated products, if the product received differs from the evaluated version, then the assurance gained from any evaluation may not necessarily apply. For unevaluated products that do not have evaluated delivery procedures, it is recommended agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

Other factors to consider when assessing delivery procedures include:

- the intended environment of the product
- the types of intrusions that the product will defend against
- the resources of any potential intruders
- the likelihood of an intrusion
- the importance of maintaining confidentiality of the product purchase
- the importance of ensuring adherence to delivery time frames.

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. Examples of other secure delivery procedures can include tamper evident seals, cryptographic checksums and signatures, and secure transportation.

Agencies will also need to confirm the integrity of the software that has been delivered before deploying it on an operational system to ensure that no unintended software is installed at the same time. Software delivered on physical media, and software delivered over the Internet, could contain malicious code or malicious content that is installed along with the legitimate software.

Control: 0285; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

Control: 0286; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies procuring High Assurance products must contact ASD and comply with any product specific delivery procedures.

Control: 0937; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should 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 in an unaltered state.

Control: 0284; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- verify the integrity of software using vendor supplied checksums when available
- validate the software's interaction with the operating system and network in a test environment prior to use on operational systems.

Leasing arrangements

Agencies should consider security and policy requirements when entering into a leasing agreement for products in order to avoid potential cyber security incidents during maintenance, repairs or disposal processes.

Control: 0287; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that leasing agreements for products take into account the:

- difficulties that could be encountered when the product needs maintenance
- difficulties that could be encountered in sanitising a product before returning it
- the possible requirement for destruction if sanitisation cannot be performed.

Ongoing maintenance of assurance

Developers that have demonstrated a commitment to continuous evaluation of product versions are more likely to ensure that security updates and changes are independently assessed.

A developer's commitment to continuity of assurance can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

Control: 0938; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should choose products from developers that have made a commitment to the continuing maintenance of the assurance of their product.

References

Additional information on the EPL, AISEP, Protection Profiles and the Common Criteria can be found at:

http://www.asd.gov.au/infosec/epl.htm
http://www.asd.gov.au/infosec/aisep.htm
http://www.commoncriteriaportal.org/
http://www.commoncriteriaportal.org/schemes.html.

Product Installation and Configuration

Objective

Products are installed and configured using best practice security.

Scope

This section describes installing and configuring evaluated products that provide security functionality. It does not describe installing and configuring general products or physical security products.

Context

Evaluated configuration

An evaluated product is considered to be operating in its evaluated configuration if:

- functionality that it uses was in the scope or target of evaluation and it is implemented in the specified manner
- only product updates that have been assessed through a formal assurance continuity process have been applied
- the environment complies with assumptions or organisational security policies stated in the product's Security Target or similar document.

Unevaluated configuration

An evaluated product is considered to be operating in an unevaluated configuration when it does not meet the requirements of the evaluated configuration and guidance provided from the Certification Report.

Patching evaluated products

Agencies need to consider that evaluated products may have had patches applied since the time they were evaluated. In the majority of cases, the latest patched product version is more secure than the older evaluated product version. While the application of security patches will normally not place a product in an unevaluated configuration, some product vendors incorporate new functionality with security patches, which have not been evaluated. In such cases agencies will need to use their judgement to determine whether the product remains in an evaluated configuration or whether sufficiently new functionality has been incorporated into the product such that it no longer remains in an evaluated configuration.

Controls

Installation and configuration of evaluated products

Evaluation of products provides assurance that the product will work as expected in a clearly defined configuration. The scope or target of evaluation specifies the security functionality that can be used and how the product is configured and operated.

Using an evaluated product in a manner for which it was not intended could result in the introduction of new vulnerabilities that were not considered as part of the evaluation.

For products evaluated under the Common Criteria scheme, information is available from the product vendor regarding the product's installation, administration and use. Additional information is available in the Security Target and Certification Report. Configuration guidance for High Assurance products can be obtained from ASD.

Control: 0289; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

Control: 0290; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must ensure that High Assurance products are installed, configured, operated and administered in accordance with all product specific guidance produced by ASD.

Use of evaluated products in unevaluated configurations

When using a product in a manner for which it was not intended, a security risk assessment must be conducted upon the unevaluated configuration. The further a product deviates from its evaluated configuration, the less assurance can be gained from the evaluation.

Given the potential threat vectors and the value of the information being protected, High Assurance products must be configured in accordance with ASD's guidance.

Control: 0291; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies wishing to use an evaluated product in an unevaluated configuration must undertake a security risk assessment including:

- the necessity of the unevaluated configuration
- testing of the unevaluated configuration in the agency's environment
- new vulnerabilities introduced due to the product being used outside of its evaluated configuration.

Control: 0292; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must not; Authority: ASD
High Assurance products must not be used in an unevaluated configuration.

References

Nil.

Product Classifying and Labelling

Objective

Products and ICT equipment are classified and appropriately labelled.

Scope

This section describes classifying and labelling of both evaluated products and general ICT equipment.

Context

Non–essential labels

Non–essential labels are labels other than protective marking and asset labels.

Controls

Classifying ICT equipment

When media is used in ICT equipment there is no guarantee that the equipment has not automatically accessed information from the media and stored it locally without the knowledge of the user. The ICT equipment therefore needs to be afforded the same degree of protection as that of the associated media.

Control: 0293; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must classify ICT equipment based on the sensitivity or classification of information for which the equipment and any associated media in the equipment are approved for processing, storing or communicating.

Labelling ICT equipment

The purpose of applying protective markings to all ICT equipment in an area is to reduce the likelihood that a user will accidentally input sensitive or classified information into another system residing in the same area that is not accredited to handle that information.

Applying protective markings to assets helps determine the appropriate sanitisation, disposal or destruction requirements of the ICT equipment based on its sensitivity or classification.

Control: 0294; Revision: 3; Updated: Apr-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must clearly label all ICT equipment capable of storing information, with the exception of High Assurance products, with the appropriate protective marking.

Control: 1168; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When using non–textual protective markings for ICT equipment due to operational security reasons, agencies must document the labelling scheme and train personnel appropriately.

Labelling High Assurance products

High Assurance products often have tamper–evident seals placed on their external surfaces. To assist users in noticing changes to the seals, and to prevent functionality being degraded, agencies must only place seals on equipment when approved by ASD to do so.

Control: 0296; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must seek ASD authorisation before applying labels to external surfaces of High Assurance products.

References

Nil.

Product Maintenance and Repairs

Objective

Products and ICT equipment are repaired by cleared or appropriately escorted personnel.

Scope

This section describes maintaining and repairing of both evaluated products and general ICT equipment.

Context

Information relating to the sanitisation of ICT equipment and media can be found in the *Product Sanitisation and Disposal* section of this chapter and the *Media Sanitisation* section of the *Media Security* chapter.

Controls

Maintenance and repairs

Making unauthorised repairs to products and ICT equipment could impact the integrity of the product or equipment.

Using cleared technicians on–site is considered the most desired approach to maintaining and repairing ICT equipment. This ensures that if sensitive or classified information is disclosed during the course of maintenance or repairs the technicians are aware of the protection requirements for the information.

Control: 1079; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must have ASD approval before undertaking any repairs to High Assurance products.

Control: 0305; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where possible, maintenance and repairs for ICT equipment should be carried out on–site by an appropriately cleared technician.

Maintenance and repairs by an uncleared technician

Agencies choosing to use uncleared technicians to maintain or repair ICT equipment need to be aware of the requirement for cleared personnel to escort the uncleared technicians during maintenance or repair activities.

Control: 0307; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, agencies should sanitise and reclassify or declassify the equipment and associated media before maintenance or repair work is undertaken.

Control: 0306; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician must be escorted by someone who:

- is appropriately cleared and briefed
- takes due care to ensure that sensitive or classified information is not disclosed
- takes all responsible measures to ensure the integrity of the equipment
- has the authority to direct the technician.

Control: 0308; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that the ratio of escorts to uncleared technicians allows for appropriate oversight of all activities.

Control: 0943; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician should be escorted by someone who is sufficiently familiar with the equipment to understand the work being performed.

Off–site maintenance and repairs

Agencies choosing to have ICT equipment maintained or repaired off–site need to be aware of requirements for the company's off–site facilities to be approved to process and store the products at an appropriate level as specified by the *Australian Government Physical Security Management Protocol.*

Agencies choosing to have ICT equipment maintained or repaired off–site can sanitise and reclassify or declassify the equipment prior to transport and subsequent maintenance or repair activities to lower the physical transfer, processing and storage requirements specified by the *Australian Government Information Security Management Protocol* and *Australian Government Physical Security Management Protocol.*

Control: 0310; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies having ICT equipment maintained or repaired off–site must ensure that the physical transfer, processing and storage requirements are appropriate for the sensitivity or classification of the equipment and that procedures are complied with at all times.

Maintenance and repair of ICT equipment from secured spaces

When ICT equipment resides in an area that also contains ICT equipment of a higher classification, a technician could modify the lower classified ICT equipment in an attempt to compromise co–located ICT equipment of a higher classification.

Control: 0944; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies having ICT equipment maintained or repaired off–site should treat the equipment as per the requirements for the highest classification processed, stored or communicated in the area that the equipment will be returned to.

References

Nil.

Product Sanitisation and Disposal

Objective

Products and ICT equipment are sanitised and disposed of in an approved manner.

Scope

This section describes sanitising and disposing of both evaluated products and general ICT equipment. This is applicable to any ICT hardware equipment capable of storing data, regardless of whether the data storage ability of the item in question is temporary or permanent in nature.

This chapter does not provide guidance on sanitisation or disposal of High Assurance or TEMPEST rated ICT equipment.

Context

Additional information on the sanitisation, destruction and disposal of media can be found in the *Media Security* chapter.

Sanitisation removes data from storage media, so that there is complete confidence the data will not be retrieved and reconstructed.

With the convergence of technology, sanitisation requirements are becoming increasingly complex. For example, some televisions and even electronic whiteboards now contain non–volatile media.

When sanitising and disposing of ICT equipment, it is the storage media component of the equipment which must be sanitised.

Disposal of ICT equipment can also include recycling, reusing or donating ICT equipment.

Media typically found in ICT equipment includes:

- electrostatic memory devices such as laser printer cartridges, MFD and Multifunction Printers (MFP)
- non–volatile magnetic memory such as hard disks and solid state drives
- non–volatile semiconductor memory such as flash cards
- volatile memory such as RAM sticks.

Controls

Disposal of ICT equipment

When disposing of ICT equipment, agencies need to sanitise any media in the equipment that is capable of storing sensitive or classified information, remove the media from the equipment and dispose of it separately or destroy the equipment in its entirety. Removing labels and markings indicating the classification, codewords, caveats and owner details will ensure the sanitised unit does not display indications of its prior use.

Once the media in ICT equipment has been sanitised or removed, the equipment can be considered sanitised. Following subsequent declassification approval from the owner of the information previously processed by the ICT equipment, it can be disposed of into the public domain or disposed of through unclassified material waste management services.

ASD provides specific advice on how to securely dispose of High Assurance products and TEMPEST rated ICT equipment. There are a number of security risks that can arise due to improper disposal including providing an intruder with an opportunity to gain insight into government capabilities.

ICT equipment located overseas that has processed or stored AUSTEO and AGAO material has more severe consequences for Australian interests if not sanitised and disposed of appropriately. Taking appropriate steps will assist in providing complete assurance that caveated information on ICT equipment is not recoverable.

Control: 0313; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a documented process for the disposal of ICT equipment.

Control: 0311; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When disposing of ICT equipment containing sensitive or classified media, agencies must sanitise the equipment by either:

- sanitising the media within the equipment
- removing the media from the equipment and disposing of it separately
- destroying the equipment in its entirety.

Control: 1217; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When disposing of ICT equipment, agencies must remove labels and markings indicating the classification, codewords, caveats, owner, system or network name, or any other marking that can associate the equipment with its original use.

Control: 0315; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must contact ASD and comply with any requirements for the disposal of High Assurance products.

Control: 0321; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must contact ASD and comply with any requirements for disposing of TEMPEST rated ICT equipment.

Control: 1218; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: should; Authority: AA
ICT equipment and associated media that is located overseas and has processed or stored AUSTEO or AGAO information should be sanitised in situ where possible.

Control: 0312; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
ICT equipment and associated media that is located overseas and has processed or stored AUSTEO or AGAO information that cannot be sanitised must be returned to Australia for destruction.

Control: 0316; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must formally authorise the disposal of ICT equipment, or waste, into the public domain.

Sanitising printers and MFDs

Printing random text with no blank areas on each colour printer cartridge or MFD print drum ensures that no residual information exists within the print path. ASD is able to, upon request, provide a suitable sanitisation file to use.

Control: 0317; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must print at least three pages of random text with no blank areas on each colour printer cartridge or MFD print drum.

When sanitising and disposing of the entire printer or MFD, extra steps must be taken to ensure no residual sensitive or classified information is left on the unit. The printer cartridge or MFD print drum should be sanitised as described above, with the additional following controls.

For sanitisation and disposal of any hard disk drives present in the printer or MFD, see the *Media Security* chapter.

Transfer rollers and platens can become imprinted with text and images over time, which could allow an intruder to retrieve information after the unit has been decommissioned from use. (In the case of a flatbed scanner, photocopier or MFD, the glass where a document is placed is the platen.) Similarly, paper jammed in the paper path provides a similar risk of retrieval of information after disposal.

Control: 1219; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should inspect MFD print drums and image transfer rollers and:

- remove any remnant toner with a soft cloth
- destroy if there is remnant toner which cannot be removed
- destroy if a print is visible on the image transfer roller.

Control: 1220; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must inspect photocopier or MFD platens and destroy them if any images are retained on the platen.

Control: 1221; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must inspect all paper paths and remove all paper from the printer or MFD, including paper that may have jammed inside the unit.

Printers and photocopiers can then be considered sanitised, and may be disposed of through unclassified material waste management services.

Destroying printer cartridges and MFD print drums

When printer cartridges and MFD print drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them. Printer ribbons cannot be sanitised and must be destroyed.

Control: 0318; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies unable to sanitise printer cartridges or MFD print drums must destroy the cartridge or MFD print drum in accordance with the requirements for electrostatic memory devices.

Sanitising televisions and computer monitors

All types of televisions and computer monitors are capable of retaining information on the screen if appropriate mitigation measures are not taken during the lifetime of the screen. Cathode Ray Tube (CRT) monitors and plasma screens can be affected by burn–in, while Liquid Crystal Display (LCD) screens can be affected by image persistence.

Control: 0319; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must visually inspect televisions and computer monitors by turning up the brightness and contrast to the maximum level to determine if any information has been burnt into or persists on the screen.

Control: 1076; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must attempt to sanitise televisions and computer monitors with minor burn–in or image persistence by displaying a solid white image on the screen for an extended period of time.

If burn–in or image persistence is removed through these measures, televisions and computer monitors can then be considered sanitised, and may be disposed of through unclassified waste management services.

If burn–in or persistence is not removed through these measures, televisions and computer monitors cannot be sanitised and must be destroyed.

If the television or computer monitor cannot be powered on (e.g. due to a faulty power supply) the unit cannot be sanitised and must be destroyed. Additionally, if the screen retains a compromising burnt–in image, the unit must be destroyed.

Control: 1222; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must destroy televisions and computer monitors that cannot be sanitised.

Sanitising network devices

Routers, switches, network interface cards and firewalls contain memory which is used in the operation of the network device. Resetting the device and loading a dummy config (or equivalent) will exercise the device memory and provide a read back to verify the reset was successful.

Control: 1223; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
To sanitise network devices, agencies must perform a full reset and load a dummy config file to confirm the reset was successful.

Sanitising fax machines

Faxmachines store information such as phone number directories and stored pages ready for transmission. Sanitising faxmachines ensures no residual information exists on the unit.

For sanitisation of non–volatile media, see the *Media Security* chapter.

Control: 1224; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise or destroy memory (such as phone number directories and pages stored for transmission) from the fax machine.

Control: 1225; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should remove the paper tray of the fax machine and transmit an unclassified fax with a minimum length of four pages. The paper tray should then be re–installed to allow the fax summary page to be printed.

Control: 1226; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must check fax machines to ensure no pages are trapped in the paper path due to a paper jam.

References

Nil.

Media Security

Media Handling

Objective

Media is appropriately classified and labelled.

Scope

This section describes classifying and labelling media.

Context

Information relating to classifying and labelling ICT equipment can be found in the *Product Classifying and Labelling* section of the *Product Security* chapter. Information on accounting for ICT media can be found in the *ICT Equipment and Media* section of the *Physical Security* chapter.

Controls

Removable media policy

Establishing an agency removable media policy will allow sound oversight and accountability of agency information transported or transferred between systems on removable media.

A well–enforced media policy can decrease the likelihood and consequence of accidental data spills and information theft or loss.

This policy could form part of broader risk management or policy documents of the agency.

Control: 1359; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should have a removable media policy that includes:

- details of the authority for removable media within an agency
- media registration and accounting requirements
- media classification requirements
- the types of media permitted within the agency
- explicit cases where removable media is approved for use
- requirements for the use of media
- requirements for disposal of media.

Reclassification and declassification procedures

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
- the intended destination of the media.

Control: 0322; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the reclassification and declassification of media.

Classifying media storing information

Media that is not correctly classified could be stored, identified and handled inappropriately or accessed by a person who does not have the appropriate security clearance.

Control: 0323; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must classify media to the highest sensitivity or classification stored on the media since any previous reclassification.

Classifying media connected to systems

There is no guarantee that sensitive or classified information has not been copied to media while connected to a system unless either read–only devices or read–only media are used.

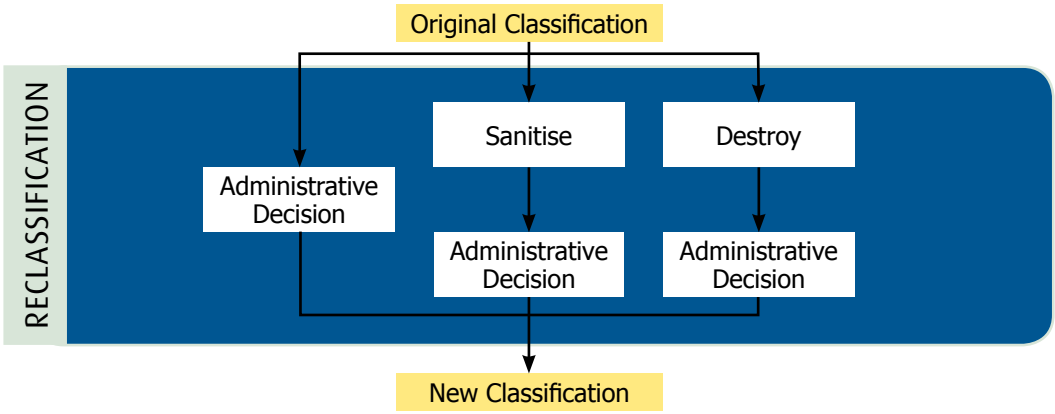
Control: 0325; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must classify any media connected to a system the same sensitivity or classification as the system, unless either:

- the media is read–only
- the media is inserted into a read–only device
- the system has a mechanism through which read–only access can be assured.

Reclassifying media

The media will always need to be protected according to the sensitivity or classification of the information it stores. If the sensitivity or classification of the information on the media changes, then so will the protection afforded to the media.

The following diagram shows an overview of the mandated reclassification process.



Control: 0330; Revision: 2; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies wishing to reclassify media to a lower classification must ensure that:

- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed
- a formal administrative decision is made to reclassify the media.

Control: 0331; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must reclassify media if either:

- information copied onto the media is of a higher classification than the sensitivity or classification of the information already on the media
- information contained on the media is subjected to a classification upgrade.

Labelling media

Labelling helps personnel to identify the sensitivity or classification of media and ensure that they apply appropriate security measures when handling or using it.

Control: 0332; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should label media with a marking that indicates the sensitivity or classification applicable to the information it stores; unless it is internally mounted fixed media and the ICT equipment containing the media is labelled.

Control: 0333; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the sensitivity or classification of all media is easily visually identifiable.

Control: 0334; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When using non–textual protective markings for media due to operational security reasons, agencies must document the labelling scheme and train personnel appropriately.

Labelling sanitised media

It is not possible to apply the sanitisation and reclassification process to non–volatile media in a cascaded manner. Therefore, SECRET media that has been sanitised and reclassified to a CONFIDENTIAL level must be labelled as to avoid inadvertently being reclassified to a lower classification a second time.

Control: 0335; Revision: 3; Updated: Sep-11; Applicability: S; Compliance: must; Authority: AA
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 SECRET to CONFIDENTIAL. Further lowering of classification only via destruction.'

References

For further requirements on media security see the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Usage

Objective

Media is used with systems in a controlled and accountable manner.

Scope

This section describes the requirements needed to use media with sensitive or classified information. This section includes information on connecting media to systems, using media to transfer information and storage of media. The controls are equally applicable to all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players.

Context

Further information on using media to transfer data between systems can be found in the *Data Transfers and Content Filtering* chapter. More information on reducing storage and physical transfer requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Controls

Using media with systems

To prevent data spills agencies need to prevent sensitive or classified media from being connected to, or used with, systems not accredited to process, store or communicate the information on the media.

Control: 0337; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use media with a system that is not accredited to process, store or communicate the information on the media.

Storage of media

The requirements for the storage and physical transfer of sensitive or classified media are specified in the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework.*

Control: 0338; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that sensitive or classified media meets the minimum physical security storage requirements in the *Australian Government Protective Security Policy Framework.*

Connecting media to systems

Some operating systems provide the functionality to automatically execute certain types of programs that reside on optical media and flash drives. While this functionality was designed with a legitimate purpose in mind—such as automatically loading a graphical user interface for the user to browse the contents of the media, or to install software residing on the media—it can also be used for malicious purposes.

An intruder can create a file on media that the operating system believes it should automatically execute. When the operating system executes the file, it can have the same effect as when a user explicitly executes malicious code. However, in this case the user is taken out of the equation as the operating system executes the file without explicitly asking the user for permission.

Some operating systems will cache information on media to improve performance. Using media with a system could therefore cause data to be read from the media without user intervention.

Device access control and data loss prevention software allows greater control over media that can be connected to a system and the manner in which it can be used. This assists in preventing unauthorised media being connected to a system and, if desired, preventing information from being written to it.

Media can also be prevented from connecting to a system by physical means including, but not limited to, using wafer seals or applying epoxy to the connection ports. If physical means are used to prevent media connecting to a system, then procedures covering detection and reporting processes are needed in order to respond to attempts to bypass these controls.

Control: 0341; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable any automatic execution features in operating systems for connectable media.

Control: 0342; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must prevent unauthorised media from connecting to a system via the use of either:

- device access control or data loss prevention software
- physical means.

Control: 0343; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should prevent media being written to, via the use of device access control or data loss prevention software, if there is no business need.

External interface connections that allow Direct Memory Access

Known vulnerabilities have been demonstrated where adversaries can connect media to a locked workstation via a communications port that allows Direct Memory Access (DMA) and subsequently gain access to encryption keys in memory. Furthermore, with DMA an intruder can read or write any content to memory that they desire. The best defence against this vulnerability is to disable access to communication ports using either software controls or physically preventing access to the communication ports so that media cannot be connected. Communication ports that can connect media that use DMA are IEEE 1394 (FireWire), ExpressCard and Thunderbolt.

Control: 0344; Revision: 3; Updated: Sep-11; Applicability: G, P; Compliance: should; Authority: AA
Agencies should disable external interfaces on a system that allows DMA, if there is no business need.

Control: 0345; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must disable external interfaces on a system that allows DMA, if there is no business need.

Transferring media

As media is often transferred through areas not certified and accredited to process the sensitive or classified information on the media, protection mechanisms need to be put in place to protect that information. Applying encryption to media may reduce the requirements for storage and physical transfer as outlined in the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework*. Any reduction in requirements is based on the original sensitivity or classification of information residing on the media and the level of assurance in the cryptographic product being used to encrypt the media.

Further information on reducing storage and physical transfer requirements can be found in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Control: 0831; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that media containing sensitive or classified information meets the minimum physical transfer requirements as specified in the *Australian Government Protective Security Policy Framework.*

Control: 0832; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must encrypt media with at least a ASD Approved Cryptographic Algorithm (AACA) if it is to be transferred through an area not certified and accredited to process the sensitivity or classification of the information on the media.

Control: 1059; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should encrypt media with at least a AACA even if being transferred through an area certified and accredited to process the sensitivity or classification of the information on the media.

Using media for data transfers

Agencies transferring data between systems of different security domains, sensitivities or classifications are strongly encouraged to use write–once optical media. This will ensure that information from the one of the systems cannot be accidently transferred onto the media then onto another system when the media is reused for the next transfer.

Control: 0347; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies transferring data manually between two systems of different security domains, sensitivities or classifications should not use rewriteable media.

Media in secured areas

Ensuring certain types of media—including Universal Serial Bus (USB), FireWire, Thunderbolt and eSATA capable media—are explicitly approved in a TOP SECRET environment provides an additional level of user awareness. Additionally, using device access control software on workstations in case users are unaware of, or choose to ignore, security requirements for media provides a technical control to enforce the policy.

Control: 1169; Revision: 0; Updated: Sep-11; Applicability: S; Compliance: should not; Authority: AA
Agencies should not permit any media that uses external interface connections in a SECRET area without prior written approval from the accreditation authority.

Control: 0346; Revision: 2; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not permit any media that uses external interface connections in a TOP SECRET area without prior written approval from the accreditation authority.

References

For further requirements on media security see the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Sanitisation

Objective

Media that is no longer required is sanitised.

Scope

This section describes sanitising media.

Context

Additional information relating to sanitising ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Sanitising media

Sanitisation is the process of removing information from media. It does not automatically change the sensitivity or classification of the media, nor does it involve the destruction of media.

Product selection

Agencies are permitted to use non–evaluated products to sanitise media. However, the product still needs to conform to the requirements for sanitising media as outlined in this section.

Hybrid hard drives

When sanitising hybrid hard drives, the sanitisation and post sanitisation requirements for flash memory devices apply.

Solid state drives

When sanitising solid state drives, the sanitisation and post sanitisation requirements for flash memory devices apply.

Government systems

All references to 'Unclassified (DLM)' in the tables in this section relate to media containing unclassified but official/sensitive information not intended for public release, such as DLM information. ASD advises that government system (G) controls in the ISM are applied as a baseline to ICT equipment storing or processing Unclassified (DLM) information. Unclassified (DLM) and 'Government' are not classifications under the *Australian Government Security Classification System* as mandated by the Attorney–General's Department.

Media that cannot be sanitised

When attempts to sanitise media are unsuccessful, the only way to provide complete assurance the data is erased is to destroy the media. Additionally, some types of media cannot be sanitised and therefore must be destroyed. Refer to the *Media Destruction* section of this chapter for information on media that cannot be sanitised.

Controls

Sanitisation procedures

Sanitising media prior to reuse in a different environment ensures that information is not inadvertently accessed by unauthorised personnel or protected by insufficient security measures.

Using approved sanitisation methods provides a high level of assurance that no remnant data is left on the media.

The procedures used in this manual are designed not only to prevent common intrusions that are currently feasible but also to protect from those that could emerge in the future.

When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process completed successfully.

Control: 0348; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the sanitisation of media.

Volatile media sanitisation

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to times recommended in research on recovering the contents of volatile media.

Control: 0351; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies must sanitise volatile media by either:

- removing power from the media for at least 10 minutes
- overwriting all locations of the media with a random pattern followed by a read back for verification.

Control: 0352; Revision: 2; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise volatile media by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification, followed by removing power from the media for at least 10 minutes.

If read back cannot be achieved or classified information persists on the media, destroying the media as prescribed in the *Media Destruction* section of this chapter is the only way to provide complete assurance classified information no longer persists.

Treatment of volatile media following sanitisation

Published literature supports short–term remanence effects (residual information that remains on media after erasure) in volatile media. Data retention times are reported to be in the magnitude of minutes (at normal room temperatures) to hours (in extreme cold). 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 is required to remain at this classification, even after sanitisation.

Control: 0353; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, volatile media must be treated no less than as indicated below.

PRE–SANITISATION HANDLING	POST–SANITISATION HANDLING
TOP SECRET	Unclassified (under certain circumstances)
SECRET	Unclassified
CONFIDENTIAL	Unclassified
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Circumstances preventing reclassification of volatile media

Typical circumstances preventing the reclassification of TOP SECRET volatile media include a static cryptographic key being stored in the same memory location during every boot of a device and a static image being displayed on a device and stored in volatile media for a period of months.

Control: 0835; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Volatile media must not be reclassified below TOP SECRET if the volatile media either:

- stored sensitive, static data for an extended period of time
- sensitive data was repeatedly stored or written to the same memory location for an extended period of time.

Non–volatile magnetic media sanitisation

Both the host protected area and device configuration overlay table of non–volatile magnetic hard disks are normally not visible to the operating system or the computer's basic input/output system. Hence any sanitisation of the readable sectors on the media will not overwrite these hidden sectors leaving any information contained in these locations untouched. Some sanitisation programs include the ability to reset devices to their default state removing any host protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of the media during the subsequent sanitisation process.

Modern non–volatile magnetic hard disks automatically reallocate space for bad sectors at a hardware level. These bad sectors are maintained in what is known as the growth defects table or '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. While these sectors may be considered bad by the device, quite often this is due to the sectors no longer meeting expected performance norms for the device and not due to an inability to read/write to the sector. The Advanced Technology Attachment (ATA) secure erase command was built into the firmware of post–2001 devices and is able to access sectors that have been added to the g–list. Modern non–volatile magnetic hard disks also contain a primary defects table or 'p–list'. The p–list contains a list of bad sectors found during post–production processes. No information is ever stored in sectors on the p–list for a device as they are inaccessible before the media is used for the first time.

Control: 0354; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non–volatile magnetic media by:

- if pre–2001 or under 15 Gigabytes: overwriting the media at least three times in its entirety with a random pattern followed by a read back for verification.
- if post–2001 or over 15 Gigabytes: overwriting the media at least once in its entirety with a random pattern followed by a read back for verification.

Control: 1065; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should reset the host protected area and device configuration overlay table of non–volatile magnetic hard disks prior to overwriting the media.

Control: 1066; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should overwrite the growth defects table (g–list) on non–volatile magnetic hard disks.

Control: 1067; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the ATA secure erase command, where available, for sanitising non–volatile magnetic hard disks instead of using block overwriting software.

Control: 1068; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must boot from separate media to the media being sanitised to undertake the sanitisation process.

Treatment of non–volatile magnetic media following sanitisation

Highly classified non–volatile magnetic media cannot be sanitised below its original classification due to concerns with the sanitisation of the host protected area, device configuration overlay table and growth defects table. The sanitisation of TOP SECRET non–volatile media does not allow for the reduction of its classification.

Control: 0356; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, non–volatile magnetic media must be treated no less than as indicated below.

PRE–SANITISATION HANDLING	POST–SANITISATION HANDLING
TOP SECRET	TOP SECRET
SECRET	CONFIDENTIAL
CONFIDENTIAL	Unclassified
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Non–volatile Erasable Programmable Read–only Memory media sanitisation

When erasing non–volatile Erasable Programmable Read–only Memory (EPROM), the manufacturer's specification for ultraviolet erasure time is multiplied by a factor of three to provide an additional level of certainty in the process.

Control: 0357; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non–volatile EPROM media by erasing in accordance with 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 random pattern, followed by a readback for verification.

Non–volatile Electrically Erasable Programmable Read–only Memory media sanitisation

A single overwrite with a random pattern is considered best practice for sanitising non–volatile Electrically Erasable Programmable Read–only Memory (EEPROM) media.

Control: 0836; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non–volatile EEPROM media by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification.

Treatment of non–volatile EPROM and EEPROM media following sanitisation

As little research has been conducted on the ability to recover data on non–volatile EPROM or EEPROM media after sanitisation, highly classified media retains its original classification.

Control: 0358; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, non–volatile EPROM and EEPROM media must be treated no less than as indicated below.

PRE–SANITISATION HANDLING	POST–SANITISATION HANDLING
TOP SECRET	TOP SECRET
SECRET	CONFIDENTIAL
CONFIDENTIAL	Unclassified
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Non–volatile flash memory media sanitisation

In flash memory media, a technique called wear levelling ensures that writes are distributed evenly across each memory block in flash memory. This feature necessitates flash memory being overwritten with a random pattern twice, rather than once, as this helps ensure that all memory blocks are overwritten during sanitisation.

Control: 0359; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must sanitise non–volatile flash memory media by overwriting the media at least twice in its entirety with a random pattern, followed by a read back for verification.

Treatment of non–volatile flash memory media following sanitisation

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. This is why TOP SECRET, SECRET and CONFIDENTIAL flash memory media must always remain at their respective classification, even after sanitisation.

Control: 0360; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Following sanitisation, non–volatile flash memory media must be treated no less than as indicated below.

PRE–SANITISATION HANDLING	POST–SANITISATION HANDLING
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL
PROTECTED	Unclassified
Unclassified (DLM)	Unclassified

Sanitising media prior to reuse

Sanitising media prior to reuse assists with enforcing the need–to–know principle.

Control: 0947; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should sanitise all media prior to reuse.

References

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.

The RAM testing tool memtest86+ can be obtained from http://memtest.org/.

The graphics card RAM testing tool MemtestG80 can be obtained from https://simtk.org/home/memtest.

HDDerase is a freeware tool developed by the Center for Magnetic Recording Research at the University of California San Diego. It is capable of calling the ATA secure erase command for non–volatile magnetic hard disks. It is also capable of resetting host protected area and device configuration overlay table information on the media. The tool is available for download from http://cmrr.ucsd.edu/people/Hughes/secure-erase.html.

Information on Reliably Erasing Data From Flash–Based Solid State Drives can be found at http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf.

For further requirements on media security see the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Media Destruction

Objective

Media that cannot be sanitised is destroyed.

Scope

This section describes the destruction of media.

Context

Additional information relating to the destruction of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Government systems

All references to 'Unclassified (DLM)' in the tables here relate to media containing unclassified but official/sensitive information not intended for public release, such as DLM information. ASD advises that government system (G) controls in the ISM are applied as a baseline to ICT equipment storing or processing Unclassified (DLM) information. Unclassified (DLM) and 'Government' are not classifications under the *Australian Government Security Classification System* as mandated by the Attorney–General's Department.

Controls

Media that cannot be sanitised and must be destroyed

It is not possible to use some types of media while maintaining a high level of assurance that no previous data can be recovered.

Control: 0350; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must destroy the following media types prior to disposal, as they cannot be sanitised:

- microform (i.e. microfiche and microfilm)
- optical discs
- printer ribbons and the impact surface facing the platen
- programmable read–only memory
- read–only memory
- faulty or other types of media that cannot be successfully sanitised.

Control: 1347; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Where volatile media has undergone sanitisation but sensitive or classified information persists on the media, agencies must destroy the media, and handle the media at the at he sensitivity or classification of the information it contains until it is destroyed.

Destruction procedures

Documenting procedures for media destruction will ensure that agencies carry out media destruction in an appropriate and consistent manner.

Control: 0363; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the destruction of media.

Media destruction

The destruction methods given are designed to ensure that recovery of information is impossible or impractical.

Very small characters can be produced on microform. Using equipment that is capable of reducing microform to a fine powder (with resultant particles not showing more than five consecutive characters per particle upon microscopic inspection) will prevent data recovery from destroyed microform.

Control: 0364; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
To destroy media, agencies must either:

- break up the media
- heat the media until it has either burnt to ash or melted
- degauss the media.

Control: 0366; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use one of the methods shown in the table below.

ITEM	DESTRUCTION METHODS					
	FURNACE/ INCINERATOR	HAMMER MILL	DISINTEGRATOR	GRINDER/ SANDER	CUTTING	DEGAUSSER
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Magnetic floppy disks	Yes	Yes	Yes	No	Yes	Yes
Magnetic hard disks	Yes	Yes	Yes	Yes	No	Yes
Magnetic tapes	Yes	Yes	Yes	No	Yes	Yes
Optical disks	Yes	Yes	Yes	Yes	Yes	No
Semiconductor memory	Yes	Yes	Yes	No	No	No

Media destruction equipment

The National Security Agency/Central Security Service's EPL Degausser (EPLD) contains a list of certified degaussers.

The Government Communications Headquarters/Communications–Electronics Security Group's certified data erasure products list also contains a list of certified degaussers.

Control: 1160; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must employ degaussers certified by the National Security Agency/Central Security Service or the Government Communications Headquarters/Communications–Electronics Security Group for the purpose of degaussing media.

When using a degausser to destroy media, checking its field strength regularly will confirm the degausser functioning correctly.

Control: 1360; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should check the field strength of the degausser at regular intervals when destroying media.

When physically destroying media, using approved equipment will give agencies complete assurance that information residing on the media is destroyed. This includes destruction equipment:

- Listed in the ASIO Security Equipment Catalogue; or
- Meeting the ASIO Security Equipment Guides, (i.e. SEG–009 Optical Media Shredders, and SEG–018 Destructors).

The ASIO Security Equipment Catalogue may be ordered via the SCEC website (http://www.scec.gov.au). The ASIO Security Equipment Guides are available from the Protective Security Policy GOVDEX Community or ASIO—T4 by email request.

Control: 1361; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use approved equipment when destroying media.

Storage and handling of media waste particles

Following destruction, normal accounting and auditing procedures do not apply for media. It is therefore essential that when media is recorded as being destroyed, destruction is assured.

Control: 0368; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must, at minimum, store and handle the resulting media waste for all methods, except for furnace/incinerator and degausser, as indicated below.

INITIAL MEDIA HANDLING	SCREEN APERTURE SIZE PARTICLES CAN PASS THROUGH			
	LESS THAN OR EQUAL TO 3MM	LESS THAN OR EQUAL TO 6MM	LESS THAN OR EQUAL TO 9MM	LESS THAN OR EQUAL TO 12MM
TOP SECRET	Unclassified	PROTECTED	CONFIDENTIAL	SECRET
SECRET	Unclassified	Unclassified	PROTECTED	CONFIDENTIAL
CONFIDENTIAL	Unclassified	Unclassified	Unclassified	PROTECTED
PROTECTED	Unclassified	Unclassified	Unclassified	Unclassified
Unclassified (DLM)	Unclassified	Unclassified	Unclassified	Unclassified

Degaussers

Degaussing magnetic media changes the alignment of magnetic domains in the media. Data contained on the media becomes unrecoverable. Degaussing renders magnetic media unusable as the storage capability for the media is permanently corrupted.

Coercivity varies between media types and between brands and models of the same type of media. Care is needed when determining the desired coercivity since a degausser of insufficient strength will not be effective. The National Security Agency/Central Security Service's EPLD contains a list of common types of media and their associated coercivity ratings.

Since 2006 perpendicular magnetic media have become available. Some degaussers are only capable of sanitising longitudinal magnetic media. Care therefore needs to be taken to ensure that a suitable degausser is used when sanitising perpendicular magnetic media.

Agencies will need to comply with any product specific directions provided by product manufacturers and certification authorities to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome.

Control: 0361; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a degausser of sufficient field strength for the coercivity of the media.

Control: 0838; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a degausser capable of the magnetic orientation (longitudinal or perpendicular) of the media.

Control: 0362; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with any product specific directions provided by product manufacturers and certification authorities.

Supervision of destruction

To ensure that media is appropriately destroyed it needs to be supervised to the point of destruction and have its destruction overseen by at least one person cleared to the sensitivity or classification of the media being destroyed.

Control: 0370; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform the destruction of media under the supervision of at least one person cleared to the sensitivity or classification of the media being destroyed.

Control: 0371; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Personnel supervising the destruction of media must:

- supervise the handling of the media to the point of destruction
- ensure that the destruction is completed successfully.

Supervision of accountable material destruction

Since accountable material is more sensitive than standard classified media, it needs to be supervised by at least two personnel and have a destruction certificate signed by the personnel supervising the process.

Control: 0372; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform the destruction of accountable material under the supervision of at least two personnel cleared to the sensitivity or classification of the media being destroyed.

Control: 0373; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Personnel supervising the destruction of accountable media must:

- supervise the handling of the material to the point of destruction
- ensure that the destruction is completed successfully
- sign a destruction certificate.

Outsourcing media destruction

ASIO—T4 Protective Security maintains a list of external destruction services that are approved to destroy media in an approved manner. The ASIO Protective Security Circular 144 External Destruction of Australian Government Official Information provides additional advice on the use of external destruction services. The Protective Security Circular and the list of external destruction services are available from the Protective Security Policy Govdex Community or ASIO—T4 by email request.

Control: 0839; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not outsource the destruction of TOP SECRET media or accountable material.

Control: 0840; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies outsourcing the destruction of media to an external destruction service must use a service that has been approved by ASIO—T4 Protective Security.

Transporting media external destruction

Requirements for the physical transfer of media between agencies and external destruction services can be found in the *Australian Government Information Security Management Guidelines—Protectively marking and handling sensitive and security classified information*.

Control: 1069; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should sanitise media, if possible, prior to transporting it to an off–site location for destruction.

References

The National Security Agency/Central Security Service's EPLD can be found at http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

The Government Communications Headquarters/Communications–Electronics Security Group's certified data erasure products list can be found at http://www.cesg.gov.uk/ServiceCatalogue/CCTM/Pages/CCTM-Awards.aspx.

Information on the ASIO—T4 protective security requirements can be found at http://www.asio.gov.au/ASIO-and-National-Security/Units/T4-Protective-Security.html.

Further information on the *ASIO Security Equipment Catalogue* and the SCEC can be found at http://www.scec.gov.au/.

For further requirements on media security see the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework* http://www.protectivesecurity.gov.au.

Media Disposal

Objective

Media is declassified and approved for release before disposal into the public domain.

Scope

This section describes the disposal of media.

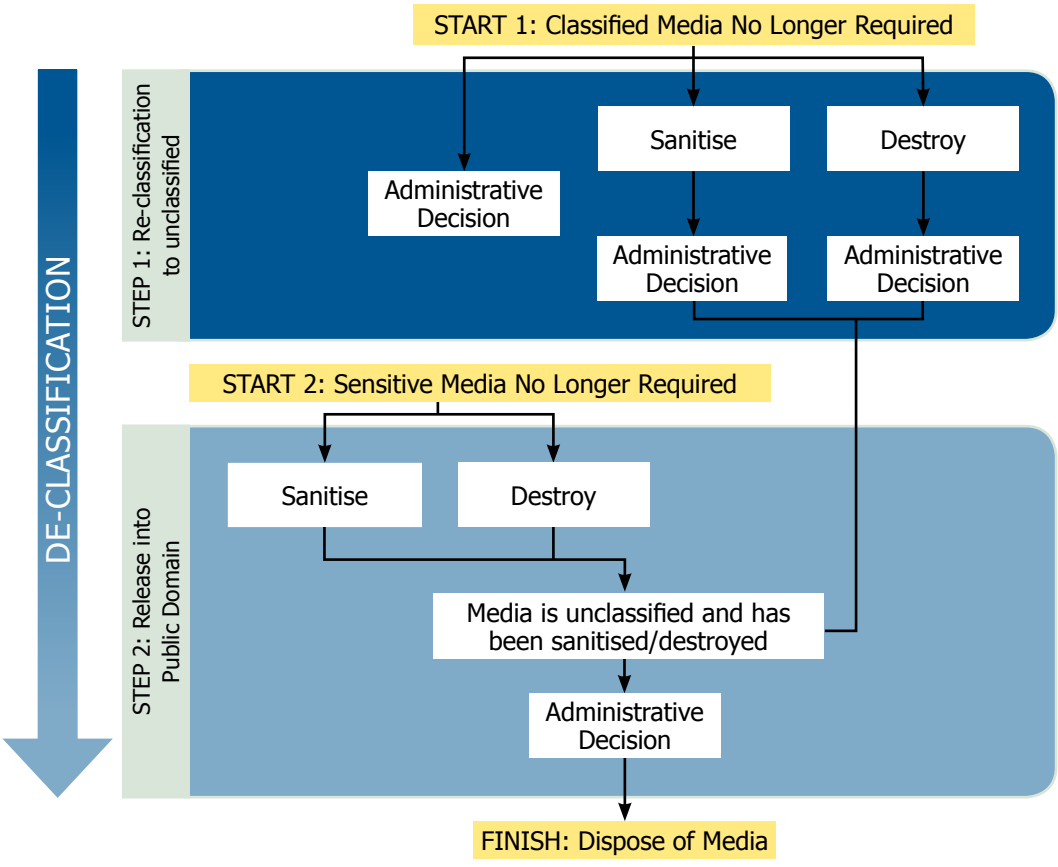
Context

Additional information relating to the disposal of ICT equipment can be found in the *Product Sanitisation and Disposal* section of the *Product Security* chapter.

Controls

Disposal procedures

The following diagram shows an overview of the typical disposal process. In the diagram there are two starting points, one for classified media and one for sensitive media. Also note that declassification is the entire process, including any reclassifications and administrative decisions, that must be completed before media and media waste can be released into the public domain.



Control: 0374; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document procedures for the disposal of media.

Control: 0329; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies declassifying media must ensure that:

- the media has been reclassified to an unclassified level either through an administrative decision, sanitisation or destruction
- a formal administrative decision is made to release the unclassified media, or its waste, into the public domain.

Declassifying media

The process of reclassifying, sanitising or destroying media is not sufficient for media to be declassified and released into the public domain. In order to declassify media a formal administrative decision will need to be made to release the media or waste into the public domain.

Control: 0375; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must declassify all media prior to disposing of it into the public domain.

Disposal of media

Disposing of media in a manner that does not draw undue attention ensures that previously sensitive or classified media is not subjected to additional scrutiny over that of regular waste.

Control: 0378; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must dispose of media in a manner that does not draw undue attention to its previous sensitivity or classification.

References

For further requirements on media security see the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol* of the *Australian Government Protective Security Policy Framework* at http://www.protectivesecurity.gov.au.

Software Security

Standard Operating Environments

Objective

Standard Operating Environments (SOEs) are secure.

Scope

This section describes the hardening of SOEs used on workstations and servers.

Context

The standards endorsed by the *Whole–of–Government Common Operating Environment Policy* come into effect when an agency is ready to deploy a new version of their base SOE. Agencies are now required to build the SOE in accordance with the standards endorsed by the Australian Government Information Management Office (AGIMO).

Controls

Developing hardened SOEs

Removing or disabling unneeded software and operating system components and functionality from a system reduces its attack surface. This could include removing hardware such as optical media recorders, removable media interfaces, or drivers for undesired inbuilt hardware components such as Bluetooth, wireless and webcams.

Antivirus and other Internet security software, while important, can be defeated by malicious code that has yet to be identified by vendors. This can include targeted intrusions, where new malicious software is engineered or existing malicious software is modified to defeat the signature–based detection schemes used by most software.

The use of antivirus and other Internet security software adds value to the defence of workstations and servers, but it cannot be relied upon by itself to protect them. Hardened SOEs still need to be deployed to help protect against a broader range of risks.

Control: 0380; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

Agencies must develop a hardened SOE for workstations and servers, covering:

- removal of unneeded software, operating system components and hardware
- disabling of unused or undesired functionality in software, operating systems and hardware
- use of data execution prevention functionality, preferably hardware based, when available
- implementation of access controls on relevant objects to limit users and programs to the minimum access required
- installation of antivirus or other Internet security software
- installation of software–based application firewalls limiting inbound and outbound network connections
- configuration of either remote logging or the transfer of local event logs to a central server.

Maintaining hardened SOEs

While a SOE can be sufficiently hardened when it is deployed, its security will progressively degrade over time.

Agencies can address the degradation of the security of an SOE by ensuring that:

- users do not have the ability to install or disable software
- users cannot disable or bypass security functionality
- antivirus and other Internet security software is appropriately maintained with the latest signatures.

Control: 0382; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that for all servers and workstations, users do not have the ability to install or disable software.

Control: 1033; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that for antivirus and other Internet security software on servers and workstations:

- detection heuristics are set to a high level
- pattern signatures are checked for updates on a daily basis
- pattern signatures are updated as soon as possible after vendors make them available
- all disks are regularly scanned for malicious code.

Control: 1390; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that reputation ratings are used for antivirus and other Internet security software on servers and workstations.

Vulnerabilities and patch availability awareness

It is important that agencies monitor relevant sources for information about new vulnerabilities and security patches. This will enable agencies to take proactive steps to address vulnerabilities in their systems.

Control: 0297; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should monitor relevant sources for information about new vulnerabilities and security patches for software and ICT equipment they use.

Patching vulnerabilities

Applying patches to operating systems, applications and devices is a critical activity in ensuring the security of systems. ASD rates this activity as one of the most effective security practices agencies can perform. Patching therefore needs to be considered as part of an agency's risk management program. Security fixes for some applications are released as new versions of the application, rather than security patches.

It is recommended that patches that address extreme–risk vulnerabilities, such as vulnerabilities enabling unauthorised code execution by an intruder using the Internet, are deployed within two days. Vendors use different means of communicating vulnerability severity. The severity may be derived from a standard such as the Common Vulnerability Scoring System or based on vendor–defined categorisation such as 'Critical' or 'Important'. Regardless of the rating system the vendor uses, these severity ratings can allow agencies to quickly conduct an initial assessment of importance in their environment. Further guidance on patching and assessing security vulnerabilities and patches can be found in ASD's Protect publication *Assessing Security Vulnerabilities and Patches*.

The latest versions of applications often incorporate newer security technologies and mitigate known vulnerabilities. The latest versions of operating systems can offer significant improvements in security features and stability.

Patching servers is not a trivial task and involves testing and planning. Agencies should weigh up the risk of holding off on patching while patches are tested against the threat of intrusion in this interim period.

As firmware provides the underlying functionality for hardware it is essential that the integrity of any firmware images or updates are maintained. Since firmware controls the low–level operations of a device, firmware vulnerabilities can have serious consequences if exploited. It is therefore important to consider firmware patching as part of your agency's patch management strategy.

Control: 1143; Revision: 3; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities.

Control: 0940; Revision: 5; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must apply all security patches as soon as possible.

Control: 1144; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
For security vulnerabilities assessed as 'extreme risk', agencies must, within two days:

- apply the security patch, or
- mitigate the vulnerability if there is no patch available.

Control: 1348; Revision: 2; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must install the latest version of applications and operating systems as soon as possible.

Control: 1349; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must install the latest version of applications within two days if the upgrade addresses an 'extreme risk' security vulnerability.

Control: 0303; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a procedure for the installation of security patches, driver/firmware updates and application installations that ensures the integrity and authenticity of each patch or update.

Control: 0298; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that security patches, driver/firmware updates and application installations are applied through centralised patch and application management.

Control: 1350; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should install the latest version of drivers and device firmware as soon as possible.

Control: 1351; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should install the latest version of drivers and device firmware within two days if the upgrade addresses an 'extreme risk' security vulnerability.

If a patch is released for a High Assurance product, ASD will conduct an assessment of the patch and might revise the product's usage guidance. Where required, ASD will subsequently conduct an assessment of the cryptographic vulnerability and might revise usage guidance in the Consumer Guide for the product or product–specific doctrine.

If a patch for a High Assurance product is approved for deployment, ASD will inform agencies of the timeframe in which the patch is to be deployed.

Control: 0300; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must not; Authority: ASD
Agencies must not patch High Assurance products without the patch being approved by ASD.

Control: 1362; Revision: 0: Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must: Authority: ASD
Once a patch for a High Assurance product has been approved by ASD, agencies must deploy the patch in accordance with the requirements and timeframes prescribed by ASD.

When security patches are not available

When a security patch is not available for a known vulnerability there are a number of approaches to reduce the security risk to a system. This includes mitigating access to the vulnerability through alternative means, preventing exploitation of the vulnerability, containing the exploit or implementing security measures to detect intrusions attempting to exploit the vulnerability.

Control: 0941; Revision: 5; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Where known vulnerabilities cannot be patched, or security patches are not available, agencies must implement one or more of:

- controls to resolve the vulnerability by either:
  - disabling the functionality associated with the vulnerability though product configuration
  - asking the vendor for an alternative method of managing the vulnerability
  - moving to a different product with a more responsive vendor
  - engaging a software developer to correct the software.
- controls to prevent exploitation of the vulnerability by either:
  - applying external input sanitisation (if an input triggers the exploit)
  - applying filtering or verification on the software output (if the exploit relates to an information disclosure)
  - applying additional access controls that prevent access to the vulnerability
  - configuring firewall rules to limit access to the vulnerable software.
- controls to contain the exploit by either:
  - applying firewall rules limiting outward traffic that is likely in the event of an exploitation
  - applying mandatory access control preventing the execution of exploitation code
  - setting file system permissions preventing exploitation code from being written to disk.
- controls to detect intrusions by either:
  - deploying an IDS
  - monitoring logging alerts
  - using other mechanisms as appropriate for the detection of exploits using the known vulnerability.

Unsupported software and products

Once a cessation date for support is announced for software or ICT equipment, agencies will find it increasingly difficult to protect against vulnerabilities found in the software or equipment as no security patches will be made available by the vendor. Once a cessation date for support is announced agencies should investigate new solutions that will be appropriately supported.

Control: 0304; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must assess the risk of using software or ICT equipment when a cessation date for support is announced or when the software or equipment is no longer supported by the vendor.

Default passphrases and accounts

Default passphrases and accounts for operating systems are often exploited as they are well documented in product manuals and can be easily checked in an automated manner with little effort required. When default passphrases are changed they must meet the requirements outlined in the *Access Control* chapter of this manual.

Control: 0383; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must reduce potential vulnerabilities in their SOEs by:

- removing or otherwise disabling unused accounts
- renaming or deleting default accounts
- replacing default passphrases.

Functional separation between servers

Servers with a high value include those in a gateway environment such as web, email, file and IP telephony servers.

Agencies may also implement separation through the use of techniques to restrict a process to a limited portion of the file system, but this is less effective.

Control: 0385; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where high value servers have connectivity to public network infrastructure, agencies should:

- maintain effective functional separation between servers allowing them to operate independently
- minimise communications between servers at both the network and file system level as appropriate
- limit users and programs to the minimum access needed to perform their duties.

Control: 0953; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that functional separation between servers is achieved either:

- physically, using single dedicated machines for each function
- using virtualisation technology to create separate virtual machines for each function in the same security domain.

Using virtualisation for functional separation between servers

Virtualisation is approved as a method of achieving functional separation between servers if the servers reside in the same security domain. Due to vulnerabilities in virtualised environments, virtualisation is not approved as a domain separation method.

Specifically, an intruder could achieve privilege escalation in a guest operating system by exploiting vulnerabilities in virtualisation products. This can be performed without breaching the separation. Additionally, vulnerabilities in virtualisation products can allow a malicious actor to gain access to one virtual machine from another residing on the same hardware, breaching the security boundary. This could also occur as a result of a misconfiguration of the virtualisation software by the agency which, unbeknownst to the agency, results in the weakening or elimination of the security boundary between two virtual machines.

Guidance on the agency use of virtualisation in cloud computing scenarios can be found in the *Industry Engagement and Outsourcing* section of the *Information Security Governance* chapter.

Control: 0841; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Virtualisation technology should not be used for functional separation between servers or network appliances in different security domains at the same classification.

Control: 0842; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Virtualisation technology must not be used for functional separation between servers or network appliances of different classifications.

Characterisation

Characterisation is a technique used to analyse and record a system's configuration. It is important since it can be used to verify the system's integrity at a later date.

Methods of characterising files and directories include:

- performing a cryptographic checksum on files/directories when they are known to be virus/malicious software 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
- for a Windows system, taking a system difference snapshot.

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 operating 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.

Control: 0386; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should:

- characterise all servers whose functions are critical, and those identified as being at a high risk of compromise
- store the characterisation information securely off the server in a manner that maintains its integrity
- update the characterisation information after every legitimate change to a system
- as part of the 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
- perform the characterisation from a trusted environment rather than the standard operating system wherever possible
- resolve any detected changes in accordance with cyber security incident management procedures.

Control: 0954; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should meet the requirement for characterisation using an AACA to perform cryptographic checksums.

Automated outbound connections by software

Examples of applications that include beaconing functionality are applications that initiate a connection to the vendor website over the Internet (a continuous signalling of error or location information) and applications for inbound remote management.

Control: 0387; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should review all software applications to determine whether they attempt to establish any external connections.

Control: 0388; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
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.

Knowledge of software used on systems

Information about installed software that could be disclosed includes:

- user agent on web requests disclosing the web browser type
- network and email client information in email headers
- email server software headers.

This information could provide a malicious entity with knowledge of how to tailor intrusions to exploit vulnerabilities in the systems.

Control: 0381; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should limit the disclosure of software installed on their systems.

References

Independent testing of different antivirus and other Internet security software and their effectiveness can be found at http://www.av-comparatives.org/.

Further information on the Whole–of–Government COE can be found at http://www.finance.gov.au/category/common-operating-environment/.

Further guidance on patching can be found in ASD's Protect publication *Assessing Security Vulnerabilities and Patches*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Application Whitelisting

Objective

Only approved applications are used on operating systems.

Scope

This section describes the use of technical controls to restrict the specific applications that can be accessed by a user or group of users.

Context

Application whitelisting is an approach by which all executables and applications are prevented from executing by default unless explicitly specified. These whitelisted executables and applications are allowed to execute.

Controls

Application whitelisting

Application whitelisting can be an effective mechanism to prevent the compromise of a system resulting from the exploitation of vulnerabilities in an application or from the execution of malicious code.

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—a blacklist.

Application whitelisting is just one part of a defence–in–depth strategy for preventing intrusions and reducing their consequences.

Control: 0843; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must implement application whitelisting as part of the SOE for both workstations and servers to ensure users can only execute an agency–defined set of trusted applications.

User permissions

An average user requires access to only a few applications, or groups of applications, in order to conduct their work. Restricting the user's permissions to this limited set of applications reduces the opportunities for compromising the system. It is preferable that agencies are proactive in defining the applications to prevent the execution of malicious or unapproved applications, including DLLs, scripts and installers permitted to execute, rather than using default lists in application whitelisting software. It is important that application whitelisting does not replace antivirus and other Internet security software already in place on a system.

Control: 0845; Revision: 4; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must restrict a 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.

Control: 0846; Revision: 4; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that a user cannot disable the application whitelisting mechanism.

System administrator permissions

Since the consequences of running malicious code as a privileged user are much more severe than as an unprivileged user, application whitelisting must also be enforced for system administrators.

Control: 0848; Revision: 3; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that system administrators are not exempt from application whitelisting policy.

Application whitelisting configuration

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.

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.

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.

Application whitelisting based on parent folder or executable path is futile if access control list permissions allow a user to write to the folders or overwrite permitted executables.

Adequate logging information can allow system administrators to further refine the application whitelisting implementation and detect patterns or occurrences of users being denied access.

Control: 0851; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should plan and test application whitelisting thoroughly prior to implementation.

Control: 0955; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict the decision whether to run an executable based on the following, in the order of preference shown:

- cryptographic hash
- executable absolute path
- digital signature
- parent folder.

Control: 0849; Revision: 3; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the default policy is to deny the execution of software.

Control: 0956; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict the write access to folders of any executables which are permitted to run by the application whitelisting controls.

Control: 0957; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure logs from the application whitelisting implementation include all relevant information such as the enforcement setting, file name, date and time, and username.

References

Further information on implementing application whitelisting using AppLocker by Microsoft can be found at http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx.

Additional information regarding application whitelisting can be found in the *Application Whitelisting Explained* document. This can be found on the ASD website at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

Software Application Development

Objective

Secure programming methods and testing are used for software application development.

Scope

This section describes developing, upgrading and maintaining application software used on systems.

Context

By following the guidelines in this section, the software flaws and vulnerabilities which are able to be exploited by an intruder will be considered and addressed.

Controls

Software development environments

Segregating development, testing and production environments limits the spread of malicious code and minimises the likelihood of faulty code being put into production.

Limiting access to development and testing environments will reduce the information that can be obtained by an internal intruder.

Control: 0400; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that software development environments are configured such that:

- there are at least three environments covering:
  - development
  - testing
  - production.
- information flow between the environments is strictly limited according to a defined and documented policy, with access granted only to users with a clear business requirement
- new development and modifications only take place in the development environment
- write access to the authoritative source for the software is disabled.

Secure software design

Proper security design is a key step in producing secure software. Threat modelling is an important part of secure software design. Threat modelling identifies at–risk components of software, enabling appropriate security controls to be identified to mitigate risk.

Control: 1238; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use threat modelling and other secure design techniques to ensure that all threats to software and appropriate mitigations to these threats are identified.

Secure programming

Once the secure software design has been identified, the secure technical implementation of the controls during development is essential.

Examples of secure programming includes performing correct input validation and handling, robust and fault–tolerant programming and ensuring the software uses the least amount of privileges required.

Control: 0401; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that software developers use secure programming practices when writing code, including:

- designing software to use the lowest privilege level needed to achieve its task
- denying access by default
- checking return values of all system calls
- validating all inputs
- following secure coding standards.

Software testing

Software security testing will lessen the possibility of vulnerabilities being introduced into a production environment. Software security testing can be performed using both static testing, such as code analysis, as well as dynamic testing, such as input validation and fuzzing.

Using an independent party for software testing will remove any bias that can occur when a developer tests their own software.

Control: 0402; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Software should be reviewed or tested for vulnerabilities before it is used in a production environment.

Control: 0403; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Software should be reviewed or tested by an independent party as well as the developer.

References

An example of a Secure Development Life cycle model, used by Microsoft in the development of all versions of Windows since Windows 2003, can be found at http://msdn.microsoft.com/en-us/library/ms995349.aspx.

Secure coding standards can be found at http://www.cert.org/secure-coding/.

Web Application Development

Objective

Security measures are incorporated into all web applications.

Scope

This section describes developing, upgrading and maintaining web applications used on systems.

Context

Protecting web applications

Even though web applications may only contain information authorised for release into the public domain there still remains a need to protect the integrity and availability of the information and the systems it is hosted on and connected to. Web applications and servers are therefore to be treated in accordance with the requirements of the sensitivity or classification of the system they are connected to.

Controls

Web application frameworks and libraries

Web application frameworks and libraries can be leveraged by developers to enhance the security of a web application while decreasing development time. These resources can assist developers to securely implement complex components such as session management, input handling and cryptographic operations.

Control: 1239; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should utilise robust web application libraries to aid the secure development of web applications.

Secure input handling

The majority of web application vulnerabilities are due to the lack of secure input handling by the web application. It is essential that web applications do not trust any user controlled input without first properly validating and/or sanitising it in an appropriate manner. User controlled input includes:

- the URL and URL parameters
- HTML form data
- cookie values
- HTTP request headers.

Examples of validation and sanitisation include, but are not limited to:

- ensuring a telephone form field contains only numerals
- ensuring data used in an SQL query is sanitised properly
- ensuring Unicode input is handled appropriately.

Control: 1240; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform appropriate validation and/or sanitisation on all input handled by a web application.

Output encoding

The threat of cross–site scripting and other content injection attacks can be further mitigated through the use of appropriate, contextual output encoding. The most common example of output encoding is the use of HTML entities. Performing HTML entity encoding causes potentially dangerous HTML characters such as '<', '>' and '&' to be converted into their encoded equivalents '<', '>' and '&'.

Output encoding is particularly useful where external data sources, which may not be subject to the same level of input filtering, are output to users.

Control: 1241; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that output encoding is performed where appropriate.

Browser based security controls

Security controls applied at the web application or server that leverage security functionality present in web browsers can help secure web applications.

These security controls are implemented by inserting HTTP headers in outgoing responses. This makes them possible to be applied to legacy or proprietary web applications where changes to the web server are possible but changes to the source code are not.

Control: 1242; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must secure, configure and harden web servers.

Additional resources

The *Open Web Application Security Project* provides a comprehensive resource to consult when developing web applications.

Control: 0971; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should follow the documentation provided in the *Open Web Application Security Project* guides to building secure web applications and web services.

References

Further information on web application security is available from the *Open Web Application Security Project* at https://www.owasp.org/index.php/Main_Page.

Further guidance on implementing browser based security controls can be found in ASD's Protect publication *Protecting Web Applications and Users*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Database Systems

Objective

Database systems are appropriately protected from theft, corruption, loss, and unauthorised access and exposure.

Scope

This section describes databases and database management system (DBMS) software, collectively known as database systems, as well as their environment.

Context

The following controls can be applied to production, test and development database systems and their environment to increase their security posture. Doing so will enable agencies to conduct their business with a reduced risk of theft, corruption, loss, or unauthorised access and exposure of, information critical to their business.

Further information on AACAs can be found in the *Cryptography* chapter of this manual.

Controls

Maintaining an accurate inventory of databases

Without knowledge of all the databases in an agency, and the sensitive or classified information they contain, an agency will be unable to apply appropriate protection to these assets. For this reason, it is important an accurate inventory of all databases deployed by an agency and their contents is maintained and regularly reviewed.

Control: 1243; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should maintain and regularly review an accurate inventory of all deployed databases and their contents.

DBMS software versions and patching

Using unsupported or unpatched DBMS software can expose databases to publicly known vulnerabilities. These vulnerabilities can be exploited by an intruder to gain access to database content or even the underlying operating system. Deploying the latest security patches and product updates from vendors to DBMS software in a timely manner will assist in protecting databases. Furthermore, agencies may choose to deploy the latest versions of DBMS software as it is released. This will allow agencies to take advantage of any new security functionality and continued vendor support for their DBMS software.

Control: 1244; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must apply the latest security patches and product updates from vendors to DBMS software as soon as possible.

DBMS software installation and configuration

DBMS software will often leave temporary installation files and logs during the installation process, in case an administrator needs to troubleshoot a failed installation. Information in these files, which can include passwords in the clear, could provide valuable information to an intruder. Removing all temporary installation files and logs after DBMS software has been installed will minimise this risk.

Control: 1245; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should remove all temporary installation files and logs after DBMS software has been installed.

Poorly configured DBMS software could provide an opportunity for an intruder to gain unauthorised access to database content. To assist agencies in deploying database systems, vendors often provide guidance on how to securely configure their DBMS software.

Control: 1246; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should securely configure DBMS software as per their vendor's guidance.

DBMS software is often installed with most features enabled by default as well as being pre–configured with a sample database and anonymous user accounts for testing purposes. Additional functionality often brings with it an increased risk. Thus, disabling or removing DBMS software features and stored procedures that are not required will minimise the risk. Furthermore, removing all sample databases on database servers will minimise the attack surface of the DBMS software.

Control: 1247; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should disable or remove DBMS software features and stored procedures that are not required.

Control: 1248; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should remove all sample databases on database servers.

DBMS software operating as a local administrator or root account can present a significant risk to the underlying operating system if compromised by an intruder. Therefore, it is important to configure DBMS software to run as a separate account with the minimum privileges needed to perform its functions. In addition, limiting access of the account under which the DBMS server runs to non–essential areas of the database server's file system will limit the impact of any compromise of the DBMS software.

Control: 1249; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must configure DBMS software to run as a separate account with the minimum privileges needed to perform its functions.

Control: 1250; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The account under which DBMS software runs must have limited access to non–essential areas of the database server's file system.

DBMS software is often capable of accessing files that it has read access to on the local database server.

For example, an intruder using an SQL injection could use the command LOAD DATA LOCAL INFILE 'etc/passwd' INTO TABLE Users or SELECT load_file("/etc/passwd") to access the contents of a Linux password file. Disabling the ability of the DBMS software to read local files from a server will prevent such SQL injection from succeeding. This could be performed, for example, by disabling use of the LOAD DATA LOCAL INFILE command.

Control: 1251; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should disable the ability of DBMS software to read local files from a server.

Protecting authentication credentials in databases

Storing authentication credentials such as usernames and passwords as plaintext in databases poses a significant risk to agencies. An intruder that manages to gain access to database contents can extract these authentication credentials to gain access to users' accounts. In addition, it is possible that a user could have reused a username and password for their corporate workstation posing an additional risk to an agency. To prevent authentication credentials from being exposed, usernames and passwords stored in databases must be hashed with a strong hashing algorithm which is uniquely salted. Further guidance on AACAs can be found in the *Cryptography* chapter of this manual.

Control: 1252; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure usernames and passwords stored in databases are hashed with a strong hashing algorithm which is uniquely salted.

Protecting database contents

Storing particularly sensitive content on databases can worsen the consequences if the database is compromised. Carefully considering the business requirement for storing sensitive content on databases and its effect on the agency's risk profile is imperative. In addition, to ensure that appropriate protective measures are applied to such information, database administrators and database users need to know what level of sensitivity is associated with the database and its contents. This can be achieved by using appropriate protective markings to information stored in databases.

Control: 1253; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must only store particularly sensitive content in databases when absolutely necessary to meet their business requirements.

Control: 0393; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Information stored in databases must be associated with appropriate protective markings.

Implementing database user roles that limit user's access to content needed to perform their work duties will ensure the need–to–know principle is applied. Restricting database user roles to selecting, updating and inserting content into databases based on the essential business requirement and work duties of users will further improve database security.

Control: 1254; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement database user roles limiting user's access to content needed to perform their work duties.

Control: 1255; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict database user roles to selecting, updating and inserting content into databases based on the essential business requirements and work duties of their users.

Database contents can be protected from unauthorised copying and subsequent offline analysis by applying appropriate file–based access controls to database files. However, should an intruder gain access to database files, for example, cases of physical theft of a database server, compromised administrative credentials on a database server or failure to sanitise database server hardware before disposal, an additional layer of protection is required. Appropriately encrypting particularly sensitive content within databases, for example, using Advanced Encryption Standard (AES) before being stored in a database will assist in addressing this risk. Further guidance can be found in the *Cryptography* chapter. In addition to preventing unauthorised access to particularly sensitive information using offline analysis, encrypting particularly sensitive content before storing it in a database, as opposed to encrypting database columns or tablespaces using transparent encryption, has the added benefit of preventing unauthorised access to particularly sensitive information as part of an SQL injection against a database.

Control: 1256; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must apply appropriate file–based access controls to database files.

Control: 1257; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should appropriately encrypt particularly sensitive content before being stored in a database.

Aggregation of database contents

Where concerns exist that the sum, or aggregation, of separate pieces of sensitive or classified information from within databases could lead to an intruder determining more highly sensitive or classified information, database views in combination with database user access roles should be implemented. Alternatively, the information of concern could be separated by implementing multiple databases, each with restricted data sets. If implemented properly, this will ensure an intruder cannot access the sum of information components leading to the aggregated information.

Control: 1258; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where concerns exist that the sum, or aggregation, of separate pieces of information from within databases could lead to a database user determining more highly classified information, database views in combination with database user access roles should be implemented.

Hardening database server SOE

Using a hardened SOE for database servers will make it more difficult for an intruder to compromise database servers in order to exploit database systems.

Control: 1259; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Database servers must use a hardened SOE.

Database administrator accounts

DBMS software often comes pre–configured with default database administrator accounts and passwords that are listed in product documentation, for example, sa/<blank> for SQL Server, root/<blank> for MySQL, scott/tiger for Oracle and db2admin/db2admin for DB2. To assist in preventing an intruder from exploiting this, default database administrator accounts must be removed or have their passwords changed to strong complex passwords. Furthermore, passwords should not be shared across separate database instances as doing so can exacerbate any password compromise by an intruder.

Control: 1260; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Default database administrator accounts must be removed or have their passwords changed to strong complex passwords.

Control: 1261; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Passwords should not be shared across separate database instances.

When sharing database administrator accounts for the performance of administrative tasks on databases, any actions undertaken cannot be attributed to an individual database administrator. Ensuring database administrators have unique and identifiable accounts will assist in auditing activities on databases. This is particularly helpful during investigations relating to an attempted (or successful) cyber intrusion. Furthermore, it is important to use database administrator accounts exclusively for administrative tasks with standard database user accounts used for general purpose interactions with databases.

Control: 1262; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Database administrators must have unique and identifiable accounts.

Control: 1263; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Database administrator accounts must be used exclusively for administrative tasks with standard database user accounts used for general purpose interactions with databases.

When creating new database administrator accounts, the accounts are often allocated all privileges available to administrators. Most database administrators will only need a subset of all available privileges to undertake their authorised duties. Therefore, for improved security, database administrator access can be restricted to defined roles rather than accounts with default administrative permissions, or all permissions.

Control: 1264; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Database administrator access should be restricted to defined roles rather than accounts with default administrative permissions, or all permissions.

Even though database administrators may use strong complex passwords for their accounts, an intruder could still install a key logger on their workstations to capture their usernames and passwords. The use of multi–factor authentication can minimise the threat of key logging. This will assist in preventing the compromise of databases by an intruder should a database administrator's password be compromised. In addition, implementing the Top 4 of ASD's *Strategies to Mitigate Targeted Cyber Intrusions* on workstations used to administer databases will assist in protecting database administrators' passwords by minimising the risk that their workstations are compromised.

Control: 1265; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Database administrators must be authenticated to databases using multi–factor authentication.

Database user accounts

DBMS software often comes pre–configured with anonymous database user accounts with blank passwords. Removing anonymous database user accounts will assist in preventing an intruder from exploiting this feature.

Control: 1266; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Anonymous database user accounts must be removed.

Databases often contain information and metadata of varying sensitivities, classifications and compartments. It is important users are only granted access to information in databases for which they have the appropriate security clearance, briefings and a need–to–know. The need–to–know principle can be enforced through the application of minimum privileges, database views and database roles.

Control: 1267; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Database users must only be granted access to information in databases, including metadata, for which they have the appropriate security clearance, briefs and a need–to–know.

Control: 1268; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The need–to–know principle should be enforced through the application of minimum privileges, database views and database roles.

Network environment

Placing database systems used by web applications on the same physical server as a web server in the demilitarised zone of a gateway environment can expose them to an increased risk of cyber intrusion over the Internet. Locating database systems used by web applications on a physically separate database server in a separate demilitarised zone to web servers will reduce this risk.

Control: 1269; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Database systems used by web applications should be located on a physically separate database server in a separate demilitarised zone to web servers.

Placing database servers on the same network segment as the rest of an agency's corporate workstations and allowing them to communicate with other network resources exposes them to an increased risk of compromise. Placing database servers on a different network segment to the rest of an agency's corporate workstations will make it more difficult for an intruder that manages to compromise a workstation or server to interact with database servers. Additionally, implementing network access controls to restrict database servers' communications to strictly defined network resources such as web servers, application servers and storage area networks will improve security.

Control: 1270; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Database servers should be placed on a different network segment to the rest of an agency's corporate workstations.

Control: 1271; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Network access controls should be implemented to restrict database servers' communications to strictly defined network resources such as web servers, application servers and storage area networks.

In cases where database systems will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary risk. If only local access to a database system is required, networking functionality of DBMS software should be disabled or directed to listen solely to the localhost interface.

Control: 1272; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If only local access to a database system is required, networking functionality of DBMS software should be disabled or directed to listen solely to the localhost interface.

Separation of production, test and development environments

Using production databases for test and development activities could result in accidental damage to their integrity or contents.

Control: 1273; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Databases used in production, test and development environments must use separate database servers.

Using sensitive or classified information from production databases in test or development databases could result in inadequate protection being applied to the information. As such, it is imperative information in production databases is not used in test or development databases unless appropriately sanitised of sensitive or classified information first.

Control: 1274; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Information in production databases must not be used in testing or development databases unless the testing or development databases are accredited to the same standard as the production environment.

Interacting with database systems from web applications

SQL injections pose a significant threat to database confidentiality, integrity and availability. SQL injections can allow an intruder to steal information from databases, modify database contents, delete an entire database or even in some circumstances gain control of the underlying database server. To protect against SQL injections, all queries to database systems from web applications must be filtered for legitimate content and correct syntax. Furthermore, to prevent against injection of content into dynamically generated queries, stored procedures should be used for database interaction instead of dynamically generated queries.

Control: 1275; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All queries to database systems from web applications must be filtered for legitimate content and correct syntax.

Control: 1276; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Stored procedures should be used for database interaction instead of dynamically generated queries.

Information communicated between database systems and web applications, especially over the Internet, is susceptible to capture by an intruder. Appropriately encrypting sensitive or classified information communicated between databases systems and web applications (for example, using Transport Layer Security (TLS)) will prevent an intruder from capturing such information.

Control: 1277; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Sensitive or classified information communicated between database systems and web applications must be appropriately encrypted.

When database queries by web applications fail they are capable of displaying detailed error information. This can include the DBMS software version and patch levels. In addition, the failed database query can be displayed revealing information about the database schema. To prevent an intruder from using such information to exploit published vulnerabilities in DBMS software, or further tailor SQL injections, it is important web applications are be designed to provide as little error information as possible about DBMS software and database schemas.

Control: 1278; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Web applications should be designed to provide as little error information as possible about DBMS software and database schemas.

Event logging and auditing

Logging and auditing database events can assist in monitoring for unusual activity, unauthorised actions or in conducting investigations after an attempted, or successful, cyber intrusion.

Control: 1279; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The following types of database events, at a minimum, should be logged:

- database logons and logoffs
- database administrator actions
- attempted accesses that are denied
- attempts to elevate privileges
- changes to user roles or rights
- addition of new users, especially administrative users
- changes to the database structure
- access to particularly sensitive information
- any query or database alerts or failures
- any query containing comments
- any query containing multiple embedded queries.

To assist in the coordination of audits of event logs from multiple sources, and in identifying patterns of activity that might not be noticeable when reviewing event logs from a single source, database event logs should be centrally logged to a secure logging server. Furthermore, database event logs should be time–stamped using a trusted time source.

Control: 1280; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Database event logs should be centrally logged to a secure logging server.

Control: 1281; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Database event logs should be time–stamped using a trusted time source.

While DBMS software may appropriately log database events for unusual activity or unauthorised actions, an intruder may attempt to cover signs of a cyber intrusion by modifying or deleting the database event logs. As such, it is imperative database event logs be appropriately protected from unauthorised access, modification, deletion or loss.

Control: 1282; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Database event logs must be appropriately protected from unauthorised access, modification, deletion or loss.

While an agency may sufficiently log and correlate database events, if they are not audited on a regular basis cyber intrusions may go unnoticed for an extended period of time.

Control: 1283; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Database event logs should be audited on a regular basis for signs of attempted, or successful, cyber intrusions.

References

Nil.

Email Security

Email Policy

Objective

Agencies have a defined policy which outlines the correct use of email communications.

Scope

This section describes email policy for agency systems.

Context

Information on ISPs can be found in the *Information Security Policy* section of the *Information Security Documentation* chapter.

Controls

Email usage policy

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 risks and how they might affect business operations.

Control: 0264; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a policy governing the use of email.

Awareness of email usage policies

There is little value in having email usage policies for personnel if they are not made aware of their existence.

Control: 0266; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must make personnel aware of their email usage policies.

Monitoring email usage

Monitoring breaches of email usage policies—for example, attempts to send prohibited file types or executables, attempts to send excessively sized attachments or attempts to send sensitive or classified information without appropriate protective markings will help enforce email usage policy.

Control: 0822; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement measures to monitor their personnel's compliance with email usage policies.

Public web–based email services

Allowing staff to access web–based email services can pose a security risk if there are insufficient malicious web content filtering controls in place to mitigate malicious web mail attachments. Additionally the agency is reliant upon the web mail provider implementing mitigations such as SPF and DomainKeys.

Web–based email is email accessed using a web browser, examples include Gmail, Hotmail and email portals provided by Internet Service Providers.

Control: 0267; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow personnel to access consumer–grade web–based email services from agency systems.

Socially engineered emails

Socially engineered emails are one of the most common techniques used to spread malicious software. Should technical measures fail, users are the last line of defence in ensuring a socially engineered email does not lead to malicious software being installed on a workstation. Agencies need to ensure their users are aware of the threat and educated on how to detect and report suspicious emails.

Control: 1340; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure users are made aware of the social engineering threat, as well as methods to detect suspicious emails in their environment and processes to report these events.

References

Further guidance can be found in ASD's Protect publications *Detecting Socially Engineered Emails* and *Malicious Email Mitigation Strategy Guide*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Email Protective Markings

Objective

Emails are protected by protective markings. Protective markings are inspected and handled appropriately.

Scope

This section describes protective markings on email and their enforcement at both the server and workstation levels.

Context

Additional requirements and guidance for email protective markings can be found in AGIMO's *Email Protective Marking Standard for the Australian Government*.

Controls

Marking emails

As for paper–based information, all electronic–based information needs to be marked with an appropriate protective marking. This ensures that appropriate security measures are applied to the information and helps prevent unauthorised information being released into the public domain. When a protective marking is applied to an email it is important that it reflects the sensitivity or classification of the information in the body of the email and in any attachments to the email.

This supports the requirements outlined in the *Australian Government Information Security Management Protocol.*

Control: 0273; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All official emails must have a protective marking.

Control: 0275; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Email protective markings must accurately reflect each element of an email, including attachments.

Emails from outside the government

If an email is received from outside government the user has an obligation to determine the appropriate security measures for the email if it is to be responded to, forwarded on or printed out.

Control: 0278; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Where an unmarked email has originated outside the government, users must assess the information and determine how it is to be handled.

Marking personal emails

Applying incorrect protective markings to emails that do not contain government information places an extra burden on protecting emails that do not need protection.

Emails that do not contain official government information are recommended to be marked with an UNOFFICIAL protective marking to clearly indicate the email is of a personal nature.

Control: 0852; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Where an email is of a personal nature and does not contain government information, protective markings for official information should not be used.

Receiving unmarked emails

If an email is received without a protective marking the user has an obligation to contact the originator to seek clarification on the appropriate security measures for the email. Alternatively, where the user receives unmarked non–government emails as part of its business practice the application of protective markings can be automated by a system.

Control: 0967; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where an unmarked email has originated from an Australian or overseas government agency, users should contact the originator to determine how it is to be handled.

Receiving emails with unknown protective markings

If an email is received with a protective marking that the user is not familiar with, they have an obligation to contact the originator to clarify the protective marking and the appropriate security measures for the email.

Control: 0968; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where an email is received with an unknown protective marking from an Australian or overseas government agency, users should contact the originator to determine appropriate security measures.

Preventing unmarked or inappropriately marked emails

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, where the requirements for the entire network can be enforced. In addition, email servers can apply controls for emails generated by applications.

While blocking at the email server is considered the most appropriate control there is still an advantage to blocking at the workstation. This adds an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

Control: 1368; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must prevent unmarked emails or emails marked with an unrecognised or invalid protective marking from being sent to the intended recipients by blocking the email at the email server.

Control: 1022; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should prevent unmarked emails or emails marked with an unrecognised or invalid protective marking from being sent to intended recipients by blocking the email at the workstation.

Blocking inbound emails

Blocking an inbound email with a protective marking higher than the sensitivity or classification that the receiving system is accredited to will prevent a data spill from occurring on the receiving system.

Control: 0565; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must configure email systems to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the sensitivity or classification of the receiving system.

Control: 1023; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should notify the intended recipient of any blocked emails.

Blocking outbound emails

Blocking an outbound email with a protective marking higher than the sensitivity or 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.

Agencies may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from their gateways.

Control: 0563; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must configure systems to block any outbound emails with a protective marking indicating that the content of the email exceeds the sensitivity or classification of the path over which the email would be communicated.

Control: 0564; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should configure systems to log every occurrence of a blocked email.

Protective marking standard

Applying markings that reflect the protective requirements of an email informs the recipient on how to appropriately handle the email.

The application of protective markings as per the AGIMO standard facilitates interoperability across government.

Control: 0270; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must comply with the current standard for the application of protective markings to emails as promulgated by AGIMO.

Printing protective markings

The *Australian Government Information Security Management Protocol* requires that paper–based information have the protective marking of the information placed at the top and bottom of each piece of paper.

Control: 0969; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should configure systems so that the protective markings appear at the top and bottom of every page when the email is printed.

Protective marking tools

Requiring user intervention in the marking of user generated emails assures a conscious decision by the user, lessening the chance of incorrectly marked emails.

Allowing users to choose only protective markings for which the system is accredited lessens the chance of a user inadvertently over–classifying an email. It also reminds users of the maximum sensitivity or classification of information permitted on the system.

Email gateway filters generally only check the most recent protective marking applied to an email. Therefore when users are forwarding or responding to an email, forcing them to apply a protective marking that is at least as high as that of the email they received will help email gateway filters prevent emails being sent to systems that are not accredited to handle the original sensitivity or classification of the email.

Control: 0271; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow a protective marking to be inserted into user generated emails without their intervention.

Control: 0272; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies providing a marking tool should not allow users to select protective markings that the system has not been accredited to process, store or communicate.

Control: 1089; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies providing a marking tool should not allow users replying to or forwarding an email to select a protective marking that is lower than previously used for the email.

Caveated email distribution

Often the membership and nationality of members of email distribution lists is unknown. Therefore users sending emails with AUSTEO, AGAO or other nationality releasability marked information to distribution lists could accidentally cause a data spill.

Control: 0269; Revision: 1; Updated: Sep-09; Applicability: P, C, S, TS; Compliance: should; Authority: AA
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.

References

The AGIMO *Email Protective Marking Standard for the Australian Government* and its associated implementation guide are available from http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/.

Email Infrastructure

Objective

Email infrastructure and the emails it handles are secured.

Scope

This section describes security controls which apply to email server software and the servers which host this software.

Context

Information on using email applications can be found in the *Email Applications* section of this chapter. Information on usage policies for personnel is located in the *Email Policy* section of this chapter, and the *Using the Internet* section of the *Personnel Security for Systems* chapter.

Controls

Undeliverable messages

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. Sending bounces only to senders that can be verified via Sender Policy Framework (SPF), or other trusted means avoids contributing to this problem and allows trusted parties to receive legitimate bounce messages.

Control: 1024; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should only send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means.

Automatic forwarding of emails

Automatic forwarding of emails, if left unsecured, can pose a security risk to the unauthorised disclosure of sensitive or classified information. For example, a user could setup a server–side rule to automatically forward all emails received on an Internet–connected system to their personal email account outside work.

Control: 0566; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

Open relay email servers

An open relay email server (or open mail relay) is a server that is configured to allow anyone on the Internet to send emails through the server. Such configurations are highly undesirable as they allow spammers and worms to exploit this functionality.

Control: 0567; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable open email relaying so that email servers will only relay messages destined for their domains and those originating from inside the domain.

Email server maintenance activities

Email servers perform a critical business function. It is important that agencies perform regular email server auditing, security reviews and vulnerability analysis activities.

Control: 0568; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform regular email server auditing, security reviews and vulnerability analysis activities.

Centralised email gateways

Without a centralised email gateway it is exceptionally difficult to deploy SPF, DomainKeys Identified Mail (DKIM) and outbound email protective marking verification.

Adversaries will almost invariably avoid using the primary email server when sending malicious emails. This is because the backup or alternative email gateways are often poorly maintained in terms of out–of–date blacklists and content filtering.

Control: 0569; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should route email through a centralised email gateway.

Control: 0570; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Where backup or alternative email gateways are in place, additional email gateways must be maintained at the same standard as the primary email gateway.

Control: 0571; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Where users send email from outside their network, an authenticated and encrypted channel must be configured to allow email to be sent via the centralised email gateway.

Email server transport encryption

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 intrusions 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 Internet Engineering Task Force (IETF) Request for Comments (RFC) 3207 specifies the encryption as opportunistic.

Control: 0572; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must enable opportunistic TLS encryption as defined in IETF RFC 3207 on email servers that make incoming or outgoing email connections over public network infrastructure.

References

Nil.

Email Content Filtering

Objective

Emails and attachments received and sent by an agency are secure.

Scope

This section describes controls for mitigating emails with malicious content, including socially engineered emails. These controls would typically be applied on the email server software, the email content filter, or both.

Context

Email is a common vector for cyber intrusions. Email content filtering is an effective approach to preventing network compromise through cyber intruders' use of malicious emails.

Information on specific content filtering controls can be found in the *Content Filtering* chapter.

Controls

Filtering malicious and suspicious emails and attachments

Blocking specific types of emails reduces the likelihood of phishing emails and emails containing malicious code entering an agency network.

Control: 1234; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must implement applicable content filtering controls on email attachments, as recommended in the *Content Filtering* chapter of this manual.

Control: 0561; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must block at the gateway:

- emails addressed to internal email aliases with source addresses located from outside the domain
- all emails arriving via an external connection where the source address uses an internal domain name.

Active web addresses in emails

Spoofed emails often contain an active web address directing users to a malicious website to either illicit information or infect their workstation with malicious code. To reduce the success rate of such intrusions agencies can strip active web addresses from emails and replace them with non–active versions that a user can type or copy and paste into their web browser.

Control: 1057; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Email servers should strip active web addresses from emails and replace them with non–active versions.

SPF

SPF, and alternative implementations such as Sender ID, aid in the detection of spoofed emails. The SPF record specifies a list of IP addresses or domains that are allowed to send email 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.

Control: 0574; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must specify their mail servers using SPF or Sender ID.

Control: 1183; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a hard fail SPF record when specifying their mail servers.

Control: 1151; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use SPF or Sender ID to verify the authenticity of incoming emails.

Control: 1152; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must block, mark or identify incoming emails that fail SPF checks in a manner that is visible to the email recipient.

DKIM

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 does not match the signed content of the email, the verification fails.

Control: 0861; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should enable DKIM signing on all email originating from their domain.

Control: 1025; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use DKIM in conjunction with SPF.

Control: 1026; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.

Control: 1027; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies operating email distribution list software used by external senders should configure the software so that it does not break the validity of the sender's DKIM signature.

References

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*
- RFC 5617, *DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP).*

Further information on email server security can be obtained from National Institute of Standards and Technology publication SP 800–45 v2, *Guidelines on Electronic Mail Security.*

Guidance on implementing SPF can be found in ASD's Protect publication *Mitigating Spoofed Emails—Sender Policy Framework Explained*. Information on email attachment filtering can be found in ASD's *Malicious Email Mitigation Strategies Guide*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Email Applications

Objective

Email applications used to view and send email are secure.

Scope

This section describes the handling of active content in email.

Context

Although most effective email content filtering controls are applied at the email server or email content filter, applying security controls at the email client software helps create a defence in depth approach.

Information on email infrastructure is located in the *Email Infrastructure* section of this chapter. Information on usage policies for personnel is located in the *Email Policy* section of this chapter and the *Using the Internet* section of the *Personnel Security for Systems* chapter.

Automatically generated emails

The requirements for emails in this section apply equally to automatically generated emails.

Controls

Email active content

Controlling the software that runs on systems helps prevent malicious software and unauthorised applications running. Constraining active content delivered through email, especially on Internet–facing systems, ensures that it cannot arbitrarily access users' files or deliver malicious code. Unfortunately the implementation of email permits such activity.

If active content is displayed automatically in the preview pane it can run even though an email item has not been explicitly opened. If active content is allowed, restricting the preview pane to only render content as plaintext ensures emails from a suspicious source would need a user to make a conscious decision to open an email before the active content is displayed.

Control: 1172; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: should; Authority: AA

Agencies should block client–side active content, by viewing email in plaintext mode instead of in Rich Text Format or Hypertext Markup Language mode.

References

Nil.

Access Control

Identification and Authentication

Objective

Passphrase selection policies and passphrase management practices are implemented on systems.

Scope

This section describes the identification and authentication for all users.

Context

Methods for user identification and authentication

User authentication can be achieved by various means, including biometrics, cryptographic tokens, passphrases, passwords and smart cards. Where this manual refers to passphrases it equally applies to passwords.

Multi–factor authentication uses independent means of evidence to assure an entity's identity. The three authentication methods are:

- something one knows, such as a passphrase or a response to a security question
- something one has, such as a passport, physical token or an identity card
- something one is, such as biometric data, like a fingerprint or face geometry.

Any two of these authentication methods must be used to achieve multi–factor authentication. If something that one knows, such as the passphrase, is written down or typed into a file and stored in plain text, this evidence becomes something that one has and can defeat the purpose of multi–factor authentication.

Strong identification and authentication mechanisms significantly reduce the security risk that unauthorised users will gain access to a system.

Controls

Policies and procedures

Developing policies and procedures will ensure consistency in identification, authentication and authorisation.

Control: 0413; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

Agencies must:

- develop and maintain a set of policies and procedures covering users':
  - identification
  - authentication
  - authorisation.
- make their users aware of the policies and procedures.

User identification

Having uniquely identifiable users ensures accountability.

Control: 0414; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all users are:

- uniquely identifiable
- authenticated on each occasion that access is granted to a system.

Identification of foreign nationals

Where systems contain AUSTEO, AGAO or other nationality releasability marked information, with foreign nationals having access to such systems, it is important that agencies implement appropriate security measures to ensure identification of users who are foreign nationals. Such security measures can help prevent the release of AUSTEO and AGAO information to those not authorised to access it.

Control: 0420; Revision: 4; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Where systems contain AUSTEO, AGAO or other nationality releasability marked information, agencies must implement appropriate security measures to ensure identification of users who are foreign nationals, including seconded foreign nationals.

Control: 0975; Revision: 4; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies implementing security measures to ensure identification of users who are foreign nationals, including seconded foreign nationals, should ensure that this identification includes their specific nationality.

Shared accounts

Using shared non user–specific accounts can hamper efforts to attribute actions on a system to specific personnel. Agencies allowing the use of non user–specific accounts need to determine an appropriate method of attributing actions undertaken by such accounts to specific personnel. For example, a logbook may be used to document the date and time that a person takes responsibility for using a shared account and the actions logged against the account by the system.

Control: 0973; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S; Compliance: should not; Authority: AA
Agencies should not use shared non user–specific accounts.

Control: 0415; Revision: 1; Updated: Nov-10; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not use shared non user–specific accounts.

Control: 0416; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
If agencies choose to allow shared, non user–specific accounts they must ensure that another method of determining the identification of the user is implemented.

Using passphrases for user identification and authentication

A numerical password (or personal identification number) employs a small character set (0–9), making it susceptible to brute force attacks that will be successful in a short period of time.

A simple six character password can be susceptible to brute force attacks in minutes by software available on the Web. Passphrases with at least nine characters using upper and lower case alphabetic characters, numeric characters and special characters are more resistant to brute force attacks.

Due to the computer processing technology available, passphrases not meeting the requirements in this manual are able to be retrieved using brute force attacks in a short period of time. Passphrases will have to increase in length and complexity as better processing technology becomes available.

Control: 0417; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use a numerical password (or personal identification number) as the sole method of authenticating a user.

Control: 0421; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S; Compliance: must; Authority: AA
Agencies using passphrases as the sole method of authenticating a user must implement a passphrase policy enforcing either:

- a minimum length of 13 alphabetic characters with no complexity requirement; or
- a minimum length of 10characters, consisting of at least three of the following character sets:
  - lowercase alphabetic characters (a–z)
  - uppercase alphabetic characters (A–Z)
  - numeric characters (0–9)
  - special characters.

Control: 0422; Revision: 3; Updated: Feb-14; Applicability: TS; Compliance: must; Authority: AA
Agencies using passphrases as the sole method of authenticating a user must implement a passphrase policy enforcing either:

- a minimum length of 15 alphabetic characters with no complexity requirement; or
- a minimum length of 11 characters, consisting of at least three of the following character sets:
  - lowercase alphabetic characters (a–z)
  - uppercase alphabetic characters (A–Z)
  - numeric characters (0–9)
  - special characters.

Multi–factor authentication

Multi–factor authentication is one of the most effective controls an agency can implement to prevent a cyber intruder from propagating on a network and identifying and accessing sensitive information during a targeted cyber intrusion. Intruders frequently attempt to steal legitimate user or administrative credentials when they compromise a network. These credentials allow them to easily propagate through a network and conduct malicious activities without requiring additional exploits, thereby reducing the likelihood of detection.

To provide a secure authentication mechanism that is not as susceptible to brute force attacks, multi–factor authentication should be used for all accounts. Using multi–factor authentication will also reduce the demands on users to remember long passphrases.

Privileged accounts are targeted by adversaries as they can potentially allow access to the entire system. For this reason, it is important that stronger authentication is used for positions of trust, such as an account that is able to approve financial transactions or accounts that have access to sensitive information. Using multi–factor authentication for positions of trust, including access to sensitive information and databases, and privileged accounts provides a more secure authentication mechanism.

The use of multi–factor authentication for remote access does not fully mitigate users entering their passphrase on a compromised computing device. An adversary may obtain a user's passphrase when it is entered into a less trustworthy computing device used for remote access. The adversary may then use this passphrase as part of a subsequent intrusion, for example, by either gaining physical access to a corporate workstation and simply logging in as the user, or by using this passphrase to access sensitive corporate resources as part of a remote intrusion against the corporate network. Mitigations include using multi–factor authentication for all user logins including corporate workstations in the office, or ensuring that user passphrases for remote access are different to passphrases used for corporate workstations in the office. 'Remote access' constitutes remote desktop access, and does not include web–based access to DMZ resources (for example, web portal access).

Some methods of multi–factor authentication are more effective than others. It is therefore essential to correctly implement and configure your multi–factor authentication solution on your network to ensure vulnerabilities are minimised. Further guidance can be found in ASD's Protect publication *Multi–factor Authentication*.

Control: 1173; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use multi–factor authentication for privileged access, positions of trust and remote access.

Control: 0974; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use multi–factor authentication for all users.

Control: 1357; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where multi–factor authentication is implemented, none of the factors on their own should be useful for authentication on another system.

Protecting stored authentication information

Limiting the storage of unprotected authentication information reduces the security risk of an intruder finding and using the information to access a system under the guise of a valid user.

Control: 0418; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
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.

Protecting authentication data in transit

Secure transmission of authentication information reduces the security risk of an intruder intercepting and using the authentication information to access a system under the guise of a valid user.

Control: 0419; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that system authentication data is protected when in transit across networks.

Passphrase management

Good passphrase management practices provide a means of limiting the consequences of the disclosure of passphrases to unauthorised users. Requiring a passphrase to be changed at least every 90 days limits the time period in which a disclosed password could be used by an authorised user.

For the enforcement of password changing policies to be effective, steps also need to be taken to ensure users choose strong passwords and prevent users reverting to their old password or selecting new passwords which could be easily guessed based on knowledge of the user's previous password. These steps are detailed below.

- Preventing a user from changing their passphrase more than once a day stops the user from immediately changing their passphrase back to their old passphrase.
- Checking passphrases for compliance with the passphrase selection policy allows system administrators to detect unsafe passphrase selection and ensure that the user changes it.
- Disallowing predictable reset passphrases reduces the security risk of brute force attacks and passphrase guessing attacks.
- Forcing a user to change a passphrase when resetting accounts ensures that the user changes the passphrase and it is a passphrase that only they know and remember.
- Using different passphrases when resetting multiple accounts prevents a user whose account has been recently reset from logging into another such account.
- Disallowing passphrases from being reused within eight changes prevents a user from cycling between a small subset of passphrases.
- Disallowing sequential passphrases reduces the security risk of an intruder easily guessing a user's next passphrase based on their knowledge of the user's previous passphrase.

Control: 0423; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should:

- ensure that passphrases are changed at least every 90 days
- prevent users from changing their passphrase more than once a day
- check passphrases for compliance with their passphrase selection policy where the system cannot be configured to enforce complexity requirements
- force the user to change an expired passphrase on initial logon or if reset.

Control: 0424; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S; Compliance: should not; Authority: AA
Agencies should not:

- store passphrases in the clear on the system
- allow passphrases to be reused within eight passphrase changes
- allow users to use sequential passphrases.

Control: 0425; Revision: 2; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Agencies must:

- ensure that passphrases are changed at least every 90 days
- prevent users from changing their passphrase more than once a day
- check passphrases for compliance with their passphrase selection policy where the system cannot be configured to enforce complexity requirements
- force the user to change an expired passphrase on initial logon or if reset.

Control: 0426; Revision: 2; Updated: Sep-12; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not:

- store passphrases in the clear on the system
- allow passphrases to be reused within eight passphrase changes
- allow users to use sequential passphrases.

Resetting passphrases

To reduce the likelihood of social engineering attacks aimed at service desks, agencies need to ensure that users provide sufficient evidence to verify their identity when requesting a passphrase reset for their system account. This evidence could be in the form of the user either:

- physically presenting themselves and their security pass to service desk personnel who then reset their passphrase
- physically presenting themselves to a known colleague who uses an approved online tool to reset their passphrase
- establishing their identity by responding correctly to a number of challenge response questions before resetting their own passphrase.

Issuing users with complex reset passphrases ensures the security of the user account is maintained during the passphrase reset process. This also represents a good opportunity for service desk staff to demonstrate to users an example of a good passphrase.

Control: 0976; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure users provide sufficient evidence to verify their identity when requesting a passphrase reset for their system account.

Control: 1227; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure reset passphrases are:

- unique to each individual reset
- not reused when resetting multiple accounts
- not based on a single dictionary word
- not based on another identifying factor, such as the user's name or the date.

Passphrase authentication

Local Area Network (LAN) Manager's authentication mechanism uses a very weak hashing algorithm known as the LAN Manager hash algorithm. Passphrases hashed using the LAN Manager hash algorithm can easily be compromised using rainbow tables or brute force attacks.

Control: 1055; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable LAN Manager for passphrase authentication on workstations and servers.

Session termination

Developing a policy to automatically logout and shutdown workstations after an appropriate time of inactivity helps prevent the compromise of a workstation that has been authenticated to and contains sensitive or classified information in memory. Such a policy also reduces the power consumption of systems during non–operational hours.

Control: 0853; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity.

Session and screen locking

Screen and session locking prevents unauthorised access to a system to which an authorised user has already been authenticated to.

Ensuring that the screen does not appear to be turned off while in the locked state prevents users forgetting they are still logged in and will prevent other users mistakenly thinking there is a problem with a workstation and resetting it.

Control: 0427; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should:

- configure systems with a session or screen lock
- configure the lock to activate either:
  - after a maximum of 15 minutes of user inactivity
  - if manually activated by the user.
- configure the lock to completely conceal all information on the screen
- ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated
- have the user reauthenticate to unlock the system
- deny users the ability to disable the locking mechanism.

Control: 0428; Revision: 3; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Agencies must:

- configure systems with a session or screen lock
- configure the lock to activate either:
  - after a maximum of 10 minutes of user inactivity
  - if manually activated by the user.
- configure the lock to completely conceal all information on the screen
- ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated
- have the user reauthenticate to unlock the system
- deny users the ability to disable the locking mechanism.

Suspension of access

Locking a user account after a specified number of failed logon attempts reduces the security risk of brute force attacks. Removing a user account when it is no longer required prevents personnel accessing their old account and reduces the number of accounts that can be targeted. Suspending inactive accounts after a specified number of days reduces the number of accounts that can be targeted. Investigating repeated account lockouts reduces the security risk of any ongoing brute force logon attempts and allows security management to act accordingly.

Implementing account lockout functionality in a web application can increase the risk of a DoS attack. This is because this function makes it simple for a malicious actor to deliberately input wrong passwords enough times to lock users out of their accounts. Implementing an appropriate password reset functionality can help mitigate DoS effects if a web application has locked out a user.

Control: 0430; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must:

- lock user accounts after a maximum of five failed logon attempts
- have a system administrator reset locked accounts
- remove or suspend user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency
- remove or suspend inactive accounts after a specified number of days.

Investigating repeated account lockouts

Repeated account lockouts may be an indication of malicious activity being directed towards compromising a particular account.

Control: 0431; Revision: 1; Updated: Nov-10; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that repeated account lockouts are investigated before reauthorising access.

Logon banner

A logon banner for a system reminds users of their responsibilities when using the system.

Control: 0408; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should have a logon banner that requires a user to acknowledge and accept their security responsibilities before access to the system is granted.

Control: 0979; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should seek legal advice on the exact wording of logon banners.

Control: 0980; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Logon banners should explicitly state conditions of access to a system, including:

- access is restricted to authorised users
- acceptable usage and information security policies
- the user's agreement to abide by abovementioned policies
- informing the user of activity monitoring and auditing
- legal ramifications of violating the relevant policies
- a point of contact for questions on these conditions.

Displaying when a user last logged in

Displaying when a user has last logged onto a system helps users identify any unauthorised use of their account. Accordingly, when any case of unauthorised use of an account is identified, it should be reported to an ITSM immediately so that it can be investigated.

Control: 0977; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should configure systems to display the date and time of the user's previous login during the login process.

References

Information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*

Further guidance on implementing multi–factor authentication can be found in ASD's Protect publication *Multi–factor Authentication*. Further guidance on mitigating the use of stolen credentials can be found in ASD's Protect publication *Mitigating the Use of Stolen Credentials to Access Agency Information*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

System Access

Objective

Access to information on systems is controlled through appropriate access controls.

Scope

This section describes security controls for accessing systems.

Context

Additional information on security clearance, briefing and authorisation requirements can be found in the *Privileged Access* section of this chapter and the *Authorisations, Security Clearances and Briefings* section of the *Personnel Security for Systems* chapter.

Controls

Access from foreign controlled systems and facilities

If an Australian system is to be accessed from overseas, it needs to be from at least a facility owned by a foreign government with which Australia has a security of information arrangement. Furthermore, due to the sensitivities involved with AUSTEO and AGAO systems, such systems can only be accessed from facilities under the sole control of the Australian Government.

Control: 0855; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Unless a security of information arrangement is in place with a foreign government, agencies should not allow access to sensitive or classified information from systems and facilities not under the sole control of the Australian Government.

Control: 0854; Revision: 2; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow access to AUSTEO or AGAO information from systems and facilities not under the sole control of the Australian Government.

Enforcing authorisations on systems

Enforcing authorisations of users through the use of access controls on a system decreases the risk of unauthorised disclosure of classified or sensitive information. Agencies should follow a process for developing an access control list, such as:

- establish groups of all system resources based on similar security objectives
- determine the information owner for each group of resources
- establish groups encompassing all users based on similar functions or security objectives
- determine the group owner or manager for each group of users
- determine the degree of access to the resource for each user group
- decide on the degree of delegation for security administration, based on the internal security policy.

Control: 0856; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have users' authorisations enforced by access controls.

Protecting compartmented information on systems

Compartmented information is particularly sensitive. Therefore, extra security measures need to be put in place on systems to restrict access to those with sufficient authorisations, briefings and a demonstrated need–to–know.

Control: 0857; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have access to compartmented information enforced by the system access controls.

References

Nil.

Privileged Access

Objective

Privileged access to systems is appropriately controlled and monitored.

Scope

This section describes what must be in place to control and monitor privileged access to systems.

Context

In this section, privileged access is considered to be access which can give a user one or more of:

- 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 users, including backups and media
- special access for troubleshooting the system.

The requirements for using multi–factor authentication for privileged access are included in the *Identification and Authentication* section of this chapter.

Controls

Use of privileged accounts

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 on systems that lead to cyber security incidents.

Privileged access allows system–wide changes to be made. An appropriate and effective mechanism to log privileged users will provide greater accountability and auditing capabilities.

Privileged accounts are targeted by adversaries as these can potentially give full access to the system. Ensuring that privileged accounts do not have a channel from inside the agency to the Internet minimises opportunities for these accounts to be compromised.

Control: 1175; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow privileged accounts access to the Internet or to email.

Control: 0445; Revision: 4; Updated: Aug-13; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must:

- ensure that the use of privileged accounts is controlled and auditable
- ensure that system administrators are assigned a separate account for the performance of their administration tasks
- keep privileged accounts to a minimum
- allow the use of privileged accounts for administrative work only
- regularly audit the passphrases of privileged accounts to check they meet length or complexity requirements
- regularly audit the passphrases of privileged accounts to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts)
- regularly review privileges allocated to privileged user accounts.

Privileged system access by foreign nationals

As privileged users often have the ability to bypass controls on a system it is strongly encouraged that foreign nationals are not given privileged access to systems processing particularly AUSTEO or AGAO information.

Control: 0446; Revision: 1; Updated: Sep-09; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate AUSTEO information.

Control: 0447; Revision: 1; Updated: Sep-09; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow foreign nationals, excluding seconded foreign nationals, to have privileged access to systems that process, store or communicate AGAO information.

Control: 0448; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate sensitive or classified information.

References

Further guidance on minimising administrative privileges can be found in ASD's Protect publication *Minimising Administrative Privileges Explained*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Remote Access

Objective

Remote access to systems is authorised and authenticated.

Scope

This section describes the authentication required by personnel to access a system from a remote location.

Context

Remote access

Remote access is user access to agency systems originating outside an agency network. It does not include web–based access to DMZ resources.

Further information on working off–site can be found in the *Working Off–Site* chapter. The requirements for using multi–factor authentication for remote access are included in the *Identification and Authentication* section of this chapter.

Remote privileged access

Remote privileged access by a privileged user to an agency system via a less trusted security domain (for example, the Internet) may represent additional risk to the system. Controls in this section aim to prevent escalation of user privileges from a compromised remote access account.

Remote privileged access does not include privileged access across disparate physical sites that are within the same security domain or privileged access across remote sites that are connected via trusted infrastructure. Privileged access of this nature faces different threats to those discussed above. Ensuring robust processes and procedures are in place within an agency to monitor and detect the threat of a malicious insider are the most important measure for this scenario.

Controls

Authentication

Authenticating remote users and devices ensures that only authorised users and devices are allowed to connect to systems.

Control: 0858; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must authenticate each remote connection before permitting access to a system.

Control: 0706; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should authenticate both the remote user and device during the authentication process.

Remote privileged access

The extent of a compromise of remote access to a system can be limited by preventing the use of remote privileged access.

Control: 0985; Revision: 4; Updated: Sep-12; Applicability: G, P; Compliance: should not; Authority: AA
Agencies should not allow the use of privileged access remotely, including logging in as an unprivileged user and then escalating privileges.

Control: 0709; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow the use of privileged access remotely, including logging in as an unprivileged user and then escalating privileges.

References

Nil.

Event Logging and Auditing

Objective

Security related events are logged and audited.

Scope

This section describes automatic logging of information relating to network activities.

Context

Information on event logging associated with a cyber security incident can be found in the *Cyber Security Incidents* section.

A security event is an evident change to the normal behaviour of a network, system or user. Event logging helps raise the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected. Agencies should ensure sufficient detail is recorded in order for the logs to be useful when reviewed and determine an appropriate length of time for them to be retained. Conducting audits of event logs should be seen as an integral part of the maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

Controls

Logging requirements

Event logging helps raise the security posture of a system by increasing the accountability for all user actions.

Event logging increases the chances that malicious behaviour will be detected by logging the actions of a malicious party.

Well configured event logging allows for easier and more effective auditing if a cyber security incident occurs.

Control: 0580; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop and document logging requirements covering:

- the logging facility, including:
  - log server availability requirements
  - the reliable delivery of log information to the log server.
- the list of events associated with a system or software component to be logged
- event log protection and retention requirements.

Events to be logged

The events to be logged are listed in their importance to monitoring the security posture of systems and contributing to reviews, audits and investigations.

Control: 0582; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S; Compliance: should; Authority: AA
Agencies should log, at minimum, the following events for all software components:
- all privileged operations
- failed attempts to elevate privileges
- security related system alerts and failures
- user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 0583; Revision: 2; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Agencies must log, at minimum, the following events for all software components:
- all privileged operations
- failed attempts to elevate privileges
- security related system alerts and failures
- user and group additions, deletions and modification to permissions
- unauthorised access attempts to critical systems and files.

Control: 1176; Revision: 1; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Agencies should log the following events for any system requiring authentication:
- logons
- failed logon attempts
- logoffs.

Control: 0584; Revision: 1; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must log the following events for any system requiring authentication:
- logons
- failed logon attempts
- logoffs.

Additional events to be logged

The additional events to be logged below can be useful for reviewing, auditing or investigating software components of systems.

Control: 0987; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should log the events listed below for specific software components.

SOFTWARE COMPONENT	EVENTS TO LOG
Database	User access to the database
	Attempted access that is denied
	Changes to user roles or database permissions
	Addition of new 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 user accounts
	Failed attempts to access data and system resources
	Attempts to use special privileges
	Use of special privileges
	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
	Transfer of data to external media
	DNS (Domain Name System) and HTTP requests
Web application	User access to the web application
	Attempted access that is denied
	User access to the web documents
	Search engine queries initiated by users

Event log facility

For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed.

Control: 0585; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA

For each event identified as needing to be logged, agencies must ensure that the log facility records at least the following details, where applicable:

- date and time of the event
- relevant users or process
- event description
- success or failure of the event
- event source (for example, application name)
- ICT equipment location/identification.

Control: 0988; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should establish an accurate time source, and use it consistently throughout their systems, to assist with the correlation of logged events across multiple systems.

Event log protection

Effective log protection and storage (possibly involving the use of a dedicated event log server) will help ensure the integrity and availability of the collected logs when they are audited.

Control: 0586; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Event logs must be protected from:

- modification and unauthorised access
- whole or partial loss within the defined retention period.

Control: 1344; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that systems are configured to save event logs to a separate secure log server.

Control: 0989; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that event log data is archived in a manner that maintains its integrity.

Control: 0587; Revision: 1; Updated: Nov-10; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should configure systems to save event logs to separate secure servers as soon as possible after each event occurs.

Event log retention

It is important that agencies determine an appropriate length of time to retain event logs for systems. Since event logs can assist in reviews, audits and investigations, logs should ideally be retained for the life of the system and potentially longer. The retention requirement for these records under National Archives of Australia's (NAA's) *Administrative Functions Disposal Authority* is a minimum of 7 years after action is completed.

Control: 0859; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must retain event logs for a minimum of 7 years after action is completed in accordance with the NAA's *Administrative Functions Disposal Authority*.

Control: 0991; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should retain DNS and proxy logs for at least 18 months.

Event log auditing

Conducting audits of event logs should be seen as an integral part of the maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions. Agencies can use a centralised audit system to correlate logs from multiple sources to identify patterns of suspicious behaviour. This functionality may be provided by existing systems such as the Security Information and Event Management solution. Automated solutions are available to help agencies proactively identify such patterns.

Control: 0109; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop and document event log auditing requirements covering:

- the scope of audits
- the audit schedule
- what constitutes a violation of information security policy
- action to be taken when violations are detected
- reporting requirements
- specific responsibilities.

Control: 1228; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should correlate events across logs to prioritise audits and focus investigations.

References

Further information on retaining event logs can be found in the NAA's *Administrative Functions Disposal Authority.*

Secure Administration

Objective

Administration of agency networks and systems is performed in a secure and resilient manner.

Scope

This chapter describes the security controls and processes which can improve the security of administrative credentials, infrastructure and actions performed on a network or system.

The rationale and controls within this chapter are intended to apply to the administration of business defined critical assets by highly privileged administrators as opposed to, for example, the administration of user workstations by helpdesk or similar support staff.

Context

Secure enterprise administration allows agencies to be resilient in the face of malicious cyber intrusions by protecting privileged machines and accounts from compromise, as well as making adversary movement throughout a network more difficult. If a secure administration system withstands a cyber intrusion and remains clean after other areas of the environment have been compromised, incident response will be far more agile, the damage will be limited and remediation work will be completed faster. The controls in this chapter are designed to protect the administration of a network even if an adversary has already compromised unprivileged elements of the network.

A jump server (also known as a jump host or jump box) is a computer which is used to manage sensitive or critical resources in a separate security domain.

With the increased use of cloud–based resources agencies may require administrative assets to communicate with external assets on the Internet. In this scenario it is still important that controls are put in place to prevent unnecessary communication with arbitrary hosts and protocols.

Further information on remote access to privileged accounts can be found in the *Remote Access* section of the *Access Control* chapter. The requirements for using multi–factor authentication for remote access are included in the *Identification and Authentication* section of the *Access Control* Chapter. Further information about network segmentation for security purposes can be found in the *Network Design and Configuration* section of the *Network Security* chapter.

Controls

Separate administrator workstations

One of the greatest threats to the security of a network as a whole is the compromise of a workstation used for IT administration.

Providing a physically separate, hardened workstation to administrators responsible for critical assets in addition to their workstation used for unprivileged user access provides greater assurance that administrator activities and credentials will not be compromised.

The use of the same credentials on both the dedicated administration workstation and regular use workstation puts the dedicated workstation at risk if the regular workstation is compromised. The table below provides clarification on the different accounts.

REGULAR USER ACCOUNT	UNPRIVILEGED ADMINISTRATION ACCOUNT	PRIVILEGED ADMINISTRATION ACCOUNT
• Used for web and email access • Day to day non–administrative tasks • Unprivileged account	• Authentication to dedicated administration workstation • Authentication to jump server(s) • Different username and password to Regular User Account • Unprivileged account	• Used for performance of administration tasks • Privileged account

Control: 1380; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Administrators should use a dedicated physical workstation when performing administrative tasks on critical assets.

Control: 1381; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that dedicated administration workstations are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.

Control: 1382; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that administrators are assigned an unprivileged administration account for authenticating to their dedicated administration workstations.

Control: 1383; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all administrative infrastructure including, but not limited to, administrator workstations and jump servers are hardened appropriately as per the recommendations in the *Software Security* chapter.

Multi–factor authentication

Multi–factor authentication is a vital component of any secure administration implementation. Multi–factor authentication can limit the consequences of a compromise by preventing or slowing the adversary's ability to gain unrestricted access to assets secured using multi–factor authentication.

Multi–factor authentication can be implemented as part of the jump server authentication process rather than performing multi–factor authentication on all critical assets and actions, some of which may not support multi–factor authentication.

Agencies should refer to the *Identification and Authentication* section of the *Access Control* chapter for further multi–factor authentication guidance.

Control: 1384; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all administrative actions have passed through at least one multi–factor authentication process.

Dedicated administration zones and communication restrictions

Administration security can be improved by segregating administrator workstations from the wider network. There are a number of ways through which this segregation can be achieved, including:

- virtual LANs
- firewalling
- Network Access Control
- IPsec Server and Domain Isolation.

It is recommended that segmentation and segregation be applied regardless of whether administrators have a physically separate workstation for administrative purposes, or a regular workstation used by administrators.

Control: 1385; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should place the workstations used for administrative purposes into a separate administrative network zone as outlined in the *Network Design and Configuration* section of the *Network Security* chapter.

Restriction of management traffic flows

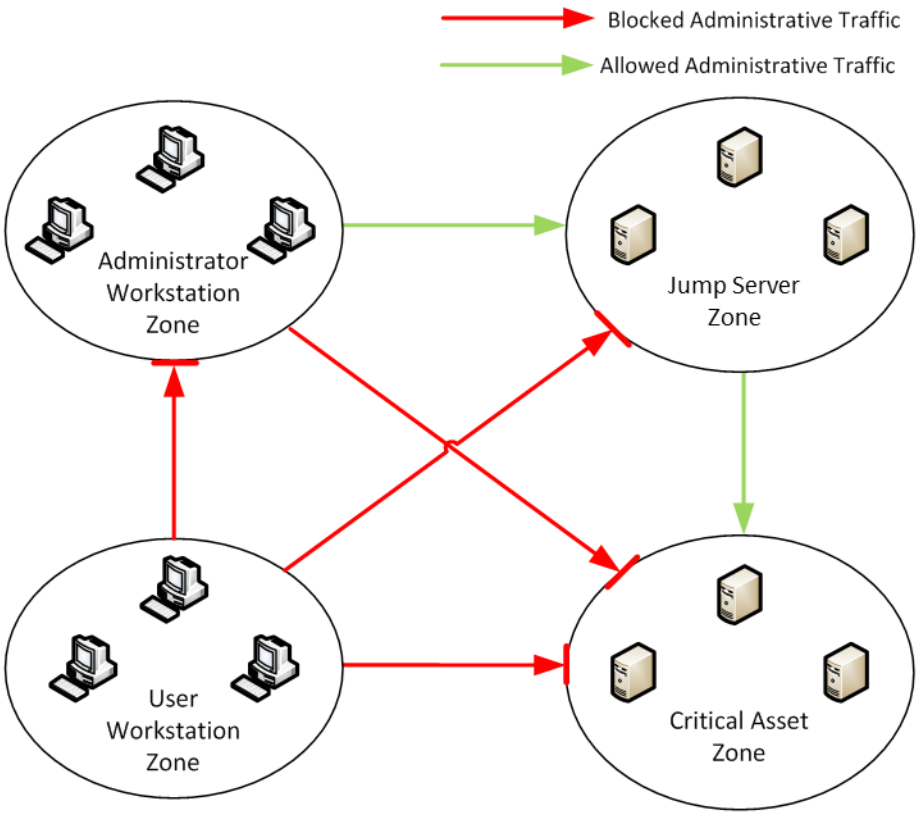
Limiting the flow of management traffic to those network elements and segments explicitly required to communicate can reduce the consequences of a network compromise and make such a compromise easier to detect.

Although regular user workstations will have a need to communicate with critical assets such as web servers or domain controllers in order to function, it is highly unlikely that they need to send or receive management traffic (such as RDP, SSH and similar protocols) to these critical assets.

When designing a network for secure administration, agencies should follow the recommendations outlined in the *Network Design and Configuration* section of the *Network Security* chapter.

The following diagram outlines how management traffic filtering could be implemented between a network consisting of different zones. The only flows of management traffic allowed are those:

- between the 'Administrator Workstation Zone' and the 'Jump Server Zone', and;
- between the 'Jump Server Zone' and the 'Critical Asset Zone'.



All other traffic is blocked as there is no reason for management traffic to flow between the other zones since jump servers have been implemented and a dedicated administrator workstation zone has been created.

Control: 1386; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should only allow the flow of management traffic between network zones and assets required to perform administrative tasks and block management traffic from unauthorised sources.

Jump servers

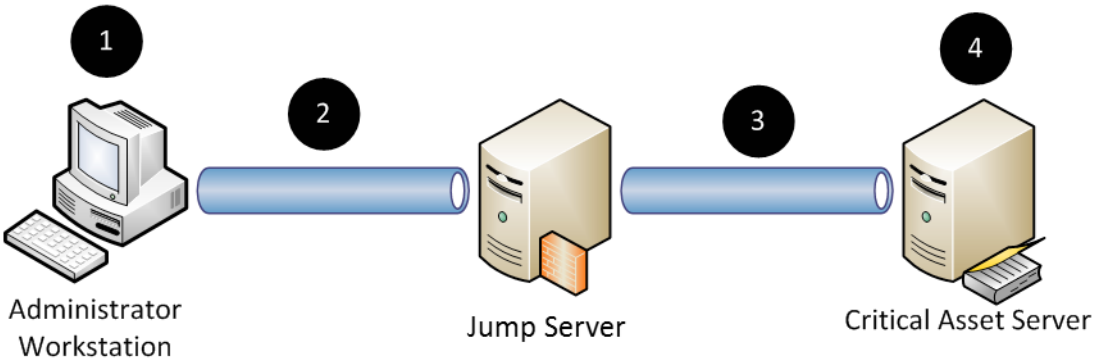
The use of jump servers as a form of 'management proxy' can be an effective way of simplifying and securing administration activities. Implementing a jump server can yield the following benefits:

- An efficient and effective focal point to perform multi–factor authentication.
- A single place to store and patch management tools.
- Simplifies the implementation of the management traffic filtering.
- A focal point for logging, monitoring and alerting.

In a typical scenario when an administrator wants to perform administrative activities they would connect directly, using RDP or SSH for example, to the target server.

In a jump server setup and administrator would first connect and authenticate to the jump server, then RDP or SSH to the target server.

When implementing a jump server it is recommended that agencies first implement multi–factor authentication, enforce strict device communication restrictions and harden administrative infrastructure otherwise a jump server will yield little security benefit.



1 Administrator authenticates to dedicated administration workstation using the Unprivileged Administration Account

2 Administrator connects (RDP, SSH) to Jump Server using their Unprivileged Administration Account

3 Administrator connects (RDP, SSH) to target server using their Privileged Administration Account

4 The Administrator, now authenticated as a privileged user, performs their administrative task.

Control: 1387; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that all administrative actions are conducted through a jump server.

Control: 1388; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that jump servers are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.

References

Further guidance on mitigating the use of stolen credentials can be found in ASD's Protect publication *Mitigating the Use of Stolen Credentials to Access Agency Information*.

Additional information and guidance can also be found in Microsoft's *Mitigating Pass–the–Hash (PtH) Attacks and Other Credential Theft Techniques* at http://www.microsoft.com/en-au/download/confirmation.aspx?id=36036.

Network Security

Network Management

Objective

The configuration of networks is controlled through appropriate change management processes.

Scope

This section describes the management of network infrastructure.

Context

Agencies can structure and configure their networks to reduce the number of potential entry points that could be used to gain unauthorised access to information or disrupt agency services. Appropriate network management practices and procedures can assist in identifying and addressing network vulnerabilities.

Further information regarding the appropriate selection of products such as automated tools can be found in the *Product Selection and Acquisition* section of the *Product Security* chapter.

Controls

Configuration management

If the network is not centrally managed there could be sections of the network that do not comply with information security policies.

Control: 0513; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should keep the network configuration under the control of a central network management authority.

Approval of all changes by a change management process involving representatives from all parties involved in the management of the network ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the network.

Control: 0514; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
All changes to the network configuration should be documented and approved through a formal change control process.

Control: 0515; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should regularly review their network configuration to ensure that it conforms to the documented network configuration.

Control: 1007; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should deploy an automated tool that compares the running configuration of network devices against the documented configuration.

Network documentation

Detailed network documentation and configuration details can contain information about IP addresses, software version numbers and patch status, security enforcing devices and information about enclaves, which is highly valuable information. This information could be used by a malicious actor to compromise an agency's network.

Control: 1177; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Detailed network configuration documentation must be classified to at least the same level as the network or enclave it covers.

Control: 1178; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Network documentation provided to a third party, such as to a commercial provider, must only contain information necessary for them to undertake their contractual services and functions, in line with the need–to–know principle.

Control: 1179; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform a security risk assessment before providing network documentation to a third party, such as a commercial provider.

Control: 1180; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Detailed network configuration information must not be published in tender documentation.

Network diagrams

A network diagram illustrates all network devices such as firewalls, IDSs and Intrusion Prevention Systems (IPSs), routers and switches. It does not need to illustrate all ICT equipment on the network, such as workstations or printers, although the inclusion of significant devices such as servers could aid in its interpretation.

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
- the network diagram indicates when it was last updated.

Control: 0516; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
For each network an agency must have:

- a high–level diagram showing all connections into the network
- a logical network diagram showing all network devices.

Updating network diagrams

Due to the importance of the network diagram, and decisions made based upon its contents, it is important to update the network diagram as changes are made to the network. This will assist system administrators to completely understand and adequately protect the network.

Control: 0518; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Network diagrams must:

- be updated as network changes are made
- include a 'Current as at [date]' statement on each page.

Accounting for network devices

Maintaining and regularly auditing an inventory of authorised network devices will assist in determining whether devices such as switches, routers and wireless access points on a network are rogue.

Control: 1301; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
An inventory of authorised network devices should be maintained and audited on a regular basis.

Manual methods that may be used to detect network devices include network scans and physical inspections while automated methods include network access controls and IDSs and IPSs. These audit methods aim to detect the presence of network devices inserted into or hidden inside systems, portable devices connected to workstations via USB ports and devices attached to a network port. It is important to note that network scans conducted over a network may not be able to detect network devices hidden inside workstations or connected via USB ports.

Control: 1302; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use an audit method capable of detecting the presence of network devices inserted into or hidden inside systems, portable devices connected to workstations via USB ports and devices attached to a network port.

Auditing of network devices that are being added or removed from networks may indicate an attempt to introduce a backdoor into a network or to conduct a DoS attack against the network.

Control: 1303; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should audit network devices that are being added or removed from networks.

References

Nil.

Network Design and Configuration

Objective

Networks including fixed, wireless and Virtual Local Area Networks (VLANs) are deployed in a secure manner that does not compromise the security of information and systems.

Scope

This section describes the design and configuration of networks.

Context

This section should be read in conjunction with the *Servers and Network Devices* section of the *Physical Security* chapter. Additional information specific to wireless networks can be found in the *Wireless Local Area Networks* section of this chapter, while additional information on deploying IDSs and IPSs can be found in the *Intrusion Detection and Prevention* section of this chapter.

Separation of networks in the same security domain

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.

VLANs can also be used to separate IP telephony traffic from data traffic at the same sensitivity or classification.

Multi Protocol Label Switching

For the purposes of this section, Multi Protocol Label Switching is considered to be equivalent to VLANs and is subject to the same controls.

Controls

Network segmentation

Network segmentation is one of the most effective controls to prevent an intruder from propagating through an agency's network once they have gained access. Well–implemented network segmentation can significantly increase the difficulty for an intruder to find and access their target information and move undetected around the network. Technologies to enforce network segmentation contain logging functionality which can prove extremely valuable in detecting an intrusion and, in the event of a compromise, isolating a compromised device from the rest of the network.

Network segmentation involves separating a network into multiple functional zones, with a view to protecting sensitive information and critical services (such as user authentication and user directory information). For example, one network zone may contain user workstations while authentication servers are in a separate zone. The growth of social engineering as a method to directly target internal agency networks is making it increasingly important for agencies to separate sensitive information from the environment where their users access the Internet and email.

Proper network segmentation assists in the creation and maintenance of proper network access control lists.

Control: 1181; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should divide their networks into multiple functional zones according to the sensitivity or criticality of information or services in that zone.

Control: 1346; Revision: 0; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Agencies should separate and apply additional security protections to network zones that contain sensitive information from the environment where their users access the Internet and external email.

Management traffic

Implementing security measures specifically for management traffic provides another layer of defence on a network should an intruder find an opportunity to connect to the network. This also makes it more difficult to enumerate their target network.

Control: 1006; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement security measures to minimise the risk of unauthorised access to network management traffic on a network.

Limiting network access

If a malicious actor has limited opportunities to connect to a given network, they have limited opportunities to compromise that network. Network access controls, for example 802.1X, not only prevent unauthorised access to a network but also prevent users carelessly connecting a network to another network.

Network access controls are also useful in segregating sensitive or compartmented information for specific users with a need–to–know or limiting the flow of information between network segments. For example, computer management traffic can be permitted between workstations and systems used for administration purposes, but not permitted between workstation to workstation.

Circumventing some network access controls can be trivial. However, their use is primarily aimed at the protection they provide against accidental connection to another network.

Control: 0520; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement network access controls on all networks.

Control: 1182, Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement network access controls to limit traffic within and between network segments to only those that are required for business operations.

Disabling unused physical ports

Disabling unused physical ports on network devices such as switches, routers and wireless access points reduces the attack surface from which intrusions could be launched.

Control: 0533; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S; Compliance: should; Authority: AA
Unused physical ports on network devices should be disabled.

Control: 0534; Revision: 1; Updated: Sep-12; Applicability: TS; Compliance: must; Authority: AA
Unused physical ports on network devices must be disabled.

Default usernames and passwords for network devices

Network devices such as switches, routers and wireless access points come pre–configured with default accounts and passwords that are freely available in product documentation and online forums. For example, it is common for wireless access points to come pre–configured with an administrator account named "admin" and a password of either "admin" or "password". Ensuring default usernames and passwords are changed before they are deployed in a network will decrease the risk of the names and passwords being exploited to gain unauthorised access to network devices.

Control: 1304; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Default usernames and passwords must be changed before network devices are deployed in networks.

Time synchronisation between network devices

When intrusions or attacks occur against networks it is critical that any events logged can be correlated with other network devices and their event logs. Synchronising all clocks between network devices will enable accurate correlation. This is generally achieved through the use of a dedicated time server on the network.

Control: 1305; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
All clocks should be synchronised between network devices.

Updating firmware for network devices

The operation of network devices is controlled by software known as firmware. Periodically network device vendors will release updated firmware to fix software bugs, resolve security issues and add new functionality and features. A security risk exists for agencies that do not update the firmware for network devices as known software bugs and security issues may be exploited to gain access to their networks. Keeping firmware for network devices up to date will assist in reducing this risk.

Control: 1306; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Firmware for network devices must be kept up to date.

Securing devices accessing networks

Devices, particularly privately owned devices and mobile devices, used to access networks have the potential to have been exposed to viruses, or malicious software or code when previously connected to non–agency networks such as the Internet and mobile networks. This presents a security risk as these devices could inadvertently be infecting other devices on networks, leveraging a user's legitimate access to steal an agency's sensitive or classified information or impacting the availability of networks. Validating a device as secure through the use of network access control before being granting access to networks will assist in reducing this risk. Using network access control, system administrators can set policies for system health requirements. This can include a check that all operating system patches are up to date, an anti–virus program is installed, all signatures are up to date, and that a software firewall is installed and being used. Devices that comply with all health requirements can be granted access to networks, while devices that do not comply can be quarantined or granted limited access.

Control: 1307; Revision: 1; Updated: Apr-13; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use network access control to validate devices as secure before granting them access to networks.

Bridging networks

Allowing devices that are connected to an agency controlled network to simultaneously connect to another non–agency controlled network allows the devices to act as a gateway by bridging the two networks. This opens an attack vector into an agency controlled network.

Control: 1345; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Devices must be prevented from simultaneously connecting to an agency controlled network and to a non–agency controlled data network such as the Internet.

Control: 1308; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should disable the following features on devices:

- ad hoc networks
- routing between virtual private network interfaces and other network interfaces
- Internet–connection sharing.

Intrusion detection and prevention

Special anomaly detection techniques can be used by IDSs and IPSs. IDSs will raise alerts to system administrators when any anomalous activity is detected on networks; while IPSs are capable of automatically quarantining suspected rogue devices from networks until they can be assessed by system administrators. Using either an IDS or IPS on networks is an effective way of identifying and responding to known intrusions profiles. Further information on implementing these systems can be found in the *Intrusion Detection and Prevention* section of this chapter.

Control: 1309; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use an IDS or IPS on networks.

Using Virtual Local Area Networks

Using network devices to only manage VLANs of different security domains at the same classification and not to manage VLANs of different security classifications or sensitivities will assist in reducing the security risk of data spills across VLANs. Furthermore, disabling trunking on network devices that carry VLANs of differing security domains will also reduce the security risk of data leakage across the VLANs.

Control: 1138; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Network devices must not be used to manage VLANs for both classified networks and unclassified networks or non–classified networks and unclassified networks.

Control: 1310; Revision: 1; Updated: Feb-14; Applicability: G, P; Compliance: should not; Authority: AA
Network devices should not be used to manage VLANs for both classified networks and non–classified networks.

Control: 1363; Revision: 0; Updated: Feb-14; Applicability: C, S, TS; Compliance: must not; Authority: AA
Network devices must not be used to manage VLANs for both classified networks and non–classified networks.

Control: 0529; Revision: 3; Updated: Feb-14; Applicability: C, S, TS; Compliance: must not; Authority: AA
Network devices must not be used to manage VLANs for networks of different classifications.

Control: 1364; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Network devices managing VLANs must terminate each VLAN of a different security domain on a separate physical network interface.

Control: 0535; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
VLAN trunking must not be used on network devices managing VLANs of differing security classifications.

Configuration and administration of network devices

When administrative access is limited to originating from the most trusted network on a network device using VLANs, the risk of a data spill is reduced.

Control: 0530; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Administrative access for network devices using VLANs must only be permitted from the most trusted network.

Using IP version 6

Introducing IP version 6 (IPv6) functionality into a network can potentially introduce additional security risks for an agency. Disabling IPv6 functionality until it is intended to be used will minimise the attack surface of the network. This will ensure that any IPv6 functionality that is not intended to be used cannot be exploited before appropriate security measures have been put in place. 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 security measures for IPv6 are working effectively and redundant IPv4 systems are disabled.

Control: 0521; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Dual–stack network devices, ICT equipment and operating systems that support IPv6 must disable the functionality unless it is being used.

Control: 0525; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies enabling a dual–stack environment or a wholly IPv6 environment must reaccredit their networks.

Control: 1186; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Network security devices, for example firewalls and IDSs/IPSs, on IPv6 or dual–stack networks must be IPv6 capable.

Use of Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices such as switches, routers and wireless access points. The first two iterations of SNMP were inherently insecure as they used trivial authentication methods. Disabling SNMP, or if required using SNMPv3, mitigates this risk. Furthermore, changing all default SNMP community strings on network devices and limiting access to read only access is desirable.

Control: 1311; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
SNMP should be disabled if its use is not required. If the use of SNMP is required, agencies should use SNMPv3.

Control: 1312; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
All default SNMP community strings should be changed on network devices and access should be limited to read only access.

References

A *Strategy for the Transition to IPv6 for Australian Government agencies* can be found on the Australian Government Information Management Office website at http://www.finance.gov.au/e-government/infrastructure/docs/Endorsed_Strategy_for_the_Transition_to_IPv6_for_Australian_Government_agencies.pdf.

Information on network plans can be found at the United States National Security Agency's document: http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf.

Information on network segmentation and segregation is available in ASD's Protect publication *Network Segmentation and Segregation* available at http://www.asd.gov.au.

Additional IPv6 information can be found at http://www.cpni.gov.uk/Documents/Publications/2006/2006005-TN0206_Security_IPv6.pdf.

Ensuring Service Continuity

Objective

Steps are taken to ensure that Internet services are available if an attacker attempts to flood an agency network with unwanted traffic.

Scope

This section outlines steps for minimising the effect of attacks aimed at disrupting or degrading Internet services provided to an agency.

Context

Additional information on business continuity and disaster recovery can be found in the *Information Security Monitoring* chapter.

Controls

Contacting Internet service providers

Internet service providers are in a unique position to assist in the mitigation of distributed denial–of–service (DDoS) attacks. Proper coordination between agencies and their Internet service providers is essential to ensure resilience against such attacks.

Control: 1188; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure their Internet service provider is capable of responding in the event of a DDoS attack against their network.

Planning

Effective planning with an Internet service provider is a key part of defending against DDoS attacks.

Control: 1189; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should agree upon a denial of service mitigation plan with their Internet service provider, outlining pre–approved actions that can be taken in the event of a DDoS attack.

Maintaining multiple Internet links

The use of multiple Internet links increases an agency's options for responding to DDoS attacks, and increases the complexity required for a successful DDoS attack.

Control: 1190; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use multiple Internet links provided by different Internet service providers.

Control: 1191; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Separate Internet links should be used for public facing services (e.g. web servers and public DNS) and routine business (e.g. Internet access for system users and remote connectivity).

References

Further guidance can be found in ASD's Protect publication *Denial of Service Attacks: Strategies for Mitigation*. Protect publications can be accessed through OnSecure, the ASD public website (in some cases) or upon request.

Wireless Local Area Networks

Objective

Wireless Local Area Networks are deployed and accessed in a secure manner that does not compromise the security of sensitive or classified information and systems.

Scope

This section describes 802.11 Wi–Fi based wireless networks.

Context

Information covering wireless communications other than 802.11 Wi–Fi, such as 802.15 Bluetooth, can be found in the *Communications Systems and Devices* chapter. Additional information on encryption and key management requirements for wireless networks can be found in the *Cryptography* chapter.

Controls

Using wireless communications

ASD is the accreditation authority for TOP SECRET systems, which includes wireless TOP SECRET networks.

Control: 0538; Revision: 3; Updated: Feb-14; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not use wireless networks unless the security of the wireless deployment has been approved by ASD.

Wireless networks for public access

When an agency introduces wireless networks for public access, e.g. a public hotspot, connecting such wireless networks to, or sharing infrastructure with any networks that communicate or store sensitive or classified information creates an entry point for an intruder to target a connected network to steal sensitive or classified information or disrupt services.

Control: 0536; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Wireless networks deployed for the general public to access must be physically segregated from all other agency networks.

Connecting wireless networks to fixed networks

When an agency has a business requirement to connect a wireless network to a fixed network, it is important that they consider the security risks. While fixed networks are often afforded a certain degree of physical security, wireless networks are often easily accessible outside of the controlled perimeter of an agency. Treating connections between wireless networks and fixed networks in the same way agencies would treat connections between fixed networks and the Internet can help protect against an intrusion originating from a wireless network against a fixed network. For example, by implementing a gateway to inspect and control the flow of information between the two networks.

Control: 1313; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Connections between wireless networks and fixed networks should be treated in the same way as connections between fixed networks and the Internet.

Choosing wireless access points

Wireless access points that have been certified against a Wi–Fi Alliance certification program provide an agency with the assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will prevent any problems on the network due to incompatibility of wireless standards supported or incorrect implementation of wireless standards by vendors.

Control: 1314; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All wireless access points used for wireless networks must be Wi–Fi Alliance certified.

Administrative interfaces for wireless access points

Administrative interfaces allow users to modify the configuration and security settings of wireless access points. Often wireless access points by default allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. Disabling the administrative interface on wireless access points will prevent unauthorised connections.

Control: 1315; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should disable the administrative interface on wireless access points for wireless connections.

Default service set identifiers

All wireless access points come with a default Service Set Identifier (SSID). The SSID is commonly used to identify the name of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passwords, it is important to change the default SSID of wireless access points.

Control: 1316; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must change the default SSID of wireless access points.

When changing the default SSID, it is important that the new SSID lowers the profile of an agency's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an agency, the location of or within their premises, or the functionality of the network.

Control: 1317; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
The SSID of a wireless network should not be readily associated with an agency, the location of or within their premises, or the functionality of the network.

A method commonly recommended to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re–association requests for the network. Some malicious actors will still be able to determine the SSID of wireless networks by capturing these requests and responses. Additionally, by disabling SSID broadcasting agencies will make it more difficult for users to connect to wireless networks as legacy operating systems only have limited support for hidden SSIDs. Furthermore, a risk exists where an intruder could configure a wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network.

In this scenario, devices will automatically connect to the wireless access point that is broadcasting the SSID they are configured to use before probing for a wireless access point that accepts the hidden SSID. Once the device is connected to the intruder's wireless access point the intruder can steal authentication credentials from the device to perform a man–in–the–middle attack to capture legitimate wireless network traffic or to later reuse to gain access to the legitimate wireless network. For these reasons, it is recommended agencies enable SSID broadcasting.

Control: 1318; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should enable SSID broadcasting on wireless networks.

Static addressing

Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a network from being assigned a routable IP address. However, some malicious actors will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP address ranges for wireless networks. Configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit.

Control: 1319; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the dynamic host configuration protocol for assigning IP addresses on wireless networks.

Media Access Control address filtering

Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead of configuring whitelists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, some malicious actors will be able to determine valid MAC addresses of legitimate users already on wireless networks and use this information to spoof valid MAC addresses and gain access to a network. MAC address filtering introduces a management overhead without any real tangible security benefit.

Control: 1320; Revision: 1; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
MAC address filtering should not be used as a security mechanism to restrict which devices can connect to a wireless network.

802.1X authentication

Where an agency chooses to deploy a secure wireless network, they can choose from a number of Extensible Authentication Protocol (EAP) methods that are supported by the Wi–Fi Protected Access 2 (WPA2) protocol.

Agencies deploying a secure wireless network can choose WPA2–Enterprise with EAP–Transport Layer Security (EAP–TLS), WPA2–Enterprise with EAP–Tunnelled Transport Layer Security (EAP–TTLS) or WPA2–Enterprise with Protected EAP (PEAP) to perform mutual authentication.

WPA2–Enterprise with EAP–TLS is considered one of the most secure EAP methods. Due to its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. EAP–TLS uses a public key infrastructure (PKI) to secure communications between devices and a Remote Access Dial In User Service (RADIUS) server through the use of X.509 certificates. While EAP–TLS provides strong mutual authentication, it requires an agency to have established a PKI. This involves either deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses the wireless network. While this introduces additional costs and management overheads to an agency, the security advantages are significant.

The EAP–TTLS/MSCHAPv2, or simply EAP–TTLS, method used with WPA2–Enterprise is generally supported through the use of third party software. It has support in multiple operating systems but does not have native support in Microsoft Windows. EAP–TTLS is different to EAP–TLS in that devices do not authenticate to the server when the initial TLS tunnel is created. Only the server authenticates to devices. Once the TLS tunnel has been created, mutual authentication occurs through the use of another EAP method. An advantage of EAP–TTLS over PEAP is that a username is never transmitted in the clear outside of the TLS tunnel. Another advantage of EAP–TTLS is that it provides support for many legacy EAP methods, while PEAP is generally limited to the use of EAP–MSCHAPv2.

PEAPv0/EAP–MSCHAPv2, or simply PEAP, is the second most widely supported EAP method after EAP–TLS. It enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. PEAP operates in a very similar way to EAP–TTLS by creating a TLS tunnel which is used to protect another EAP method. PEAP differs from EAP–TTLS in that when the EAP–MSCHAPv2 method is used within the TLS tunnel, only the password portion is protected and not the username. This may allow an intruder to capture the username and replay it with a bogus password in order to lockout the user's account, causing a denial of service for that user. While EAP–MSCHAPv2 within PEAP is the most common implementation, Microsoft Windows supports the use of EAP–TLS within PEAP, known as PEAP–EAP–TLS. This approach is very similar in operation to traditional EAP–TLS yet provides increased protection, as parts of the certificate that are not encrypted with EAP–TLS are encrypted with PEAP–EAP–TLS. The downside to PEAP–EAP–TLS is its support is limited to Microsoft products.

Ultimately, an agency's choice in authentication method will often be based on the size of their wireless deployment, their security requirements and any existing authentication infrastructure they plan on utilising. If an agency is primarily motivated by security they can implement either PEAP–EAP–TLS or EAP–TLS. If they are primarily motivated by flexibility and legacy support they can implement EAP–TTLS. If they are primarily motivated by simplicity they can implement PEAP with EAP–MSCHAPv2.

Control: 0541; Revision: 2; Updated: Sep-12; Applicability: G; Compliance: must; Authority: AA
WPA2–Enterprise with EAP–TLS, WPA2–Enterprise with PEAP–EAP–TLS, WPA2–Enterprise with EAP–TTLS or WPA2–Enterprise with PEAP must be used on wireless networks to perform mutual authentication.

Control: 1321; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
WPA2–Enterprise with EAP–TLS must be used on wireless networks to perform mutual authentication.

Evaluation of 802.1X authentication implementation

The security of 802.1X authentication is dependent on three main elements and how they interact with each other. These three elements include supplicants (clients) that support the 802.1X authentication protocol, authenticators (wireless access points) that facilitate communication between supplicants and the authentication server, and the authentication server (RADIUS server) that is used for authentication, authorisation and accounting purposes. To provide assurance that these elements have been implemented appropriately, supplicants, authenticators and the authentication server used in wireless networks must have completed an appropriate evaluation. For PROTECTED networks this entails choosing products that have successfully completed an ACE, while for networks classified CONFIDENTIAL and above this entails choosing High Assurance products.

Control: 1322; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Supplicants, authenticators and the authentication server used in wireless networks must have completed an appropriate evaluation.

Issuing certificates for authentication

Certificates for authenticating to wireless networks can be issued to either or both devices and users. For assurance, certificates must be generated using a certificate authority product or hardware security module that has completed an appropriate evaluation.

When issuing certificates to devices accessing wireless networks, agencies need to be aware of the risk that these certificates could be stolen by malicious software. Once compromised, the certificate could be used on another device to gain unauthorised access to the wireless network. Agencies also need to be aware that in only issuing a certificate to a device, any actions taken by a user will only be attributable to the device and not a specific user.

When issuing certificates to users accessing wireless networks, they can either be in the form of a certificate that is stored on a device or a certificate that is stored within a smart card. Issuing certificates on smart cards provides increased security, but at a higher cost. This is because a user is more likely to notice a missing smart card and alert their local security team, who is then able to revoke the credentials on the RADIUS server. This can minimise the time an intruder has access to a wireless network. In addition, to reduce the likelihood of a stolen smart card from being used to gain unauthorised access to a wireless network, two–factor authentication can be implemented through the use of Personal Identification Numbers (PINs) on smart cards. This is particularly important when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

For the highest level of security, unique certificates should be issued for both devices and users. In addition, the certificates for a device and user must not be stored on the same device. Finally, certificates for users accessing wireless networks should be issued on smart cards with access PINs and not stored with a device when not in use.

Control: 1323; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use unique certificates for both devices and users accessing a wireless network.

Control: 1324; Revision: 0; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must generate certificates using a certificate authority product or hardware security module that has completed an appropriate evaluation.

Control: 1325; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
The certificates for both a device and user accessing a wireless network must not be stored on the same device.

Control: 1326; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Certificates for users accessing wireless networks should be issued on smart cards with access PINs and not stored with a device when not in use.

Control: 1327; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Certificates stored on devices accessing wireless networks should be protected by implementing full disk encryption on the devices.

Using commercial certification authorities for certificate generation

A security risk exists with EAP–TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by obtaining certificates from a commercial certificate authority under false pretences, as devices can be tricked into trusting their signed certificate. This will allow the capture of authentication credentials presented by devices, which in the case of EAP–MSCHAPv2 can be cracked using a brute force attack granting not only network access but most likely Active Directory credentials as well. To reduce this risk, devices can be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise net servers or commercial certificate authorities. Additionally, setting devices to enable identity privacy will prevent usernames being sent prior to being authenticated by the RADIUS server.

Control: 1328; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Devices must be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.

Control: 1329; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Devices should be set to enable identity privacy.

Caching 802.1X authentication outcomes

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated. Upon successful authentication of a device, the PMK is capable of being cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re–authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre–authenticate a device to other neighbouring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, agencies can chose to use PMK caching and pre–authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

Control: 1330; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
The PMK caching period should not be set to greater than 1440 minutes (24 hours).

Remote Authentication Dial In User Service authentication

Separate to the 802.1X authentication process is the RADIUS authentication process that occurs between wireless access points and the RADIUS server. During the initial configuration of wireless networks using 802.1X authentication, a shared secret is entered into either the wireless access points or the RADIUS server. If configured on the wireless access points, the shared secret is sent to the RADIUS server via the RADIUS protocol, and vice versa if configured on the RADIUS server. This shared secret is used for both RADIUS authentication and confidentiality of RADIUS traffic. An intruder that is able to gain access to the RADIUS traffic sent between wireless access points and the RADIUS server may be able to perform an offline dictionary attack to recover the shared secret. This in turn allows the intruder to decrypt all communications between wireless access points and the RADIUS server. To mitigate this security risk, communications between wireless access points and a RADIUS server must be encapsulated with an additional layer of encryption using an appropriate encryption product.

Control: 1331; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Communications between wireless access points and a RADIUS server must be encapsulated with an additional layer of encryption using an appropriate encryption product.

Encryption

As wireless transmissions are capable of radiating outside of secured areas, agencies cannot rely on the traditional approach of physical security to protect against unauthorised access to sensitive or classified information on wireless networks. Using the AES based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) helps protect the confidentiality and integrity of all wireless network traffic.

Control: 1332; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
CCMP must be used to protect the confidentiality and integrity of all wireless network traffic.

Control: 0543; Revision: 4; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Classified information must be encrypted with an appropriate encryption product before being communicated over a wireless network.

CCMP was introduced in WPA2 to address feasible attacks against the Temporal Integrity Key Protocol (TKIP) used by the Wi–Fi Protected Access (WPA) protocol as well as the original Wireless Encryption Protocol (WEP). A malicious actor looking to exploit vulnerabilities in TKIP and WEP can attempt to connect to wireless access points using one of these protocols. By default, wireless access points will attempt to accommodate this request by falling back to a legacy protocol that the device supports. Disabling or removing TKIP and WEP support from wireless access points ensures that wireless access points do not fall back to an insecure encryption protocol.

Control: 1333; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
TKIP and WEP support must be disabled or removed from wireless access points.

Interference between wireless networks

Where multiple wireless networks are deployed in close proximity, there is the potential for interference to impact on the availability of the network, especially when networks are operating on commonly used default channels of 1 and 11. Sufficiently separating wireless networks through the use of channel separation can help reduce this risk. This can be achieved by using wireless networks that are configured to operate on channels that are at least one apart. For example, channels 1, 3 and 5 could be used to separate three wireless networks.

Control: 1334; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Wireless networks should be sufficiently separated through the use of channel separation.

Protecting management frames on wireless networks

Effective DoS attacks can be performed by exploiting unprotected management frames using inexpensive commercial hardware. The latest release of the 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or DoS attacks. However, 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. As such, upgrading wireless access points to support the 802.11w amendment will address this security risk.

Control: 1335; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Wireless access points and devices should be upgraded to support the 802.11w amendment.

Bridging networks

When connecting devices via Ethernet to an agency's fixed network, agencies need to be aware of the security risks posed by active wireless functionality on devices. Devices will often automatically connect to any open wireless networks they have previously connected to, which a malicious actor can use to masquerade and establish a connection to the device. This device could then be used as a bridge to access the agency's fixed network. Disabling wireless functionality on devices, preferably by a hardware switch, whenever connected to a fixed network can prevent this from occurring. Additionally, devices do not have to be configured to remember and automatically connect to open wireless networks that they have previously connected to.

Control: 1336; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Wireless functionality on devices should be disabled, preferably by a hardware switch, whenever connected to a fixed network.

Control: 1337; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Devices must not be configured to remember and automatically connect to open wireless networks that they have previously connected to.

Wireless network footprint

Minimising the output power of wireless access points will reduce the footprint of wireless networks. Instead of deploying a small number of wireless access points that broadcast on high power, it is recommended that more wireless access points that use minimal broadcast power be deployed to achieve the desired wireless network footprint. This has the added benefit of providing redundancy for a wireless network should a wireless access point become unserviceable. In such a case, the output power of other wireless access points can be increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

Control: 1338; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint.

An additional method to limit a wireless network's footprint is through the use of radio frequency shielding on an agency's premises. While expensive, this will limit the wireless communications to areas under the control of an agency. Radio frequency shielding on an agency's premises has the added benefit of preventing the jamming of wireless networks from outside of the premises in which wireless networks are operating.

Control: 1013; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: should; Authority: AA
The effective range of wireless communications outside an agency's area of control should be limited by implementing RF shielding on buildings in which wireless networks are used.

References

Information on Wi–Fi Alliance certification programs can be obtained from http://www.wi-fi.org/certification_programs.php.

Further information on 802.11–2007 can be found at http://standards.ieee.org/getieee802/download/802.11-2007.pdf.

Further information on EAP can be found in the EAP specification at http://tools.ietf.org/search/rfc3748.

Further information on EAP–TLS can be found in the EAP–TLS specification at http://tools.ietf.org/html/rfc5216.

Video Conferencing and Internet Protocol Telephony

Objective

Video conferencing and IP telephony, including Voice over Internet Protocol (VoIP), is deployed in a secure manner that does not compromise the security of information and systems.

Scope

This section describes security requirements for video conferencing and IP telephony, including VoIP. Although IP telephony refers to the transport of telephone calls over IP networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

Context

Additional information on topics covered in this section can be found in the *Product Security* chapter, the *Telephones and Telephone Systems* section of the *Communications Systems and Devices* chapter, the *Mobile Devices* section of the *Working Off–Site* chapter, the *Cross Domain Security* chapter and any section relating to the protection of data networks in this manual.

Video and voice–aware firewall requirement

Where an analog telephone network, such as the PSTN, is connected to a data network the *Gateways* section of the *Cross Domain Security* chapter does not apply.

Where a video conferencing or IP telephony network is connected to another video conferencing or IP telephony network in a different security domain the *Gateways* section of the *Cross Domain Security* chapter applies.

Hardening video conferencing and IP telephony infrastructure

Video conferencing and IP telephony traffic in a data network consists of IP packets and should be treated the same as any other data. As such, hardening can be applied to video conferencing units, handsets, software, servers, firewalls and gateways. For example, a Session Initiation Protocol (SIP) server must:

- have a fully patched operating system
- have fully patched software
- run only required services
- use encrypted non–replayable authentication
- apply network restrictions that only allow secure SIP traffic and secure Real–time Transport Protocol (RTP) traffic from video conferencing units and IP phones on a VLAN to reach the server.

Controls

Video and voice–aware firewalls

The use of video and voice–aware firewalls ensures that only video and voice traffic (e.g. signalling and data) is allowed for a given call and that the session state is maintained throughout the transaction.

The requirement to use a video or voice–aware firewall does not necessarily require separate firewalls be deployed for video conferencing, IP telephony and data traffic. If possible, agencies are encouraged to implement one firewall that is either video and data–aware, voice and data–aware; or video, voice and data–aware depending on their needs.

Control: 0546; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Where a requirement exists to implement an evaluated firewall for video conferencing or IP telephony in a gateway environment, an evaluated video or voice–aware firewall should be used.

Protecting video conferencing and IP telephony traffic

Video conferencing and IP telephony traffic is vulnerable to eavesdropping but can be easily protected with encryption. This helps protect against DoS, man–in–the–middle and call spoofing attacks made possible by inherent weaknesses in the video conferencing and IP telephony protocols.

When protecting video conferencing and IP telephony traffic, 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.

Control: 0547; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should protect video conferencing and IP telephony signalling and data to ensure confidentiality, integrity, availability, authenticity and non–replayability.

Establishment of secure signalling and data protocols

Use of secure signalling and data protocols protect against eavesdropping, some types of DoS, man–in–the–middle and call spoofing attacks.

Control: 0548; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that video conferencing and IP telephony functions can only be established using the secure signalling and data protocols.

Local area network traffic separation

Availability and quality of service are the main drivers for logical and physical separation.

Control: 0549; Revision: 2; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Video conferencing and IP telephony traffic should be separated either physically or logically from other data traffic.

Control: 0550; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Video conferencing and IP telephony traffic must be separated either physically or logically from other data traffic.

Video conferencing unit and IP phone setup

Video conferencing units and IP phones need to be hardened and logically or physically separated from the data network to ensure they do not provide an easy entry point to the network for an intruder. USB ports on video conferencing units and IP phones may be used to circumvent USB workstation policy while unprotected management interfaces may be used to upload malicious firmware for call recording/spoofing and entry into the data network. Blocking by default unauthorised devices and unauthenticated devices will reduce the security risk of a denial of service.

Control: 0554; Revision: 0; Updated: Sep-08; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
An encrypted and non–replayable two–way authentication scheme should be used for call authentication and authorisation.

Control: 0553; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Authentication and authorisation should be used for all actions on the video conferencing network, including:

- call setup
- changing settings.

Control: 0555; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Authentication and authorisation should be used for all actions on the IP telephony network, including:

- registering a new IP phone
- changing phone users
- changing settings
- accessing voice mail.

Control: 0551; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
IP telephony should be configured such that:

- IP phones authenticate themselves to the call controller upon registration
- phone auto–registration is disabled and only a whitelist of authorised devices are allowed to access the network
- unauthorised devices are blocked by default
- all unused and prohibited functionality is disabled.

Control: 0552; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
IP telephony must be configured such that:

- IP phones authenticate themselves to the call controller upon registration
- phone auto–registration is disabled and only a whitelist of authorised devices are allowed to access the network
- unauthorised devices are blocked by default
- all unused and prohibited functionality is disabled.

Control: 1014; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should use individual logins for IP phones.

Video conferencing unit and IP phone connections to workstations

Availability and quality of service are the main drivers for logical and physical separation.

Control: 0556; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: should not; Authority: AA
Workstations should not be connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Control: 0557; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must not; Authority: AA
Workstations must not be connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Lobby and shared area phones

Lobby IP phones are in public areas and may give an intruder the opportunity to access the internal data network (depending on separation arrangements) by replacing the IP phone with another device, or installing a device in–line. There are also the security risks of social engineering (since the call may appear to be internal) and data leakage from poorly protected voicemail boxes.

For further information on what constitutes a 'public area', refer to the Attorney–General's Department's *Security zones and risk mitigation control levels* document.

Control: 1015; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use traditional analog phones in lobby and shared areas.

Control: 0558; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If IP phones are used in lobby and shared areas, their ability to access data networks and functionality for voice mail and directory services should be limited.

Software used for softphones and webcams

Software used for softphones and webcams can introduce additional vulnerabilities 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 video conferencing or IP telephony network.

Softphones and webcams 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.

Control: 0559; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not use softphones or webcams.

On workstations using softphones and webcams, separate network cards can facilitate a simple VLAN separation. Host–based firewalls ensure a minimal set of ports are exposed to a minimal set of workstations.

Control: 1016; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies using softphones or webcams should have separate dedicated network interface cards on the host for video conferencing and IP telephony network access.

Control: 1017; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies using softphones and webcams should install a host–based firewall on workstations that only allows traffic to and from the minimum number of ports required.

Workstations using USB phones and webcams

Adding USB phones and webcams to a whitelist of allowed USB devices on a workstation will assist with restricting access to only authorised devices, and allowing the Standard Operating Environment to maintain defences against removable media storage and other unauthorised USB devices.

Control: 1018; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use access control software to control USB ports on workstations using USB phones and webcams by using the specific vendor and product identifier of authorised USB phones and webcams.

Developing a denial of service response plan

Telephony is considered critical for any business and is therefore especially vulnerable to a denial of service. A denial of service response plan will assist in responding to video conferencing and IP telephony DoS attacks, signalling floods, established call teardown and RTP data floods.

A denial of service response plan will need to address the following:

- how to identify the source of the denial of service, either internal or external (location and content of logs)
- how to minimise the effect on video conferencing and IP telephony of a denial of service of the data network (for example, Internet or internal denial of service), including separate links to other office locations and quality of service prioritisation
- strategies that can mitigate the denial of service (banning certain devices/IPs at the call controller and firewalls, implementing quality of service, changing authentication, changing dial–in authentication
- alternative communication options (such as personal mobile phones) that have been identified for use in case of an emergency.

Control: 1019; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA

Agencies should develop a denial of service response plan which includes:

- how to identify signs of a denial of service
- how to diagnose the source of a denial of service
- what actions can be taken to clear a denial of service
- how capabilities could be maintained during a denial of service.

Control: 1020; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA

Resources and services to monitor for signs of a denial of service should include:

- router and switch logging and flow data
- packet captures
- proxy and call manager logs and access control lists
- video and voice–aware firewalls and gateways
- network redundancy
- load balancing
- PSTN failover.

References

The Attorney–General's Department's *Security zones and risk mitigation control levels* document provides further information on physical security controls for security zones.

Intrusion Detection and Prevention

Objective

An intrusion detection and prevention strategy is implemented for systems.

Scope

This section describes detecting and preventing malicious code propagating through networks as well as detecting and preventing unusual or malicious activities.

Context

Methods of infections or delivery

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
- security weaknesses in an application
- contact with an infected system or media.

Controls

Intrusion detection and prevention strategy

An IDS/IPS when configured correctly, kept current and supported by appropriate processes can be an effective way of identifying and responding to known intrusion profiles. Appropriate resources need to be allocated to an IDS/IPS to allow maintenance and monitoring including training and time assigned to the validation of alerts and the tuning of rules.

Control: 0576; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop, implement and maintain an intrusion detection and prevention strategy that includes:

- appropriate intrusion detection and prevention mechanisms, including network–based IDSs/IPSs and host–based IDSs/IPSs as necessary
- the audit analysis of event logs, including IDS/IPS logs
- a periodic audit of intrusion detection and prevention procedures
- information security awareness and training programs
- a documented Incident Response Plan
- the capability to detect cyber security incidents and attempted network intrusions on gateways and provide real–time alerts.

Control: 1184; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that if an IDS/IPS is deployed, appropriate resources are allocated to maintenance and monitoring.

Control: 1185; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When deploying IDSs/IPSs on a network that is not connected to the Internet, either directly or indirectly via a cascaded connection, agencies must use IDSs/IPSs that monitor unusual patterns of behaviours or traffic flows, rather than detect specific Internet–based communication protocol signatures.

IDSs and IPSs in gateways

If a firewall is configured to block all traffic on a particular range of port numbers, then IDSs/IPSs should inspect traffic for these port numbers and generate an alert if they are detected.

Control: 0577; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
IDSs/IPSs should be deployed in all gateways between agency networks and public network infrastructure.

Control: 1029; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
IDSs/IPSs should be deployed in all gateways between agency networks and any other network they do not manage.

Control: 1028; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
IDSs/IPSs in gateway environments should be located immediately inside the outermost firewall.

Generating alerts for information flows that contravene any rule in the firewall rule set helps security personnel respond to suspicious or malicious traffic entering a network due to a failure or configuration change to the firewall.

Control: 1030; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
IDSs/IPSs located behind a firewall should be configured to generate a log entry, and an alert, for any information flows that contravene any rule in the firewall rule set.

Signature–based intrusion detection and prevention

When signature–based intrusion detection and prevention is used the effectiveness of IDSs/IPSs will degrade over time as new intrusion methods are developed. It is for this reason that signatures for IDSs/IPSs need to be kept current to identify the latest intrusion methods.

Control: 0578; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When signature–based intrusion detection is used, agencies must keep the signatures current.

Configuring IDSs and IPSs

Testing IDS/IPS rule sets prior to implementation can assist in ensuring they perform as expected and do not cause any undesired activity on the network.

Control: 1031; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should test IDS/IPS rule sets prior to implementation.

Event management and correlation

Deploying tools to manage the archival and correlation of events of interest across all networks helps identify suspicious patterns in information flows.

Control: 1032; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should deploy tools for:

- the management and retention of security event information, with the appropriate metadata for the maintenance of the information's integrity
- the correlation of events of interest across all networks.

Host–based IDSs and IPSs

Host–based IDSs (HIDSs) and Host–based IPSs (HIPSs) use behaviour–based detection schemes and can therefore assist agencies in identifying anomalous behaviour, such as process injection, keystroke logging, driver loading and call hooking, as well as detecting malicious code that has yet to be identified by vendors. Importantly, however, some antivirus products are evolving into converged endpoint security products that incorporate HIDS/HIPS functionality.

Control: 1034; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must install HIPS/HIDS on high value servers, such as authentication servers (e.g. Active Directory Domain Controllers and RADIUS servers), DNS servers, web servers, file servers and email servers.

Control: 1341; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should install HIDS/HIPS on all workstations.

References

Additional information relating to intrusion detection and audit analysis is contained in HB 171:2003, *Guidelines for the Management of Information Technology Evidence.*

Peripheral Switches

Objective

An evaluated peripheral switch is used when sharing keyboards, monitors and mice between different systems.

Scope

This section describes the use of keyboard/video/mouse switches.

Context

For more information on ASD's EPL see the *Product Security* chapter.

Controls

Peripheral switches

The level of assurance needed in a peripheral switch is determined by the highest and lowest sensitivity or classification of systems connected to the switch.

When accessing systems through a peripheral switch it is important that sufficient assurance is available in the operation of the switch to ensure that information does not accidently pass between the connected systems.

Control: 0591; Revision: 4; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies must use a Common Criteria–evaluated product when accessing a classified system and a sensitive system via a peripheral switch.

Control: 0593; Revision: 5; Updated: Apr-13; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must use a High Assurance product from ASD's EPL when accessing a highly classified system and a less classified system or sensitive system via a peripheral switch.

Peripheral switches for particularly sensitive systems

AUSTEO and AGAO systems require additional security measures to be put in place when connecting to other systems.

Control: 0594; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a Common Criteria–evaluated product when accessing a system containing AUSTEO or AGAO information and a system of the same classification that is not accredited to process the same caveat.

References

Nil.

Cryptography

Cryptographic Fundamentals

Objective

Cryptographic products, algorithms and protocols that have been evaluated by ASD are used.

Scope

This section describes the fundamentals of cryptography including the use of encryption to protect data at rest and in transit.

Context

Information on product security such as product selection, acquisition, installation and configuration can be found in the *Product Security* chapter.

Detailed information on algorithms and protocols approved to protect sensitive or classified information can be found in the *ASD Approved Cryptographic Algorithms* and ASD *Approved Cryptographic Protocols* sections of this chapter.

Purpose of cryptography

The purpose of cryptography is to provide confidentiality, integrity, authentication and non–repudiation of information.

Confidentiality is one of the most common cryptographic functions, with encryption providing protection to information by making it unreadable to all but authorised users.

Integrity is concerned with protecting information from accidental or deliberate manipulation. It provides assurance that the information has not been modified.

Authentication is the process of ensuring that a person or entity is who they claim to be. A robust authentication system is essential for protecting access to systems.

Non–repudiation provides proof that a user performed an action, such as sending a message, and prevents them from denying that they did so.

Using approved encryption generally reduces the likelihood of an unauthorised party gaining access to the encrypted information. However, it does not reduce the consequences of a successful intrusion.

Care needs to be taken, with encryption systems that do not encrypt the entire media content, to ensure that either all of the data is encrypted or that the media is handled in accordance with the sensitivity or classification of the unencrypted data.

Using encryption

Encryption of data at rest can be used to reduce the physical storage and handling requirements of media or systems containing sensitive or classified information to an unclassified level.

Encryption of data in transit can be used to provide protection for sensitive or classified information being communicated over public network infrastructure.

When agencies use encryption for data at rest, or in transit, they are not reducing the sensitivity or classification of the information. However, because the information is encrypted, the consequences of the encrypted information being accessed by unauthorised parties are considered to be less. Therefore the security requirements applied to such information can be reduced. However, as the sensitivity or classification of the unencrypted information does not change, the lowered security requirements cannot be used as a baseline to further lower requirements with an additional cryptographic product.

Product specific cryptographic requirements

This section describes the use of cryptography to protect sensitive or classified information. Additional requirements can exist in consumer guides for products once they have completed an ASD Cryptographic Evaluation (ACE). Such requirements supplement this manual and where conflict occurs the product specific requirements take precedence.

Using products with ASD Approved Cryptographic Algorithms and Protocols

Where this manual states a requirement for a product that implements an ASD Approved Cryptographic Algorithm (AACA) or ASD Approved Cryptographic Protocol (AACP) to be used to provide protection for information at rest or in transit, the product does not need to have undergone a ACE.

Federal Information Processing Standard 140

The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of both hardware and software cryptographic modules.

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.

FIPS 140 is not a substitute for an ACE of a product with cryptographic functionality. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.

Cryptographic evaluations of products will normally be conducted by ASD. Where a product's cryptographic functionality has been validated under FIPS 140, ASD can, at its discretion, and in consultation with the vendor, reduce the scope of an ACE.

ASD will review the FIPS 140 validation report to confirm compliance with Australia's national cryptographic policy.

Controls

Reducing storage and physical transfer requirements

When encryption is applied to media, whether the media resides in ICT equipment or not, it provides an additional layer of defence. Encryption does not change the sensitivity or classification of the information, but when encryption is used the storage and physical transfer requirements of the ICT equipment or media can be treated at an unclassified level.

Control: 1161, Revision: 2, Updated: Feb-14; Applicability: G; Compliance: must; Authority: AA

Agencies must use an encryption product that implements an AACA if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains sensitive information to an unclassified level.

Control: 0457; Revision: 4; Updated: Feb-14; Applicability: P; Compliance: must; Authority: AA
Agencies must use a Common Criteria–evaluated encryption product that has completed an ACE if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.

Control: 0460; Revision: 6; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies must use High Assurance products if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to that of a lower classification.

Encrypting information at rest

Full disk encryption provides a greater level of protection than file–based encryption. While file–based encryption may encrypt individual files there is the possibility that unencrypted copies of the file may be left in temporary locations used by the operating system.

Control: 0459; Revision: 2; Updated: Nov-10; Applicability: G, P; Compliance: should; Authority: AA
Agencies using encryption to secure data at rest should use either:

- full disk encryption
- partial encryption where the access control will only allow writing to the encrypted partition.

Control: 0461; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies using encryption to secure data at rest must use either:

- full disk encryption
- partial encryption where the access control will only allow writing to the encrypted partition.

Encrypting particularly sensitive information at rest

Due to the sensitivities associated with AUSTEO and AGAO information is, it needs to be encrypted when at rest.

Control: 1080; Revision: 1; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: must; Authority: AA
In addition to any encryption already in place, agencies must, at minimum, use an AACA to protect AUSTEO and AGAO information when at rest on a system.

Data recovery

The requirement for an encryption product to provide a key escrow function, where practical, was issued under a Cabinet directive in July 1998.

Control: 0455; Revision: 1; Updated: Nov-10; Applicability: G, P; Compliance: must; Authority: AA
Where practical, cryptographic products must provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Control: 0456; Revision: 1; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: ASD
Where practical, cryptographic products must provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted ICT equipment

When a user authenticates to ICT equipment employing encryption functionality, all information becomes accessible. At such a time, the ICT equipment will need to be handled as per the sensitivity or classification of the information it processes, stores or communicates.

Control: 0462; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When a user authenticates to ICT equipment storing encrypted information, it must be treated in accordance with the original sensitivity or classification of the equipment.

Reducing network infrastructure requirements

When encryption is applied to sensitive or classified information being communicated over networks, less assurance needs to be placed in the protection of the network infrastructure. In some cases, where no security can be applied to the network infrastructure—for example where information is in the public domain—encryption of sensitive or classified information is the only mechanism to prevent the information being compromised.

In some cases, agencies may have a business requirement to send unclassified but sensitive/official government information to stakeholders over public network infrastructure without applying encryption. Unencrypted information sent over the Internet should be considered unprotected and uncontrolled. Agencies need to understand and accept this risk if considering non–compliance with the below controls due to their business needs.

Control: 1162; Revision: 2; Updated: Feb-14; Applicability: G; Compliance: must; Authority: AA
Agencies must use an encryption product that implements an AACP if they wish to communicate sensitive information over public network infrastructure.

Control: 0465; Revision: 5; Updated: Feb-14; Applicability: P; Compliance: must; Authority: AA
Agencies must use a Common Criteria–evaluated encryption product that has completed an ACE if they wish to communicate classified information over public network infrastructure.

Control: 0467; Revision: 6; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: ASD
Agencies must use High Assurance products if they wish to communicate classified information over networks of a lower classification or public network infrastructure.

Encrypting particularly sensitive information in transit

Due to the sensitivities associated with AUSTEO and AGAO information, it needs to be encrypted when being communicated across network infrastructure.

Control: 0469; Revision: 2; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: must; Authority: AA
In addition to any encryption already in place for communication mediums, agencies must, at minimum, use an AACP to protect AUSTEO and AGAO information when in transit.

References

Further information on the FIPS 140 standards can be found at http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

The storage and physical transfer requirements for sensitive or classified information can be found in the *Australian Government Physical Security Management Protocol* and *Australian Government Information Security Management Protocol.*

ASD Approved Cryptographic Algorithms

Objective

Information at rest is protected by an AACA.

Scope

This section describes cryptographic algorithms that ASD has approved for use in government.

Context

Implementations of the algorithms in this section need to undergo an ACE before they can be approved to protect classified information.

High Assurance cryptographic algorithms, which are not covered in this section, can be used for the protection of classified information if they are found suitably implemented in a product that has undergone a High Assurance evaluation by ASD. Further information on High Assurance algorithms can be obtained by contacting ASD.

AACAs

There is no guarantee or proof of security of an algorithm against presently unknown intrusion methods. 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 intrusion. There have been some cases where theoretically impressive vulnerabilities have been found, however these results are not of practical application.

AACAs fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

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
- Rivest–Shamir–Adleman (RSA) for digital signatures and passing encryption session keys or similar keys.

The approved hashing algorithm is:

- Secure Hashing Algorithm 2 (SHA–224, SHA–256, SHA–384 and SHA–512).

The approved symmetric encryption algorithms are:

- AES using key lengths of 128, 192 and 256 bits
- Triple Data Encryption Standard (3DES).

Where there is a range of possible key sizes for an algorithm, some of the smaller key sizes do not provide an adequate safety margin against intrusion methods that might be found in the future. For example, future advances in integer factorisation could render the use of smaller RSA moduli a vulnerability.

Suite B

Suite B is the collective name for the following set of four well–established, public domain cryptographic algorithms:

- Encryption: AES
- Hashing: SHA–2
- Digital Signature: ECDSA
- Key Exchange: ECDH.

When used in combination, these four algorithms can provide adequate information assurance for classified information.

Suite B has been approved by ASD in specific configurations and evaluated implementations for the protection of highly classified (CONFIDENTIAL, SECRET and TOP SECRET) information.

Controls

Using AACAs

If a product implementing an AACA has been inappropriately configured, it is possible that relatively weak cryptographic algorithms could be selected without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

When configuring unevaluated products that implement an AACA, agencies can ensure that only the AACA can be used by disabling the unapproved algorithms in the products (which is preferred) or advising users not to use them via a policy.

Control: 0471; Revision: 4; Updated: Feb-14; Applicability: G, P; Compliance: must; Authority: AA
Agencies using an unevaluated product that implements an AACA must ensure that only AACAs can be used.

Approved asymmetric/public key algorithms

Over the last decade, DSA and DH cryptosystems have been subject to increasingly successful sub–exponential index–calculus based attacks. ECDH and ECDSA offer more security per bit increase in key size than either DH or DSA and are considered more secure alternatives.

Control: 0994; Revision: 4; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Agencies should use ECDH and ECDSA in preference to DH and DSA.

Using Diffie–Hellman

A modulus of at least 1024 bits for DH is considered best practice by the cryptographic community.

Control: 0472; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies using DH for the approved use of agreeing on encryption session keys must use a modulus of at least 1024 bits.

Using the Digital Signature Algorithm

A modulus of at least 1024 bits for DSA is considered best practice by the cryptographic community.

Control: 0473; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies using DSA for the approved use of digital signatures must use a modulus of at least 1024 bits.

Using Elliptic Curve Diffie–Hellman

A field/key size of at least 160 bits for ECDH is considered best practice by the cryptographic community.

Control: 0474; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies using ECDH for the approved use of agreeing on encryption session keys must use a field/key size of at least 160 bits.

Using the Elliptic Curve Digital Signature Algorithm

A field/key size of at least 160 bits for ECDSA is considered best practice by the cryptographic community.

Control: 0475; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies using ECDSA for the approved use of digital signatures must use a field/key size of at least 160 bits.

Using Rivest–Shamir–Adleman

A modulus of at least 1024 bits for RSA is considered best practice by the cryptographic community.

Control: 0476; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
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.

Control: 0477; Revision: 5; Updated: Feb-14; Applicability: G, P; Compliance: must; Authority: AA
Agencies using RSA, both for the approved use of digital signatures and for passing encryption session keys or similar keys, must ensure that the key pair used for passing encrypted session keys is different from the key pair used for digital signatures.

Approved hashing algorithms

Recent research conducted by the cryptographic community suggests that SHA–1 may be susceptible to collision attacks. While no practical collision attacks have been published for SHA–1, they may become feasible in the near future.

Control: 1054; Revision: 2; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Agencies should use a hashing algorithm from the SHA–2 family.

Approved symmetric encryption algorithms

The use of Electronic Code Book mode in block ciphers allows repeated patterns in plaintext to appear as repeated patterns in the ciphertext. Most clear text, including written language and formatted files, contains significant repeated patterns. A malicious actor can use this to deduce possible meanings of ciphertext by comparison with previously intercepted data. The use of other modes such as Cipher Block Chaining, Cipher Feedback, Output Feedback or Counter prevents such attacks.

Control: 0479; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: should not; Authority: AA
Agencies using AES or 3DES should not use electronic codebook mode.

Using the Triple Data Encryption Standard

Using three distinct keys is the most secure option, while using two distinct keys in the order key 1, key 2, key 1 is also deemed secure for practical purposes. All other keying options are equivalent to single DES, which is not deemed secure for practical purposes.

Control: 0480; Revision: 4; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies using 3DES must use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.

Protecting highly classified information

Suite B, a set of public domain cryptographic algorithms, has been approved by ASD for use in specific configurations and evaluated implementations for the protection of CONFIDENTIAL, SECRET and TOP SECRET information.

Control: 1231; Revision: 0; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
If using Suite B, agencies must use them in the configuration specified in the table below, to appropriately protect CONFIDENTIAL, SECRET and TOP SECRET information.

	CRYPTOGRAPHIC ALGORITHM OR PROTOCOL	REQUIREMENTS FOR INFORMATION CLASSIFIED CONFIDENTIAL AND SECRET	REQUIREMENTS FOR INFORMATION CLASSIFIED TOP SECRET
Encryption	AES	128 bit key OR 256 bit key	256 bit key
Hashing	SHA	SHA–256 OR SHA–384	SHA–384
Digital Signature	ECDSA	NIST P–256 OR NIST P–384	NIST P–384
Key Exchange	ECDH	NIST P–256 OR NIST P–384	NIST P–384

ASD has approved classified cryptographic algorithms for the protection of highly classified information. As with Suite B, these are only approved when used in an evaluated implementation.

Control: 1232; Revision: 1; Updated: Apr-13; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies using Suite B algorithms to protect CONFIDENTIAL, SECRET and TOP SECRET information must use them in a High Assurance product.

References

The following references are provided for the approved asymmetric/public key algorithms, hashing algorithms and encryption algorithms.

Further information on DH can be found in Diffie, W and Hellman, ME '*New Directions in Cryptography*', IEEE Transactions on Information Theory, vol. 22, is. 6, pp. 644–654, November 1976.

Further information on DSA can be found in *FIPS 186–3.*

Further information on ECDH can be found in ANSI X9.63 and ANSI X9.42 and NIST SP800–56A.

Further information on ECDSA can be found in FIPS 186–3, ANSI X9.63 and ANSI X9.62.

Further information on RSA can be found in *Public Key Cryptography Standards #1*, RSA Laboratories.

Further information on SHA can be found in FIPS 180–2.

Further information on AES can be found in FIPS 197.

ASD Approved Cryptographic Protocols

Objective

Information in transit is protected by an AACP implementing an AACA.

Scope

This section describes cryptographic protocols that ASD has approved for use in government.

Context

Implementations of the protocols in this section need to undergo an ACE before they can be approved to protect classified information.

High Assurance protocols, which are not covered in this section, can be used for the protection of classified information if they are found suitably implemented in a product that has undergone a High Assurance evaluation by ASD. Further information on High Assurance protocols can be obtained by contacting ASD.

AACPs

In general, ASD only approves the use of cryptographic products that have passed a formal evaluation. However, ASD approves the use of some commonly available cryptographic protocols even though their implementations in specific products have not been formally evaluated by ASD. This approval is limited to cases where they are used in accordance with the requirements in this manual.

The AACPs are:

- TLS
- Secure Shell (SSH)
- Secure Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)
- WPA2 (when used in accordance with the advice contained in the *Wireless Local Area Networks* section of the *Network Security* chapter).

Controls

Using AACPs

If a product implementing an AACP has been inappropriately configured, it is possible that relatively weak cryptographic algorithms could be selected without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

When configuring unevaluated products that implement an AACP, agencies can ensure that only the AACA can be used by disabling the unapproved algorithms in the products (which is preferred) or advising users not to use them via a policy.

While many AACPs support authentication, agencies should be aware that these authentication mechanisms are not fool proof. 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
- using a legitimate identity registration scheme.

Control: 0481; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies using a product that implements an AACP must ensure that only AACAs can be used.

References

Further information on the OpenPGP Message Format can be found in the OpenPGP Message Format specification at http://www.ietf.org/rfc/rfc3156.txt.

Transport Layer Security

Objective

Transport Layer Security (TLS) is implemented correctly as an AACP.

Scope

This section describes the conditions under which TLS can be used as an AACP. Additionally, as File Transfer Protocol over TLS is built on TLS, it is also considered in scope.

Context

The terms SSL and TLS have traditionally been used interchangeably. As SSL 3.0 is no longer an AACP, for the purposes of this document instances of 'SSL' refer to SSL version 3.0 and below, and TLS refers to TLS 1.0 and beyond.

When using a product that implements TLS, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Further information on handling TLS traffic through gateways can be found in the *Web Content and Connections* section of the *Software Security* chapter.

Controls

Using Secure Sockets Layer and Transport Layer Security

Version 1.0 of SSL was never released and version 2.0 had significant security flaws leading to the development of SSL 3.0. SSL has since been superseded by TLS, with the latest version being TLS 1.2 which was released in August 2008.

Control: 0482; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use SSL.

Control: 1139; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the current version of TLS.

Control: 1369; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use AES–GCM for symmetric encryption when available.

Control: 1370; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a TLS implementation that supports secure renegotiation.

Control: 1371; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
If secure renegotiation is not available, agencies must disable renegotiation.

Control: 1372; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use ephemeral DH over RSA or static DH for key establishment.

Control: 1373; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use anonymous DH.

Control: 1374; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use SHA–2 based certificates where available.

Control: 1375; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
When selecting the cipher suite Message Authentication Code (MAC) and Pseudo Random Function (PRF) algorithms, agencies should use SHA–2. When SHA–2 is not available, SHA–1 should be used.

References

Further information on TLS can be found in the TLS 1.2 definition at http://tools.ietf.org/html/rfc5246.

Secure Shell

Objective

SSH is implemented correctly as an AACP.

Scope

This section describes the conditions under which implementations of SSH can be used as an AACP. Additionally, secure copy and Secure File Transfer Protocol use SSH and are therefore also covered by this section.

Context

When using a product that implements SSH, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Controls

Using Secure Shell

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.

SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to a man–in–the–middle attack, where someone 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.

SSH has the ability to forward connections and access privileges in a variety of ways. This means if any of these features can be exploited, unauthorised access to a potentially large amount of information can also be gained.

Host–based authentication requires no credentials (for example, passphrase or public key) to authenticate (though in some cases it might make use of a host key). This renders SSH vulnerable to an IP spoofing attack.

An intruder 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.

Control: 0484; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
The settings below should be implemented when using SSH.

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
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 passphrases	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

Authentication mechanisms

Public key–based systems have greater potential for strong authentication—put simply, people cannot remember particularly strong passphrases. Passphrase–based authentication schemes are also more susceptible to interception than public key–based authentication schemes.

Passphrases are more susceptible to guessing attacks, therefore if passphrases are used in a system, counter–measures should be put into place to reduce the chance of a successful brute force attack.

Control: 0485; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use public key–based authentication in preference to using passphrase–based authentication.

Control: 0486; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies that allow passphrase authentication should use techniques to block brute force attempts against the passphrase.

Automated remote access

If passphrase–less authentication is enabled, allowing access from unknown IP addresses would allow untrusted parties to automatically authenticate to systems without needing to know the passphrase.

If port forwarding is not disabled, or it is not configured securely, access may be gained to forwarded ports, thereby creating a communication channel between the intruder and the host.

If agent credential forwarding is enabled, an intruder could connect to the stored authentication credentials and then use them to connect to other trusted hosts or even intranet hosts, if port forwarding has been allowed as well.

X11 is a computer software system and network protocol that provides a graphical user interface for networked computers. Failing to disable X11 display remoting could result in an intruder being able to gain control of the computer displays as well as keyboard and mouse control functions.

Allowing console access allows every user who logs into the console to run programs that are normally restricted to the root user.

Control: 0487; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies that use logins without a passphrase for automated purposes should disable:

- access from IP addresses that do not need access
- port forwarding
- agent credential forwarding
- X11 display remoting
- console access.

Control: 0488; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies that use remote access without the use of a passphrase should use the 'forced command' option to specify what command is executed.

Control: 0997; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use parameter checking when using the 'forced command' option.

SSH–agent

SSH–agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH–agent launches, it will request the user's passphrase. This passphrase is used to unlock the user's private key. Subsequent access to remote systems is performed by the agent and does not require the user to re–enter their passphrase. Screen locks and expiring key caches ensure that the user's private key is not left unlocked for long periods of time.

Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

Control: 0489; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies that use SSH–agent or other similar key caching programs should:

- only use the software on workstation and servers with screen locks
- ensure that the key cache expires within four hours of inactivity
- ensure that agent credential forwarding is used when multiple SSH transversal is needed.

References

Further information on SSH can be found in the SSH specification at http://tools.ietf.org/html/rfc4252.

Secure Multipurpose Internet Mail Extension

Objective

S/MIME is implemented correctly as an AACP.

Scope

This section describes the conditions under which S/MIME can be used as an AACP.

Context

When using a product that implements S/MIME, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Information relating to the development of passphrase selection policies and passphrase requirements can be found in the *Identification and Authentication* section of the *Access Control* chapter.

Controls

Using S/MIME

S/MIME 2.0 required the use of weaker cryptography (40–bit keys) than is approved for use in this manual. Version 3.0 was the first version to become an Internet Engineering Task Force standard.

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 and other Internet security software to scan for viruses and other malicious code.

Control: 0490; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should not; Authority: AA
Agencies should not allow versions of S/MIME earlier than 3.0 to be used.

References

Further information on S/MIME can be found in the S/MIME charter at http://www.tools.ietf.org/search/rfc5751.

Internet Protocol Security

Objective

IPsec is implemented correctly as an AACP.

Scope

This section describes conditions under which IPsec can be used as an AACP.

Context

When using a product that implements IPsec, requirements for using AACPs also need to be consulted in the *ASD Approved Cryptographic Protocols* section of this chapter.

Modes of operation

IPsec can be operated in two modes: transport mode or tunnel mode.

Cryptographic protocols

IPsec contains two major protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP).

Cryptographic algorithms

Most IPsec implementations can handle a number of cryptographic algorithms for encrypting data when the ESP protocol is used. These include 3DES and AES.

Key exchange

Most IPsec implementations handle a number of methods for sharing keying material used in hashing and encryption processes. Available methods are manual keying and Internet Key Exchange (IKE), versions 1 and 2, using the Internet Security Association Key Management Protocol (ISAKMP).

Internet Security Association Key Management Protocol authentication

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.

IKE Extended Authentication

Agencies should disable the use of IKE Extended Authentication (XAUTH) for IPsec connections using IKEv1.

Internet Security Association Key Management Protocol modes

Agencies using ISKMP in IKEv1 should disable aggressive mode.

Controls

Mode of operation

The tunnel mode of operation provides full encapsulation of IP packets while the transport mode of operation only encapsulates the payload of the IP packet.

Control: 0494; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use tunnel mode for IPsec connections.

Control: 0495; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies choosing to use transport mode should additionally use an IP tunnel for IPsec connections.

Protocols

In order to provide a secure Virtual Private Network style connection, both authentication and encryption are needed. AH and ESP can provide authentication for the entire IP packet and the payload respectively. However, ESP is generally preferred for authentication since AH by its nature has network address translation limitations. ESP is the only way of providing encryption.

If, however, maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH which will then authenticate the entire IP packet and not just the encrypted payload.

Control: 0496; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use the ESP protocol for IPsec connections.

Key Exchange

There are several methods for establishing shared key material for an IPsec connection. IKE supersedes and addresses a number of risks associated with manual keying. For this reason, IKE is the preferred method for key establishment.

Control: 1233; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use manual keying for Key Exchange when establishing an IPsec connection.

Internet Security Association Key Management Protocol modes

Using ISAKMP main mode instead of aggressive mode provides greater security since all exchanges are protected.

Control: 0497; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies using ISAKMP in IKEv1 should disable aggressive mode for IKE.

Security association lifetimes

Using a secure association lifetime of four hours, or 14400 seconds, provides a balance between security and usability.

Control: 0498; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a security association lifetime of less than four hours, or 14400 seconds.

Hashed Message Authentication Code algorithms

MD5 and SHA–1 are no longer AACAs that can be used with Hashed Message Authentication Code (HMAC). The approved HMAC algorithms are HMAC–SHA256, HMAC–SHA384 or HMAC–SHA512.

Control: 0998; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use HMAC–SHA256, HMAC–SHA384 or HMAC–SHA512 as a HMAC algorithm.

Diffie–Hellman groups

Using a larger DH group provides more entropy for the key exchange.

Control: 0999; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the largest modulus size available for the DH exchange.

Perfect Forward Secrecy

Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

Control: 1000; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use Perfect Forward Secrecy for IPsec connections.

IKE Extended Authentication

XAUTH using IKEv1 has documented vulnerabilities associated with its use.

Control: 1001; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should disable the use of XAUTH for IPsec connections using IKEv1.

References

Further information on IPsec can be found in the *Security Architecture for the Internet Protocol* at http://tools.ietf.org/search/rfc4301.

Key Management

Objective

Cryptographic keying material is protected by key management procedures.

Scope

This section describes the general management of High Assurance cryptographic system keying material.

Context

Due to the wide variety of cryptographic systems and technologies available, and the varied security risks for each, only general key management guidance can be provided in this manual.

If a High Assurance product is being used, agencies are advised to consult the respective equipment ACSI.

Cryptographic systems

Cryptographic systems comprise of equipment, either High Assurance or commercial and keying material. Keying material will be symmetric, asymmetric or certificates in nature. 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.

Controls

Compromise of keying material

If keying material or certificates used for encrypting messages are suspected of being compromised (that is, stolen, lost, copied, loss of control or transmitted over the Internet), then no assurance can be placed in the integrity of subsequent messages that are encrypted in that key. Likewise no assurance can be placed in the confidentiality of a message encrypted using the public key, since third parties could intercept the message and decrypt it using the private key.

In accordance with ACSI 107 and the equipment specific doctrine, agencies are to immediately report to ASD any High Assurance keying material or certificates when they are suspected of being compromised.

Control: 1091; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must immediately revoke keying materials or certificates when they are suspected of being compromised.

High Assurance Equipment

ACSI 53 and ACSI 105 provide product specific policy for High Assurance equipment.

Control: 0499; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: ASD
Agencies must comply with ACSI 53 and ACSI 105 when using High Assurance equipment.

Transporting commercial grade cryptographic equipment

Transporting High Assurance cryptographic equipment in a keyed state is permitted provided, the movement of the equipment complies with the requirements of the equipment specific doctrine and ACSI 103.

Communications security custodian access

Since communications security custodian access involves granting privileged access to a cryptographic system, extra precautions need to be put in place surrounding the personnel chosen to be cryptographic system administrators.

Control: 0502; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Before personnel are granted communications security custodian access, agencies must ensure that they have:

- a demonstrated need for access
- read and agreed to comply with the relevant Key Management Plan (KMP) for the High Assurance cryptographic system they are using
- a security clearance at least equal to the classification of the keying material
- agreed to protect the authentication information for the cryptographic system at the sensitivity or classification of information it secures
- agreed not to share authentication information for the cryptographic system without approval
- agreed to be responsible for all actions under their accounts
- agreed to report all potentially security related problems to an ITSM.

Accounting

As cryptographic keying material and High Assurance equipment, and the keys it stores, provide a significant security function for cryptographic systems, agencies must be able to account for all keying material and High Assurance cryptographic equipment.

Control: 0503; Revision: 2; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must be able to readily account for all transactions relating to High Assurance cryptographic system material, including identifying hardware and software that was issued with the cryptographic equipment and materials, when they were issued and where they were issued.

Compliance checks

High Assurance cryptographic systems compliance checks are used to verify that all account personnel are following proper safeguarding and accounting procedures for keying material and High Assurance equipment.

Inventory

An inventory (also referred to as a muster) is a list of all keying material and High Assurance COMSEC equipment on a COMSEC account which is submitted to the issuing authority for comparison and acquittal. In accordance with ACSI 53, *Communications Security Handbook (Rules and Procedures for the Agency COMSEC Officer and Custodian)*, an inventory is required to be summited twice yearly to the issuing authority.

Control: 0504; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must conduct inventory of cryptographic system material:

- on handover/takeover of administrative responsibility for the cryptographic system
- on change of personnel with access to the cryptographic system
- at least twice a year.

Control: 1003; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform inventory to check all cryptographic system material as per the accounting documentation.

Control: 1004; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should conduct inventory using two personnel that have undergone communications security custodial training and have been appointed as COMSEC custodians.

Area security and access control

As High Assurance cryptographic systems protect particularly sensitive information, additional physical security measures need to be applied. Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*

Control: 0505; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Cryptographic equipment should be stored in a room that meets the requirements for a server room of an appropriate level based on the sensitivity or classification of information the cryptographic system processes.

Control: 0506; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Areas in which High Assurance cryptographic system material is used should be separated from other areas and designated as a cryptographic controlled area.

Developing Key Management Plans for cryptographic systems

Most modern High Assurance cryptographic systems are designed to be highly resistant to cryptographic analysis but it must be assumed that a determined malicious actor 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 High Assurance cryptographic system material by using adequate personnel, physical, documentation and procedural security measures is therefore crucial.

Control: 0509; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: A
Agencies must have an approved KMP in place prior to implementing a High Assurance cryptographic system using High Assurance equipment.

Contents of Key Management Plans

When agencies implement the recommended contents for KMPs they will have a good starting point for the protection of High Assurance cryptographic systems and their material.

Control: 0510; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should document the minimum contents in their KMP as described in ACSI 105.

Control: 0511; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The level of detail included in a KMP must be consistent with the criticality and sensitivity or classification of the information to be protected.

Access register

Access registers can assist in documenting personnel who have privileged access to High Assurance cryptographic systems along with previous accounting and audit activities for the system.

Control: 1005; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA

Agencies should hold and maintain an access register that records High Assurance cryptographic system information such as:

- details of personnel with system administrator access
- details of those whose system administrator access was withdrawn
- details of system documents
- accounting activities
- compliance check activities.

References

Further information key management practices can be found in AS 11770.1:2003, *Information Technology—Security Techniques—Key Management.*

ACSI 53, ACSI 103 and ACSI 105 can also be consulted for additional information on High Assurance cryptography.

Further information relating to physical security is contained in the *Australian Government Physical Security Management Protocol.*

Cross Domain Security

Gateways

Objective

Gateways facilitate secure information transfers between different security domains.

Scope

This section describes the use of gateways.

Context

Gateways act as information flow control mechanisms at the network layer and may also control information at the transport, session, presentation and application layers of the Open System Interconnect (OSI) model.

Additional information relating to topics covered in this section can be found in the following chapters:

- *System Accreditation*
- *Information Security Monitoring*
- *Cyber Security Incidents*
- *Physical Security for Systems*
- *Product Security*
- *Access Control*
- *Network Security*
- *Data Transfers and Content Filtering.*

Deploying gateways

This section describes a baseline for deploying gateways. Agencies need to consult additional sections of this manual depending on the specific type of gateways deployed.

For devices used to control data flow in bi–directional gateways the *Firewalls* section of this chapter needs to be consulted.

For devices used to control data flow in uni–directional gateways the *Diodes* section of this chapter needs to be consulted.

For both bi–directional and uni–directional gateways the *Data Transfers and Content Filtering* chapter needs to be consulted for requirements on appropriately controlling data flows.

Controls

Using gateways

The system owner of the higher security domain of connected security domains would be most familiar with the controls required to protect the more sensitive information and as such is best placed to manage any shared components of gateways. However, in some cases where multiple security domains from different agencies are connected to a gateway it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected agencies.

Control: 0628; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that:

- all systems are protected from systems in other security domains by one or more gateways
- all gateways contain mechanisms to filter data flows at the network layer.

Control: 1192; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that all gateways contain mechanisms to inspect and filter data flows for the transport and higher layers as defined in the OSI model.

Control: 0629; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
For gateways between networks in different security domains, any shared components must be managed by the system owners of the highest security domain or by a mutually agreed party.

Configuration of gateways

Given the criticality of gateways in controlling the flow of information between security domains, any failure—particularly at the higher classifications—may have serious consequences. Hence mechanisms for alerting personnel to situations that may cause cyber security incidents are especially important for gateways.

Control: 0631; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that gateways:

- are the only communications paths into and out of internal networks
- by default, deny all connections into and out of the network
- allow only explicitly authorised connections
- are configured to apply controls as specified in the *Data Transfers and Content Filtering* chapter of this manual
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)
- provide sufficient logging and audit capabilities to detect cyber security incidents, attempted intrusions and overuse/unusual usage patterns
- provide real–time alerts.

Operation of gateways

Providing a sufficient logging and auditing capability helps detect cyber security incidents including attempted network intrusions, allowing the agency to implement counter–measures to reduce the security risk of future attempts.

Storing event logs on a separate secure log server increases the difficulty for intruders to delete logging information in an attempt to destroy evidence of their intrusion.

Control: 0634; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all gateways connecting networks in different security domains are operated and maintained such that they:

- apply controls as specified in the *Data Transfers and Content Filtering* chapter of this manual
- filter and log network traffic attempting to enter the gateway, agencies may choose not to log untrusted Internet traffic providing there is application level logging related to the permitted network communications (eg. the web server logs successful connections).
- log network traffic attempting to leave the gateway
- are configured to save event logs to a separate secure log server
- are protected by authentication, logging and auditing of all physical access to gateway components
- have all controls tested to verify their effectiveness after any changes to their configuration.

Demilitarised zones

Demilitarised zones are used to prevent direct access to information and services on internal networks. Agencies that require certain information and services to be accessed from the Internet can place them in the less trusted demilitarised zone instead of on internal networks.

Control: 0637; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use demilitarised zones to house services accessed externally and mediate internal and external access to information held on agency networks.

Security risk assessment

Performing a security risk assessment on the gateway and its configuration before its implementation assists in the early identification and mitigation of security risks.

Control: 0598; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must perform a security risk assessment on gateways and their configuration before their implementation.

Security risk transfer

Gateways can connect networks in different security domains including across agency boundaries. As a result, all system owners must understand and accept the security risks from all other networks before gateways are implemented.

Control: 0605; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
All owners of systems connected via a gateway must understand and accept the residual security risk of the gateway and from any connected security domains including those connected via a cascaded connection.

Control: 1041; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should review at least annually the security architecture of the gateway and security risks of all connected security domains including those connected via a cascaded connection.

Configuration control

Changes that could introduce vulnerabilities, new security risks or increase security risks in a gateway need to be appropriately considered and documented before being implemented.

Control: 0624; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must update the Security Risk Management Plan before changes are made to the gateway to ensure all security risks have been accepted.

Control: 0625; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must document and assess all changes to gateway architecture in accordance with the agency's change management process.

Testing of gateways

Testing security measures on gateways assists in ensuring that the integrity of the gateway is being maintained. Intruders may be aware of regular testing activities. Therefore, performing testing at irregular intervals will reduce the risk that an intruder could exploit regular testing activities.

Control: 1037; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that testing of security measures is performed at random intervals no more than six months apart.

Shared ownership of gateways

As changes to a security domain connected to a gateway potentially affects the security posture of other connected security domains, system owners need to formally agree to be active information stakeholders in other security domains to which they are connected via a gateway.

Control: 0607; Revision: 1; Updated: Nov-10; Applicability: G, P; Compliance: should; Authority: AA
Once connectivity is established, system owners should become information stakeholders for all connected security domains.

Control: 0608; Revision: 1; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Once connectivity is established, system owners must become information stakeholders for all connected security domains.

User training

It is important that users know how to use gateways securely. This can be achieved through appropriate training before being granted access.

Control: 0609; Revision: 4; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
All users should be trained on the secure use and security risks of gateways before access to systems connected to a gateway is granted.

Control: 0610; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
All users must be trained on the secure use and security risks of gateways before access to the systems connected to a gateway is granted.

Administration of gateways

Administrator privileges need to be minimised and roles need to be separated to minimise the security risk posed by a malicious user with extensive access to the gateway.

Providing system administrators with formal training will ensure they are fully aware of and accept their roles and responsibilities regarding the management of gateways. Formal training could be through commercial providers, or simply through SOPs or reference documents bound by a formal agreement.

Control: 0611; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must limit access to gateway administration functions.

Control: 0612; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that system administrators are formally trained to manage gateways.

Control: 0613; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all system administrators of gateways that process AUSTEO or AGAO information are Australian nationals.

Control: 0616; Revision: 2; Updated: Nov-10; Applicability: G, P; Compliance: should; Authority: AA
Agencies should separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

Control: 0617; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

User authentication

Authentication to networks as well as gateways can reduce the security risk of unauthorised access and provide an auditing capability to support the investigation of cyber security incidents. Additional information on multi–factor authentication is in the *Access Control* chapter.

Control: 0619; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must authenticate users to all sensitive or classified networks accessed through gateways.

Control: 0620; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that only users authenticated and authorised to a gateway can use the gateway.

Control: 1039; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use multi–factor authentication for access to gateways.

ICT equipment authentication

Authenticating ICT equipment to networks accessed through gateways assists in preventing unauthorised ICT equipment connecting to a network. For example, using 802.1x.

Control: 0622; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should authenticate ICT equipment to networks accessed through gateways.

References

Further information regarding the planning, analysis, design, implementation or assessment of CDS can be found in ASD's *Guide to the Secure Configuration of Cross Domain Solutions*, available on OnSecure at https://members.onsecure.gov.au or on request via email at asd.assist@defence.gov.au.

Additional information on the OSI model can be found in the ISO/IEC 7498–1:1994 *Information technology—Open Systems Interconnection: The Basic Model* from http://iso.org/iso/iso_catelogue/catelogue_tc/catelogue_detail.htm?csnumber=20269.

Cross Domain Solutions

Objective

Cross Domain Solutions (CDS) facilitate secure information transfers between systems of different security domains with a high level of assurance.

Scope

This section describes the use of CDS.

Context

CDS provide information flow control mechanisms at each layer of the OSI model with a higher level of assurance than typical gateways. This section extends the preceding *Gateways* section. CDS systems must apply controls from both the *Gateways* and *Cross Domain Solutions* sections.

Additional information relating to topics covered in this section can be found in the following chapters:

- *System Accreditation*
- *Information Security Monitoring*
- *Physical Security for Systems*
- *Product Security*
- *Access Control*
- *Network Security*
- *Data Transfers and Content Filtering.*

Deploying CDS

This section describes a baseline for deploying CDS. Agencies need to consult additional sections of this manual depending on the specific type of CDS deployed.

Agency personnel involved in the planning, analysis, design, implementation or assessment of CDS should refer to the ASD document *Guide to the Secure Configuration of Cross Domain Solutions*, available from https://members.onsecure.gov.au/ or on request from asd.assist@defence.gov.au. This contains a detailed, comprehensive description of controls specific to CDS that are essential for applying a risk–based approach to CDS implementations.

For devices used to control data flow in bi–directional gateways the *Firewalls* section of this chapter needs to be consulted.

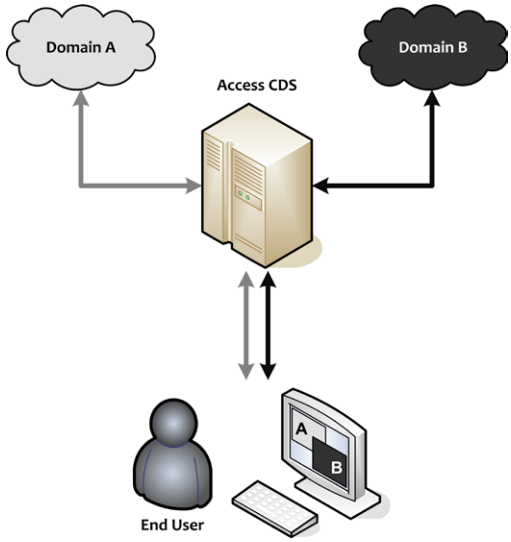
For devices used to control data flow in uni–directional gateways the *Diodes* section of this chapter needs to be consulted.

For both bi–directional and uni–directional gateways the *Data Transfers and Content Filtering* chapter needs to be consulted for requirements on appropriately controlling data flows.

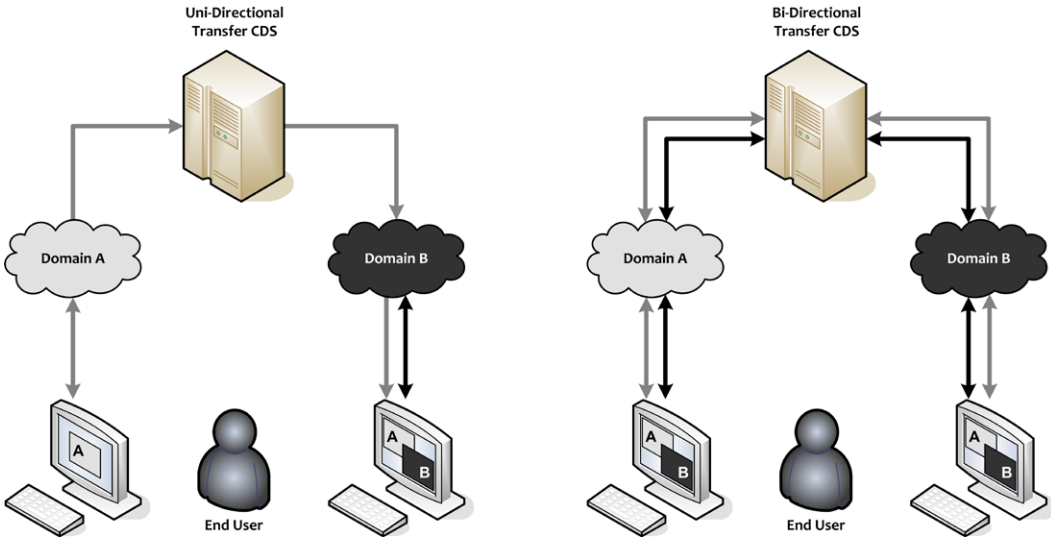
Types of CDS

This manual defines three types of CDS: Access CDS, Multilevel CDS and Transfer CDS.

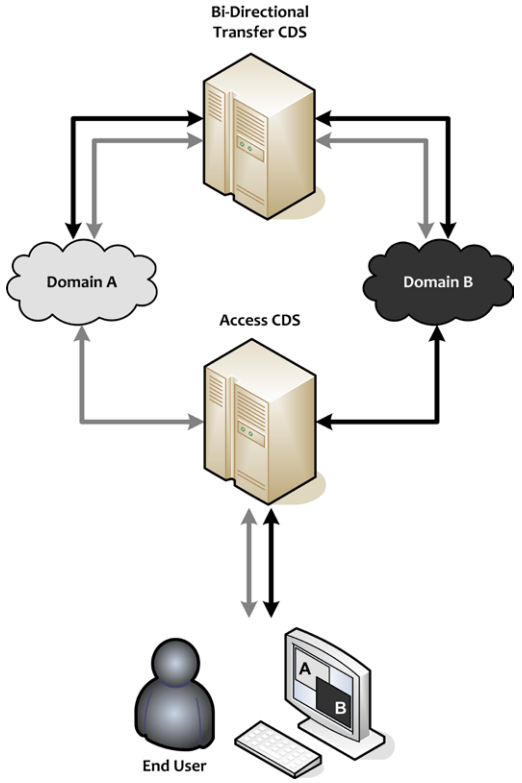
An Access CDS provides the user with access to multiple security domains from a single device.



A Transfer CDS facilitates the transfer of information, in one (uni–directional) or multiple (bi–directional) directions between different security domains.



A Multilevel CDS enables access, based on authorisations, to data at multiple classifications and sensitivity levels.



Applying the controls

For the purposes of gateways and CDS, the gateway assumes the highest sensitivity or classification of the connected security domains.

Controls

Allowable CDS

There are significant security risks associated with connecting highly classified systems to the Internet or to a sensitive or lesser classified system. A malicious actor having control of or access to a gateway can invoke a serious security risk.

Control: 0626; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies connecting a TOP SECRET, SECRET or CONFIDENTIAL network to any other network from a different security domain must implement a CDS.

Implementing CDS

CDS should implement products that have completed a High Assurance evaluation. ASD's EPL includes products that have been evaluated in the High Assurance scheme. However, the EPL is not an exhaustive list of products which are suitable for use in a given CDS. While CDS are not listed on the EPL, ASD can provide guidance on agency implementation in response to a formal request for advice and assistance.

Connecting multiple sets of gateways and CDS increases the threat surface and, consequently, the likelihood and consequence of a network compromise. When a gateway and a CDS share a common network, it exposes the higher security domain (such as a classified agency network) to exploitation from the lower security domain (such as the Internet).

Control: 0597; Revision: 5; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
When designing and deploying a CDS, agencies must consult with ASD Technical Assessments and comply with all directions provided.

Control: 0627; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies connecting a typical gateway and a CDS to a common network must consult with ASD Technical Assessments on the impact to the security of the CDS and comply with all directions provided.

Operation of CDS

In addition to the controls listed in the *Event Logging and Auditing* section in the *Access Control* chapter, CDS have comprehensive logging requirements to establish accountability for all actions performed by users. Effective logging practices can increase the likelihood that malicious behaviour will be detected.

Control: 0670; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When exporting data from a security domain, agencies must ensure that all CDS events are logged.

Separation of data flows

Gateways connecting highly classified systems to other potentially Internet–connected systems need to implement diodes, content filtering and physically separate paths to provide stronger control of information flows. Such gateways are generally restricted to highly formatted formal messaging traffic.

Control: 0635; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that all bi–directional gateways between TOP SECRET, SECRET or CONFIDENTIAL networks and any other network have separate upward and downward network paths using a diode, content filtering and physically separate infrastructure for each path.

Trusted sources

Trusted sources include security personnel such as the CISO, the ITSA, ITSMs and ITSOs.

Control: 0675; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
A trusted source must sign all data to be exported from a security domain.

References

Further information regarding the planning, analysis, design, implementation or assessment of CDS can be found in ASD's *Guide to the Secure Configuration of Cross Domain Solutions*, available on OnSecure at https://members.onsecure.gov.au or on request via email at asd.assist@defence.gov.au.

Firewalls

Objective

Networks connected to bi–directional gateways implement firewalls and traffic flow filters.

Scope

This section describes filtering requirements for bi–directional gateways between networks of different security domains.

Context

When a control specifies a requirement for a diode or filter, the appropriate information can be found in the *Diodes* section of this chapter. Additional information that also applies to topics covered in this section can be found in the *Data Transfers and Content Filtering* chapter. The *Product Security* chapter provides advice on selecting evaluated products.

Government systems

All references to 'Unclassified (DLM)' in the tables here relate to media containing unclassified but official/sensitive information not intended for public release, such as DLM information. ASD advises that government system (G) controls in the ISM are applied as a baseline to ICT equipment storing or processing Unclassified (DLM) information. Unclassified (DLM) and 'Government' are not classifications under the *Australian Government Security Classification System* as mandated by the Attorney–General's Department.

Controls

Firewalls

Where an agency connects to another agency over public network infrastructure both agencies need to implement traffic flow filtering in their gateway environment to protect themselves from intrusions that originate outside of their environment.

These gateway infrastructure requirements may not be necessary in the specific cases where:

- the public network infrastructure is used only as a transport medium
- the public network infrastructure is not a logical source or destination of data
- link encryption is used in accordance with the *Cryptography* chapter.

A proxy is a proxy server that acts as an intermediary for requests from within the agency seeking resources external to the agency. A client connects to the proxy server, requesting some service, such as a file, connection, website, or other resource, available from a source external to the agency. The proxy server evaluates the request according to its filtering rules.

The Network Device Protection Profile (NDPP), defined by the United States' National Information Assurance Partnership, outlines the security requirements for a network device (as opposed to an end–user device) that can be connected to a network.

Control: 0639; Revision: 5; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a firewall as part of their traffic flow filter which satisfies the following table.

	OTHER NETWORK			
YOUR NETWORK	PUBLIC	UNCLASSIFIED (DLM)	PROTECTED	CONFIDENTIAL SECRET TOP SECRET
CONFIDENTIAL SECRET TOP SECRET	Consult with ASD	Consult with ASD	Consult with ASD	Consult with ASD Technical Assessments
PROTECTED	NDPP–compliant firewall	NDPP–compliant firewall	NDPP–compliant firewall	Consult with ASD Technical Assessments
Unclassified (DLM)	None	None	NDPP–compliant firewall	Consult with ASD Technical Assessments

Control: 1194; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
The requirement to use a firewall as part of gateway infrastructure must be met by both parties independently; shared equipment does not satisfy the requirements of both parties.

Firewalls for particularly sensitive networks

As AUSTEO and AGAO networks are particularly sensitive, additional security measures need to be put in place when connecting them to other networks.

Control: 0641; Revision: 5; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must use an ASD approved NDPP–compliant firewall from the EPL between an AUSTEO or AGAO network and a foreign network in addition to the firewall between networks of different classifications or security domains.

Control: 0642; Revision: 5; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should use an ASD approved NDPP–compliant firewall from the EPL between an AUSTEO or AGAO network and another Australian controlled network in addition to the firewall between networks of different classifications or security domains.

References

Further information on the NDPP is available at http://www.niap-ccevs.org/pp/pp_nd_v1.0/.

Diodes

Objective

Networks connected to uni–directional gateways implement diodes.

Scope

This section describes filtering requirements for uni–directional gateways used to facilitate data transfers.

Context

Additional information can be found in the *Data Transfers and Content Filtering* chapter. The *Product Security* chapter provides advice on selecting evaluated products.

As no ASD Protection Profile exists for data diodes, diodes are to be selected in accordance with the following controls.

Controls

Diodes

A diode enforces one–way flow of network traffic thus requiring separate paths for incoming and outgoing data. This makes it much more difficult for a malicious actor to use the same path to both launch an intrusion/attack and release the information.

Control: 0643; Revision: 4; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies must use a Common Criteria–evaluated diode for controlling the data flow of uni–directional gateways between sensitive or classified networks and public network infrastructure.

Control: 0645; Revision: 4; Updated: Feb-14; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must use a High Assurance diode from ASD's EPL for controlling the data flow of uni–directional gateways between classified networks and public network infrastructure.

Control: 1157; Revision: 2; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Agencies must use a Common Criteria–evaluated diode for controlling the data flow of uni–directional gateways between sensitive and classified networks.

Control: 1158; Revision: 3; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a High Assurance diode from ASD's EPL for controlling the data flow of uni–directional gateways between sensitive or classified networks where the highest system is CONFIDENTIAL or above.

Diodes for AUSTEO and AGAO networks

While diodes between networks at the same classification generally are not needed, AUSTEO and AGAO networks are particularly sensitive and additional security measures need to be put in place when connecting them to other networks

Control: 0646; Revision: 3; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must use a Common Criteria–evaluated diode between an AUSTEO or AGAO network and a foreign network at the same classification.

Control: 0647; Revision: 5; Updated: Feb-14; Applicability: P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a Common Criteria–evaluated diode from ASD's EPL between an AUSTEO or AGAO network and another agency controlled network at the same classification.

Volume checking

Monitoring the volume of data being transferred across a diode ensures 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. Further information on monitoring can be found in the *Information Security Monitoring* and *Data Transfers and Content Filtering* chapters of this manual.

Control: 0648; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies deploying a diode to control data flow in uni–directional gateways should monitor the volume of the data being transferred.

References

Additional information on the EPL can be found on ASD's website at http://www.asd.gov.au/infosec/epl/index.php.

Web Content and Connections

Objective

Access to web content is implemented in a secure and accountable manner.

Scope

This section describes appropriate usage policies and technical controls for accessing domains and web content. The requirements in this section primarily apply to external websites.

Context

This section covers factors that need to be taken into consideration when creating policy for allowing web access to ensure the confidentiality, integrity and availability of information and to protect against the execution and spread of malicious software. This section also applies Internet–connected networks and to inter–network connections (that may not be Internet–connected) equally.

Controls

Web usage policy

If agencies allow users to access the web they will need to define the extent of web access that is granted. This can be achieved through a web usage policy and education of users.

Control: 0258; Revision: 1; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must have a policy governing appropriate web usage.

Web proxy

Web proxies are a key component in detecting and responding to malicious software incidents. Comprehensive web proxy logs are valuable in responding to a malicious software incident or user violation of web usage policies.

Control: 0260; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure all web access, including that by internal servers, is conducted through a web proxy.

Control: 0261; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
A web proxy should authenticate users and provide logging that includes the following details about websites accessed:

- address (uniform resource locator)
- time/date
- user
- amount of data uploaded and downloaded
- internal IP address
- external IP address.

Web browsers and add–ons

Many web browsers can be extended with the inclusion of add–ons. These add–ons can have access to sensitive or classified information such as page content and cookie information. A malicious or poorly written add–on may leak this sensitive information to external parties or communicate sensitive information over insecure channels.

Control: 1235; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict the installation of add–ons to only those add–ons approved by the agency.

Transport Layer Security filtering

Since Transport Layer Security (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 and TLS inspection so that web traffic can be filtered.

An alternative to TLS inspection for HTTPS websites is to allow websites that have a low risk of delivering malicious code and have a high privacy requirement, such as Internet banking, to continue to have end–to–end encryption.

Control: 0263; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies permitting TLS through their gateways should implement either:

- a solution that decrypts and inspects the TLS traffic as per content filtering requirements
- a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses either blocked or decrypted and inspected as per content filtering requirements.

Inspection of Transport Layer Security traffic

As encrypted TLS traffic may contain personally identifiable information agencies are recommended to seek legal advice on whether inspecting such traffic could be in breach of the *Privacy Act 1988.*

Control: 0996; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should seek legal advice regarding the inspection of encrypted TLS traffic by their gateways.

Whitelisting websites

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 users 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.

Even a relatively permissive whitelist offers better security than relying on blacklists, or no restriction at all, while still reducing implementation costs. An example of a permissive whitelist could be:

- whitelist the entire Australian subdomain, that is *.au
- whitelist the top 1,000 sites from the Alexa site ranking (after filtering dynamic DNS domains and other inappropriate domains).

Control: 0958; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement whitelisting for all Hypertext Transfer Protocol traffic communicated through their gateways.

Control: 0995; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies using a whitelist on their gateways to specify the external addresses to which connections are permitted, should specify whitelist addresses by domain name or IP address.

Categorising websites

Websites can be grouped into categories and non–work related categories can be blocked via a web content filter.

Control: 1170; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If agencies do not whitelist websites they should implement categories for all websites and block prohibited categories and uncategorised sites.

Blacklisting websites

Blacklists are collections of websites that have been deemed to be inappropriate due to their content or hosting of malicious content. Sites are listed individually and can be categorised.

Intrusions commonly use dynamic or other domains where domain names can be registered anonymously for free due to their lack of attribution.

Control: 0959; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
If agencies do not whitelist websites they should blacklist websites to prevent access to known malicious websites.

Control: 0960; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies blacklisting websites should update the blacklist on a daily basis to ensure that it remains effective.

Control: 1171; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should block attempts to access a website through its IP address instead of through its domain name.

Control: 1236; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should block dynamic and other domains where domain names can be registered anonymously for free.

Web content filter

An effective web content filter greatly reduces the risk of a malicious code infection or other inappropriate content from being accessed. Web content filters can also disrupt or prevent an intruder from communicating with their malicious software.

Some content filtering performed by a web content filter is the same as that performed by email or other content filters, other types of filtering is specific to the web domain.

Further information on web content filtering can be found in the *Data Transfers and Content Filtering* chapter.

Control: 0963; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use the web proxy to filter content that is potentially harmful to hosts and users.

Control: 0961; Revision: 4; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should restrict client–side active content, such as Java and ActiveX to a whitelist of approved websites. This whitelist may be the same as the HTTP whitelist, or a separate active content whitelist.

Control: 1237; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that web content filtering controls are applied to outbound web traffic where appropriate.

References

A web whitelisting software application that allows for the management of whitelists can be obtained from http://whitetrash.sourceforge.net/.

The sites http://www.shallalist.de/ and http://www.urlblacklist.com/ contain lists and categories of sites that can be used to block access to.

Examples of client–side JavaScript controls are available at http://noscript.net/.

Details of JavaScript functions that are typically used for malicious purposes can be found in advisories on the OnSecure website at https://members.onsecure.gov.au/.

Data Transfers and Content Filtering

Data Transfer Policy

Objective

Data is transferred between systems in a controlled and accountable manner.

Scope

This section describes data transfers between systems. It applies equally to data transfers using removable media or using a cross domain solution or gateway.

Context

Additional requirements for data transfers using removable media can be found in the *Media Usage* section of the *Media Security* chapter. Additional requirements for data transfers via gateways or security domains can be found in the *Content Filtering* section of this chapter.

Controls

User responsibilities

When users transfer data to or from a system they need to be aware of the potential consequences of their actions. This could include data spills of sensitive or classified data onto systems not accredited to handle the data, or the unintended introduction of malicious code to a system. Accordingly, users need to be held accountable for all data transfers that they make.

Control: 0661; Revision: 4; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that users transferring data to and from a system are held accountable for the data they transfer through agency policies and procedures.

Data transfer authorisation

Users can help prevent cyber security incidents by:

- checking protective markings to ensure that the destination system is appropriate for the data being transferred
- performing antivirus checks on data to be transferred to and from a system
- following all processes and procedures for the transfer of data.

Control: 0664; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
All data transferred to a system of a lesser sensitivity or classification must be approved by a trusted source.

Trusted sources

Trusted sources include security personnel such as the CISO, the ITSA, ITSMs and ITSOs.

Control: 0665; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Trusted sources must be:

- a strictly limited list derived from business requirements and the result of a security risk assessment
- approved by the accreditation authority.

Import of data

Scanning imported data for malicious content reduces the security risk of a system being infected, thus allowing the continued confidentiality, integrity and availability of the system.

Control: 0657; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: must; Authority: AA
Data imported to a system must be scanned for malicious and active content.

Format checks provide a method to prevent known malicious formats from entering the system. Keeping and regularly auditing these logs allow for the system to be checked for any unusual usage.

Control: 0658; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Data imported to a system must undergo:

- scanning for malicious and active content
- data format checks
- logging of each event
- monitoring to detect overuse/unusual usage patterns.

Export of data

When data is exported between systems, protective marking checks can reduce the security risk of data being transferred to a system that is not accredited to handle it or into the public domain.

Control: 1187; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: must; Authority: AA
When exporting data, agencies must implement protective marking checks.

Control: 0669; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When exporting formatted textual data with no free–text fields and all fields have a predefined set of permitted values, the following activities must be undertaken:

- protective marking checks
- logging of each event
- monitoring to detect overuse/unusual usage patterns
- data format checks
- limitations on data types
- keyword searches
- size limits.

References

Nil.

Data Transfer Procedures

Objective

Data is transferred between systems using appropriate procedures.

Scope

This section describes procedures when transferring data between systems. It applies equally to data transfers using removable media or using a cross domain solution or gateway.

Context

Additional requirements for data transfers using removable media can be found in the *Media Usage* section of the *Media Security* chapter. Additional requirements for data transfers via gateways or security domains can be found in the *Content Filtering* section of this chapter.

Controls

Data transfer procedures

Ensuring that correct procedures are adhered to facilitates the appropriate and consistent application of security controls as well as the generation of necessary audit records.

Control: 0662; Revision: 3; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Data transfers should be performed in accordance with procedures approved by the accreditation authority.

Control: 0663; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Data transfers must be performed in accordance with procedures approved by the accreditation authority.

Preventing export of particularly sensitive data to foreign systems

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.

Control: 0678; Revision: 1; Updated: Nov-10; Applicability: P, C, S, TS; Compliance: must; Authority: AA
When exporting data from an AUSTEO or AGAO system, the following additional activities must be undertaken:

- ensure that keyword searches are performed on all textual data
- ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator
- develop procedures to prevent AUSTEO and AGAO information in both textual and non–textual formats from being exported.

References

Nil.

Content Filtering

Objective

Information transiting a gateway or cross domain solution is examined to permit its flow to be controlled according to security policy.

Scope

This section describes the use of content filtering to protect security domains.

Context

Content filters reduce the security risk of unauthorised or malicious content transiting a security domain boundary.

Content filtering

The following techniques can assist agencies with assessing the suitability for data to transit a security domain boundary.

TECHNIQUE	PURPOSE
Antivirus scan	Scans the data for viruses and other malicious code.
Automated dynamic analysis	Analyses email and web content in a sandbox before delivering it to users.
Data format check	Inspects data to ensure that it conforms to expected and permitted formats.
Data range check	Checks the data in each field to ensure that it falls within the expected and permitted ranges.
Data type check	Inspects each file header to determine the actual file type.
File extension check	Inspects the file name extension to determine the purported file type.
Keyword search	Searches data for keywords or 'dirty words' that could indicate the presence of sensitivity, 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 is correct.
Manual inspection	The manual inspection of data for suspicious content that an automated system could miss, which is particularly important for the transfer of multimedia or content rich files.

Controls

Content filtering

Implementing a content filter reduces the likelihood of malicious content successfully passing into a security domain.

Control: 0659; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA

When importing data to a security domain, or through a gateway, the data must be filtered by a product designed for that purpose.

Active, malicious and suspicious content

Many files are executable and are potentially harmful if executed by a user. Many file type specifications allow active content to be embedded in the file, which increases the attack surface. The definition of suspicious content will depend on the system's security risk profile and what is considered to be normal system behaviour.

Control: 0651; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must block all suspicious data and malicious and active content from entering a security domain.

Control: 0652; Revision: 1; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must block any data identified by a content filtering process as suspicious until reviewed and approved for transfer by a trusted source other than the originator.

Automated dynamic analysis

Analysing email and web content in a sandbox is a highly effective strategy to detect suspicious behaviour including network traffic, new or modified files or other configuration changes.

Control: 1389; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Email and web content entering a security domain should be automatically run in a dynamic malware analysis sandbox to detect suspicious behaviour.

Content validation

Content validation aims to ensure that the content received conforms to a defined, approved standard. Content validation can be an effective means of identifying malformed content, allowing agencies to block potentially malicious content. Content validation operates on a whitelisting principle, blocking all content except for that which is explicitly permitted. Examples of content validation include:

- ensuring numeric fields only contain numeric numbers
- ensuring content falls within acceptable length boundaries
- ensuring XML documents are compared to a strictly defined XML schema.

Control: 1284: Revision: 0; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Agencies should perform validation on all data passing through a content filter, blocking content which fails the validation.

Control: 1285: Revision: 0; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must perform validation on all data passing through a content filter, blocking content which fails the validation.

Content conversion and transformation

Content/file conversion or file transformation can be an effective method to render potentially malicious content harmless by separating the presentation format from the data. By converting a file to another format, the exploit, active content and/or payload can be removed or disrupted enough to be ineffective.

Examples of file conversion and content transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a PDF file
- converting a Microsoft PowerPoint presentation to a series of JPEG images
- converting a Microsoft Excel spreadsheet to a Comma Separated Values (CSV) file
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. Applying the conversion process to any attachments or files contained within other files, for example, archive files or encoded files embedded in XML can increase the effectiveness of a content filter.

Control: 1286; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform content/file conversion for all ingress or egress data transiting a security domain boundary.

Content sanitisation

Sanitisation is the process of attempting to make potentially malicious content safe to use by removing or altering active content while leaving the original content as intact as possible. Sanitisation is not as secure a method of content filtering as conversion, though many techniques may be combined. Inspecting and filtering extraneous application and protocol data, including metadata, where possible will assist in mitigating the threat of content exploitation. These include:

- removal of document properties information in Microsoft Office documents
- removal or renaming of JavaScript sections from PDF files
- removal of metadata, such as EXIF information from within JPEG files.

Control: 1287: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform content/file sanitisation on suitable file types if content/file conversion is not appropriate for data transiting a security domain boundary.

Antivirus scans

Antivirus scanning is used to prevent, detect and remove malicious software that includes computer viruses, worms, Trojans, spyware and adware.

Control: 1288: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform antivirus scans on all content using up–to–date engines and signatures, using multiple different scanning engines.

Archive and container files

Archive and container files can be used to bypass content filtering processes if the content filter does not handle the file type and embedded content correctly. Ensuring the content filtering process recognises archived and container files will ensure the embedded files they contain are subject to the same content filtering measures as un–archived files.

Archive files can be constructed in a manner which can pose a denial of service risk due to processor, memory or disk space exhaustion. To limit the risk of such an attack, content filters can specify resource constraints/quotas while extracting these files. If these constraints are exceeded the inspection is terminated, the content blocked and a security administrator alerted.

Control: 1289: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should extract the contents from archive/container files and subject the extracted files to content filter tests.

Control: 1290: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should perform controlled inspection of archive/container files to ensure that content filter performance or availability is not adversely affected.

Control: 1291: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should block files that cannot be inspected and generate an alert or notification.

Whitelisting permitted content

Creating and enforcing a whitelist of allowed content/files is a strong content filtering method. Only allowing content that satisfies a business requirement can reduce the attack surface of the system. As a simple example, an email content filter might only allow Microsoft Office documents and PDF files.

Control: 0649; Revision: 2; Updated: Sep-12; Applicability: G, P; Compliance: should; Authority: AA
Agencies should identify, create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

Control: 0650; Revision: 2; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must identify, create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

Data integrity

Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. It is also essential that content that has been authorised for release from a security domain is not modified, for example by the addition or substitution of sensitive information. If content passing through a filter contains a form of integrity protection, such as digital signature, the content filter needs to verify the content's integrity before allowing it through. If the content fails these integrity checks it may have been spoofed or tampered with and should be dropped.

Examples of data integrity checks include:

- an email server or content filter verifying an email protected by DKIM
- a web service verifying the XML digital signature contained within a SOAP request
- validating a file against a separately supplied hash
- checking that data to be exported from the security domain has been digitally signed by the release authority.

Control: 1292: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should verify the integrity of content where applicable, and block the content if verification fails.

Control: 0677; Revision: 3; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
If data is signed, agencies must ensure that the signature is validated before the data is exported.

Encrypted data

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Agencies will need to consider the need to decrypt content, depending on the security domain they are communicating with and depending on whether the need–to–know principle needs to be enforced. Choosing not to decrypt content poses a risk of encrypted malicious software communications and data moving between security domains. Additionally, encryption could mask the movement of information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill. Some systems allow encrypted content through external/boundary/perimeter controls to be decrypted at a later stage, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

Control: 1293: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should decrypt and inspect all encrypted content, traffic and data to allow content filtering.

Monitoring data import and export

It is important to monitor the import and export process to ensure the confidentiality and integrity of systems and data.

Control: 0667; Revision: 3; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must use protective marking checks to restrict the export of data out of each security domain, including through a gateway.

Control: 0660; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When importing data to each security domain, including through a gateway, agencies must audit the complete data transfer logs at least monthly.

Control: 0673; Revision: 4; Updated: Sep-12; Applicability: C, S, TS; Compliance: must; Authority: AA
When exporting data out of each security domain, including through a gateway, agencies must audit the complete data transfer logs at least monthly.

Control: 1294: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
When importing content to a security domain, including through a gateway, agencies should perform monthly audits of the imported content.

Control: 1295: Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
When exporting content out of a security domain, including through a gateway, agencies should perform monthly audits of the exported content.

Preventing export of AUSTEO and AGAO data to foreign systems

As AUSTEO and AGAO data is particularly sensitive, additional security measures are needed to protect the confidentiality of this data when multiple security domains are connected.

Control: 1077; Revision: 2; Updated: Sep-12; Applicability: P, C, S, TS; Compliance: must; Authority: AA
Agencies must implement content filtering to prevent the export of AUSTEO and AGAO data to foreign systems, ensuring that:

- at a minimum, keyword searches are performed on all textual data
- any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator.

References

Nil.

Working Off–Site

Mobile Devices

Objective

Information on mobile devices is protected from unauthorised disclosure.

Scope

This section describes the use of mobile devices including mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers and other portable Internet–connected devices.

Context

The controls in this section are intended to provide advice which is applicable to a range of mobile devices. To complement this, ASD also publishes device–specific guidance. Where device–specific advice exists this should be consulted in conjunction with the controls in this section when assessing the risks related to the use of mobile devices.

Trusted Operating Environments

A Trusted Operating Environment (TOE) provides assurance that a reasonable effort has been made to secure the operating system of a mobile device such that it presents a reduced security risk to an agency's information and systems. Security measures that can be implemented to assist in the development of a TOE include:

- unnecessary software and operating system components are removed
- unused or undesired functionality in software and operating systems is disabled
- antivirus or other Internet security software is installed and regularly updated
- software–based firewalls limiting inbound and outbound network connection are installed
- installed software and operating system patching is current
- each connection is authenticated before permitting access to an agency network
- both the user and mobile device are authenticated during the authentication process
- privileged access from the mobile device to the agency network is not allowed.

Treating workstations as mobile devices

When a workstation is issued for home–based work instead of a mobile device, the requirements in this section equally apply to the workstation.

Bluetooth Devices

For devices such as keyboards that use Bluetooth and for security risks to consider, refer to the *Radio Frequency, Infrared and Bluetooth Devices* section of the *Communications Systems and Devices* chapter.

Controls

Mobile devices usage policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that policies are developed to ensure that mobile devices are protected in an appropriate manner when used outside of controlled facilities. Information on the use of encryption to reduce storage and physical transfer requirements is detailed in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Control: 1082; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must develop a policy governing the use of mobile devices.

Control: 1195; Revision: 0; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should use a Mobile Device Management solution to ensure their mobile device policy is applied to all mobile devices that are used with their systems.

Control: 0687; Revision: 4; Updated: Feb-14; Applicability: TS; Compliance: must not; Authority: ASD
Agencies must not allow mobile devices to process or store TOP SECRET information unless explicitly approved by ASD to do so.

Personnel awareness

Mobile devices can have both a data and voice component capable of processing or communicating sensitive or classified information. In such cases, personnel need to know the sensitivity or classification of information which the mobile device has been approved to process, store and communicate. This includes the use of Multimedia Message Service and Short Message Service not being appropriate for sensitive or classified information since they bypass technical security measures. Sensitive communications may require a third party product to ensure content transmitted via this means is encrypted.

Control: 1083; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must advise personnel of the sensitivities and classifications permitted for data and voice communications when using mobile devices.

Non–agency owned mobile devices

If agencies choose to allow personnel to use their personal mobile devices to access the agency's systems, they will need to ensure that the device does not present a threat to the systems. ASD recommends the use of managed separation such as an encrypted managed containers, combined with Mobile Device Management to provide a level of assurance. Alternatively, agencies could implement remote desktop software to present an endorsed SOE to personnel on their mobile devices.

Control: 1047; Revision: 4; Updated: Apr-13; Applicability: G; Compliance: should; Authority: AA
If agencies wish to allow sensitive information to be stored on the device, they should:

- use managed separation, such as an encrypted managed containers, combined with Mobile Device Management, or
- use appropriately configured remote virtual desktop software.

Control: 0693; Revision: 3; Updated: Apr-13; Applicability: P; Compliance: must; Authority: AA
If agencies wish to allow PROTECTED information to be stored on the device, they must:

- use managed separation, such as an encrypted managed container, combined with Mobile Device Management, or
- use appropriately configured remote virtual desktop software.

Control: 0694; Revision: 3; Updated: Apr-13; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not allow non–agency owned mobile devices to access highly classified systems.

Control: 0172; Revision: 2; Updated: Sep-11; Applicability: TS; Compliance: must not; Authority: AA
Agencies must not permit non–agency owned mobile devices to be brought into TOP SECRET areas without prior approval from the accreditation authority.

Allowing non–agency owned mobile devices to access agency systems can increase liability risk. Agencies must seek legal advice to ascertain whether this scenario affects agency compliance with relevant legislation (for example, compliance with government data retention laws in the *Archives Act 1983*), as well as whether the increased liability risks are acceptable to the agency. Risks will be dependent on each agency's mobile device policy and implementation.

Control: 1297; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Prior to allowing non–agency owned mobile devices to connect to an agency system, agencies must seek legal advice.

Agency owned mobile device storage encryption

Encrypting the internal storage and removable media of agency owned mobile devices will lessen the security risk associated with a lost or stolen device. While the use of encryption may not be suitable to treat the mobile device as an unclassified asset it will still present a significant challenge to a malicious actor looking to gain easy access to information stored on the device. To ensure that the benefits of encryption on mobile devices are not negated, users are reminded that they must not store passphrases for the encryption software on, or with, the device.

Information on the use of encryption to reduce storage and physical transfer requirements is detailed in the *Cryptographic Fundamentals* section of the *Cryptography* chapter.

Control: 0869; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should encrypt information on all mobile devices using at least an AACA.

Control: 1084; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption must physically transfer the device as a sensitive or classified asset in a SCEC endorsed secure briefcase.

Mobile device communications encryption

If appropriate encryption is not available the mobile device communicating sensitive or classified information presents a high risk to the information. Encrypting all sensitive or classified communications, regardless of the protocol used (whether it is communicated using Bluetooth, infrared, Wi–Fi, 3G, 4G or other wireless protocols) is the only way to have complete assurance the information remains confidential. Information encryption requirements are detailed in the *Cryptography* chapter.

Control: 1085; Revision: 1; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies using mobile devices to communicate sensitive or classified information over public network infrastructure must use encryption approved for communicating such information over public network infrastructure.

Mobile device privacy filters

Privacy filters can be applied to the screens of mobile devices to prevent onlookers from reading content off the screen of the device. This assists in mitigating risks from shoulder surfing.

Control: 1145; Revision: 2; Updated: Apr-13; Applicability: C, S, TS; Compliance: should; Authority: AA
Agencies should apply privacy filters to the screens of mobile devices.

Bluetooth functionality for mobile devices

Bluetooth provides inadequate security for information that is passed between the mobile device and other devices connected to it using Bluetooth, such as car kits. Bluetooth has a number of known weaknesses which can potentially be exploited. Therefore, use of Bluetooth on mobile devices for highly classified information introduces a risk of exploitation through these vulnerabilities. When used up to the PROTECTED level, securing Bluetooth appropriately will minimise these risks.

Control: 0682; Revision: 3; Updated: Sep-11; Applicability: C, S, TS; Compliance: must not; Authority: AA
Agencies must not enable Bluetooth functionality on mobile devices.

Agencies should be aware of the risks of Bluetooth pairing, particularly with unknown devices. Bluetooth connections with known devices are also susceptible to man–in–the–middle attacks and eavesdropping. Personnel can reduce the likelihood of a compromise to the connection by considering the security of the location in which they pair devices, for example, a controlled office environment is likely to be more secure than a public location, such as a car park.

Control: 1196; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: must; Authority: AA
Agencies must ensure mobile devices are configured to remain undiscoverable to all other Bluetooth devices except during pairing.

Control: 1198; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: must; Authority: AA
Agencies must ensure Bluetooth pairing is performed so that a connection is only made to the device intended.

Control: 1199; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: should; Authority: AA
Agencies should ensure Bluetooth pairing is only performed for a device required for business needs and pairing that is no longer required is removed from the mobile device.

The device class can be used to restrict the range that the Bluetooth communications will operate over. Typically Bluetooth class 1 devices can communicate up to 100 metres, class 2 devices can communicate up to 10 metres and class 3 devices can communicate up to 5 metres. Some mobile devices do not allow for the configuration of Bluetooth classes. The below controls apply for devices which allow this feature to be configured.

Control: 1197; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: should; Authority: AA
Agencies should ensure mobile devices are configured to allow only Bluetooth classes that are required.

Control: 1202; Revision: 0; Updated: Sep-11; Applicability: G, P; Compliance: should; Authority: AA
Agencies should restrict the range of Bluetooth headsets to less than 10 metres by only using class 2 or class 3 devices.

Bluetooth version 2.1 and subsequent versions introduced secure simple pairing and extended inquiry response. Secure simple pairing improves the pairing process for Bluetooth devices, while increasing the strength, as it uses a form of public key cryptography. Extended inquiry response provides more information during the inquiry procedure to allow better filtering of devices before connecting.

Control: 1200; Revision: 2; Updated: Apr-13; Applicability: G, P; Compliance: must; Authority: AA
If using Bluetooth on a mobile device, agencies must ensure both pairing devices use Bluetooth version 2.1 or later.

Control: 1201; Revision: 2; Updated: Apr-13; Applicability: G, P; Compliance: must; Authority: AA
If using Bluetooth on a mobile device, agencies must ensure the device is configured to avoid supporting multiple Bluetooth headset connections.

Configuration control

Poorly controlled mobile devices are more vulnerable to compromise and provide a malicious actor with a potential access point into systems. Although agencies may initially provide a secure mobile device, the state of security may degrade over time. The security of mobile devices needs to be audited regularly to ensure their integrity.

Control: 0862; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should control the configuration of mobile devices in the same manner as devices in the office environment.

Control: 0863; Revision: 2; Updated: Apr-13; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies allowing mobile devices to access sensitive or classified information should prevent personnel from installing or uninstalling applications on a mobile device once provisioned.

Control: 0864; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must prevent personnel from disabling security functions on a mobile device once provisioned.

Maintaining mobile device security

Relevant ISM controls on applying patches apply to mobile devices. These can be found in the *Software Security* chapter. It is important that mobile devices are regularly tested to ensure that they still meet the agency–defined security configuration and patches are effective.

Control: 1365; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure their mobile carrier is able to provide security updates.

Control: 1366; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure that mobile devices are able to accept security updates from the mobile carrier as soon as they become available.

Control: 1367; Revision: 0; Updated: Feb-14; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement a policy enforcing compliance with an agency–defined security configuration for mobile devices.

Connecting mobile devices to the Internet

During the time a mobile device is connected to the Internet for web browsing, instead of establishing a VPN connection to a system, it is directly exposed to intrusions originating from the Internet. Should web browsing be needed, establishing a VPN connection and browsing the Web though their agency's Internet gateway is best practice.

A split tunnel VPN can allow access to 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 intrusion from such networks. Disabling split tunnelling may not be achievable on all devices. Agencies can refer to the relevant ASD consumer or hardening guide for information on how to manage the residual risks associated with allowing split tunnelling.

Control: 0874; Revision: 3; Updated: Apr-13; Applicability: G, P; Compliance: should; Authority: AA
Agencies should ensure that web browsing from a mobile device is through the agency's Internet gateway rather than via a direct connection to the Internet.

Control: 0705; Revision: 2; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must disable split tunnelling on devices supporting this functionality when using an agency system via a VPN connection.

Paging and message services

As paging and message services do not appropriately encrypt information they cannot be relied upon for the communication of sensitive or classified information.

Control: 0240; Revision: 4; Updated: Apr-13; Applicability: P, C, S, TS; Compliance: must not; Authority: AA
Agencies must not use paging, Multimedia Message Service, Short Message Service or Instant Messaging to communicate classified information.

Control: 1356; Revision: 0; Updated: Apr-13; Applicability: G; Compliance: should not; Authority: AA
Agencies should not use paging, Multimedia Message Service, Short Message Service or Instant Messaging to communicate sensitive information.

Emergency destruction

Agencies need to develop emergency destruction procedures for agency owned mobile devices. Such procedures need to focus on destroying information on the mobile device and not necessarily the device itself if it can be avoided. Many mobile devices used for highly classified information achieve this through the use of a cryptographic key zeroise or sanitisation function. The use of a remote wipe can be used to achieve the destruction of information.

Control: 0700; Revision: 4; Updated: Apr-13; Applicability: G, P; Compliance: should; Authority: AA
Agencies should develop an emergency destruction plan for all agency owned mobile devices.

Control: 0701; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
Agencies must develop an emergency destruction plan for mobile devices.

Control: 0702; Revision: 2; Updated: Nov-10; Applicability: C, S, TS; Compliance: must; Authority: AA
If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobile device, the function must be used as part of the emergency destruction procedures.

References

Further information and specific guidance on enterprise mobility can be found in ASD's Protect publication *Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)*, available on the ASD website at http://www.asd.gov.au.

Further information on Bluetooth security can be found in the NIST SP 800–121 *Guide to Bluetooth Security* at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911133.

Working Outside the Office

Objective

Information on mobile devices is accessed with due care in public locations.

Scope

This section describes restrictions on accessing sensitive or classified information using mobile devices from unsecured locations outside of the office and home environments.

Context

This section does not apply to working from home. Requirements relating to home–based work are outlined in the *Working From Home* section of this chapter. Further information on the use of mobile devices can be found in the *Mobile Devices* section of this chapter.

Controls

Working outside the office

Personnel need to be aware of the environment they use mobile devices in to access and communicate sensitive or classified information, especially in public areas including, but not limited to, public transport, transit lounges and coffee shops. In such locations personnel taking extra care to ensure conversations are not overheard and data is not observed will assist in maintaining the confidentiality of agency information.

Control: 0866; Revision: 2; Updated: Sep-11; Applicability G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should ensure personnel are aware not to access or communicate sensitive or classified information in public locations (e.g. public transport, transit lounges and coffee shops) unless extra care is taken to reduce the chance of being overheard or having the screen of the device observed.

Carrying mobile devices

As mobile devices used outside the office will be carried through areas not certified and accredited to process the information on the device, mechanisms need to be put in place to protect the information stored on them. Carrying mobile devices in a 'secured state' will decrease the risk of accidental or deliberate compromise of sensitive or classified data. A 'secured state' implies encryption is active when the device is not in use. Depending on the type of device, the effectiveness of encrypting a device's internal storage might be reduced if the device is lost or stolen while it is in sleep mode or powered on with a locked screen.

Control: 0870; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure mobile devices are carried in a secured state when not being actively used.

Using mobile devices

As mobile devices are often portable in nature and can be easily stolen it is strongly advised that personnel do not leave mobile device unattended at any time.

Control: 0871; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When in use mobile devices must be kept under continual direct supervision.

Travelling with mobile devices

Agency personnel travelling overseas with mobile devices face additional information security risks, and therefore taking additional steps to mitigate these risks will assist in protecting agency information. When personnel leave Australian borders they also leave behind any expectations of privacy.

Prior to the departure of personnel travelling overseas with a mobile device, agencies can take the following measures:

- patch applications and operating systems
- implement multi–factor authentication
- back–up all data
- remove all non–essential data including sensitive unclassified information
- disable applications that are not essential for the period of travel
- disable Bluetooth and wireless connectivity
- configure wireless to connect only to known, secure networks.

Control: 1298; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agencies should implement technical controls on mobile devices and conduct user education prior to personnel travelling overseas with a mobile device.

Personnel lose control of the information stored on a mobile device any time the device is not on their person. This includes storing the devices in checked–in luggage or in hotel rooms. Such situations provide an opportunity for mobile devices to be stolen or tampered with.

Control: 1087; Revision: 0; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
When travelling with mobile devices and media, personnel must retain control over them at all times, this includes not placing them in checked–in luggage or leaving them unattended for any period of time.

Control: 1299; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Personnel should take the following precautions when travelling overseas with a mobile device:

- avoid storing authentication details or tokens and passphrases with the device
- avoid connecting to open Wi–Fi networks
- clear web browser after each session including history, cache, cookies, URL and temporary files
- encrypt emails where possible
- ensure login pages are encrypted before entering passphrases
- avoid connecting to untrusted computers or inserting removable media.

Inspecting mobile devices following overseas travel allows agencies to check for evidence that the device has been compromised.

Control: 1088; Revision: 2; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
If personnel are requested to decrypt mobile devices for inspection by customs personnel, or their mobile device leaves their possession at any time, they must report the potential compromise of information on the device to an ITSM as soon as possible.

Control: 1300; Revision: 0; Updated: Sep-12; Applicability: G, P, C, S, TS; Compliance: should; Authority: AA
Agency personnel should change all passphrases associated with a mobile device upon return from overseas travel.

References

Nil.

Working From Home

Objective

Personnel working from home protect information in the same manner as in the office environment.

Scope

This section describes information on accessing sensitive or classified information from a home environment in order to conduct home–based work.

Context

When a workstation is issued for home–based work, instead of a mobile device, the requirements from the *Mobile Devices* section of this chapter equally apply to the workstation.

Controls

Physical security for the home environment

When agencies consider allowing personnel to work from a home environment they need to be aware that implementing physical security measures may require modifications to the person's home at the expense of the agency.

Control: 0865; Revision: 2; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that the area in which devices are used meets the requirements in the *Australian Government Physical Security Management Protocol.*

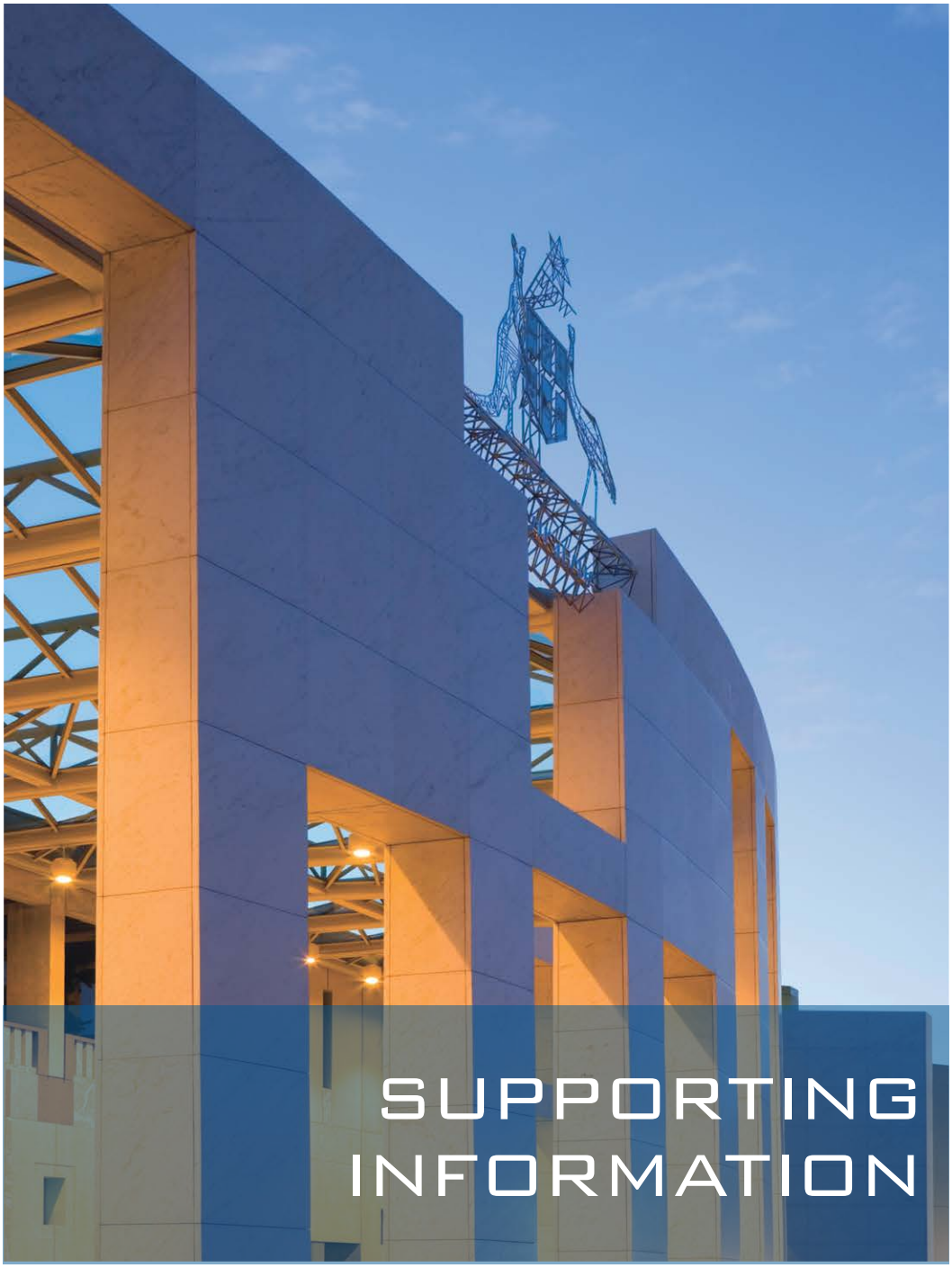
Securing devices in the home environment

All devices have the potential to store sensitive or classified information and therefore need protection against loss and compromise.

Control: 0685; Revision: 3; Updated: Sep-11; Applicability: G, P, C, S, TS; Compliance: must; Authority: AA
Agencies must ensure that when devices are not being actively used they are secured in accordance with the requirements in the *Australian Government Physical Security Management Protocol.*

References

For further information on working from home see the *Australian Government Physical Security Management Guidelines—Working Away From the Office.*



SUPPORTING INFORMATION

Supporting Information

Glossaries

Glossary of Abbreviations

ABBREVIATION	MEANING
3DES	Triple Data Encryption Standard
AACA	ASD Approved Cryptographic Algorithm
AACP	ASD Approved Cryptographic Protocol
ACE	ASD Cryptographic Evaluation
ACSI	Australian Communications Security Instruction
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AGD	Attorney–General's Department
AGIMO	Australian Government Information Management Office
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
ANAO	Australian National Audit Office
AS	Australian Standard
ASA	Agency Security Advisor
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ATA	Advanced Technology Attachment
AUSTEO	Australian Eyes Only
CC	Common Criteria
CISO	Chief Information Security Officer
COE	Common Operating Environment
CSIR	Cyber Security Incident Reporting
DDoS	Distributed denial–of–service
DH	Diffie–Hellman
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EAP–TLS	Extensible Authentication Protocol–Transport Layer Security

ABBREVIATION	MEANING
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read–only Memory
EPL	Evaluated Products List
EPLD	Evaluated Products List Degausser
EPROM	Erasable Programmable Read–only Memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HB	Handbook
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
IRAP	Information security Registered Assessors Program
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISAKMP	Internet Security Association Key Management Protocol
ISM	Australian Government Information Security Manual
ISO	International Organization for Standardization
ISP	Information Security Policy
ITSA	Information Technology Security Advisor
ITSM	Information Technology Security Manager
ITSO	Information Technology Security Officer
KMP	Key Management Plan
LAN	Local Area Network
MFD	Multifunction Device
NAA	National Archives of Australia

ABBREVIATION	MEANING
NDPP	Network Device Protection Profile
NIST	National Institute of Standards and Technology
NZS	New Zealand Standard
OSI	Open System Interconnect
PP	Protection Profile
PSPF	Protective Security Policy Framework
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
SHA	Secure Hashing Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SOE	Standard Operating Environment
SOP	Standard Operating Procedure
SP	Special Publication
SPF	Sender Policy Framework
SRMP	Security Risk Management Plan
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
TLS	Transport Layer Security
TOE	Trusted Operating Environment
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi–Fi Protected Access
WPA2	Wi–Fi Protected Access 2

Glossary of Terms

TERM	MEANING
802.11	The Institute of Electrical and Electronics Engineers standard defining Wireless Local Area Network communications.
access	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information a system contains or to control system components and functions.
access control	The process of granting or denying specific requests for obtaining and using information and related information processing services. Can also refer to the process of granting or denying specific requests to enter specific physical facilities.
access CDS	An information security system permitting access to multiple security domains from a single client device.
accountability	Assignment of actions and decisions to a defined entity.
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. Advice on who should be recognised as an agency's accreditation authority can be found in this manual's *Conducting Accreditations* section of the *System Accreditation* chapter.
agency	Includes all Australian government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the *Public Service Act 1999*, the *Financial Management and Accountability Act 1997* or the *Commonwealth Authorities and Companies Act 1997.*
agency head	The government employee with ultimate responsibility for the secure operation of agency functions, whether performed in–house or outsourced.
aggregation (of data)	A term used to describe compilations of classified or unclassified official information that may require a higher level of protection than their component parts. This is because the combination of the information generates a greater value, and the consequence of the compromise, loss of integrity, or unavailability creates an increase in the business impact level.
application whitelisting	An approach in which an explicitly defined set of applications are permitted to execute on a given system. Any application excluded from this list is not permitted to execute.
asset	Anything of value, such as ICT equipment, software and information.

TERM	MEANING
attack surface	The amount of ICT equipment and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability.
attribute	A property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means.
audit	An independent review and examination of validity, accuracy and reliability of information contained on a system to assess the adequacy of system controls and ensure compliance with established policies and procedures. In the context of conducting system accreditations, an audit is an examination and verification of an agency's systems and procedures, measured against predetermined standards.
audit log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period.
audit trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.
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 ASD, which is responsible for the overall operation of the program.
Australian Eyes Only (AUSTEO)	A caveat indicating that the information is not to be passed to or accessed by foreign nationals.
Australian Government Access Only (AGAO)	A caveat used by the Department of Defence and the Australian Security Intelligence Organisation 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 information security policy produced by ASD that aims to provide a common approach to the implementation of security measures for information and systems across government.
authentication	Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system.
Authentication Header	A protocol used in IPsec that provides data integrity and data origin authenticity but not confidentiality.
availability	The assurance that systems are accessible and useable by authorised entities when required.
biometrics	Measurable physical characteristics used to identify or verify the claimed identity of an individual.

TERM	MEANING
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 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 conforms to a specified standard.
certification authority	An official with the authority to assert that a system complies with prescribed controls in 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 overseeing the application of controls and security risk management processes.
classification	The categorisation of information or systems according to the business impact level associated with that information or a system.
classified information	Information that needs increased security to protect its confidentiality.
classified system	A system that processes, stores or communicates classified information.
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 security measures taken to deny unauthorised personnel information derived from telecommunications and to ensure the authenticity of such telecommunications.
conduit	A tube, duct or pipe used to protect cables.
confidentiality	The assurance that information is disclosed only to authorised entities.

TERM	MEANING
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.
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 ASD internal evaluations, any recommendations for use and references to relevant policy and standards.
content filter	A filter that examines content to assess conformance against a policy. Refer to the *Data Transfers and Content Filtering* chapter for further information.
cross domain solution	An information security system capable of implementing comprehensive data flow security policies with a high level of trust between two or more differing security domains.
cryptographic algorithm	An algorithm used to perform cryptographic functions such as encryption, integrity, authentication, digital signatures or key establishment.
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 to provide confidentiality, integrity, authentication and non–repudiation of information.
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, cryptographic: key, equipment, devices, documents and firmware or software that embodies or describes cryptographic logic.
cyber security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
cyber security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

TERM	MEANING
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Cyber Security Incident Reporting scheme	A scheme established by ASD to collect information on cyber security incidents that affect government systems.
data at rest	Information that is not powered or unauthenticated to that resides on media or a system.
data in transit	Information that is being communicated across a communication medium.
data spill	The accidental or deliberate exposure of classified, sensitive or official information into an uncontrolled or unauthorised environment or to persons without a need–to–know.
declassification	A process whereby information is reduced to an unclassified state and an administrative decision is made to formally authorise its release into the public domain.
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 unreadable.
delegate	A person or group of personnel to whom the authority to authorise non–compliance with requirements in this manual has been delegated by the agency head.
demilitarised zone	A small network with one or more servers that is kept separate from the core network, either on the outside of the firewall, or as a separate network protected by the firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet.
Denial of Service	An attempt by a malicious actor to prevent legitimate access to online services (typically a website), for example by consuming the amount of available bandwidth or the processing capacity of the computer hosting the online service.
device access control software	Software that can be installed on a system to restrict 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.
digital signature	A cryptographic process that allows the proof of the source (with non–repudiation) and the verification of the integrity of that data.

TERM	MEANING
diode	A device that allows data to flow in only one direction.
Dissemination Limiting Marker (DLM)	A protective marker that indicates access to the information should be limited. It is applied to official/sensitive information that has a low to medium business impact from compromise of confidentiality—that is, the level of harm does not require a security classification—and should not be made public without review, or there may be a legislative reason for limiting access. For example, Dissemination Limiting Markers include For Official Use Only and Sensitive.
dual–stack device	A product that implements both IP version 4 and 6 protocol stacks.
emanation security	The counter–measure employed to reduce 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 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 in IPsec.
enclave	A collection of information systems connected by one or more internal networks under the control of a single authority and security policy.
escort	In the context of information security, person who ensures that when maintenance or repairs are undertaken to ICT equipment that uncleared personnel are not exposed to sensitive or classified information.
event	In the context of system logs, an event constitutes an evident change to the normal behaviour of a network, system or user.
facility	An area that facilitates government business. For example, a facility can be a 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 device or software 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.

TERM	MEANING
fly lead	A lead that connects ICT 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.
fuzzing	Fuzzing (or fuzz testing) is a method used to discover errors or potential vulnerabilities in software.
gateway	Gateways securely manage data flows between connected networks from different security domains. Refer to the *Cross Domain Security* chapter for further information.
general user	A user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
government system	Systems containing official government information not intended for public release. These systems would contain at minimum Unclassified (DLM) information. Note 'Government' is not a security classification under the *Australian Government Security Classification System.*
handling requirements	An agreed standard for the storage and dissemination of classified or sensitive information to ensure its protection. This can include electronic information, paper–based information or media containing information.
hardware	A generic term for any physical component of Information and Communication Technology.
Hash–based Message Authentication Code algorithms	A cryptographic construction that can be used to compute Message Authentication Codes using a hash function and a secret key.
High Assurance Evaluation	A rigorous investigation, analysis, verification and validation of a product or system against a stringent information security standard.
High Assurance product	A product that has been approved by ASD for the protection of information classified CONFIDENTIAL or above.
host–based intrusion prevention system	A software application, 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.

TERM	MEANING
ICT equipment	Any device that can process, store or communicate electronic communication—for example, computers, multifunction devices and copiers, landline and mobile phones, digital cameras, electronic storage media and other radio devices.
ICT system	A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.
Incident Response Plan	A plan for responding to cyber security incidents.
information security	All measures used to protect official information from compromise, loss of integrity or unavailability.
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 Assessors Program	A ASD initiative designed to register suitably qualified information security assessors to carry out specific types of security assessments, including for gateways and information systems up to the SECRET classification level.
Information Technology Security Advisor	The ITSM who has responsibility for information technology security management across the agency is designated as the ITSA. This title reflects the responsibility this person has as the first point of contact for the CISO and external agencies on any information technology security management issues.
Information Technology Security Manager	ITSMs are executives that coordinate the strategic directions provided by the CISO and the technical efforts of ITSOs. The main area of responsibility of ITSMs is that of the day–to–day management of information security within an agency.
Information Technology Security Officer	ITSOs implement technical solutions under the guidance of an ITSM to ensure that the strategic direction for information security within the agency set by the CISO is achieved.
infrared device	Devices such as mice, keyboards, pointing devices and mobile devices that have an infrared communications capability.
integrity	The assurance that information is unmodified.
Internet Key Exchange Extended Authentication	Internet Key Exchange Extended Authentication is used for providing an additional level of authentication by allowing IP Security 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.
IPsec	A suite of protocols for secure communications through authentication or encryption of IP packets as well as including protocols for cryptographic key establishment.

TERM	MEANING
Internet Protocol telephony	The transport of telephone calls over IP 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 greater address space available 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 IP Security protocol that uses half the exchanges of main mode to establish an IP Security connection.
ISAKMP main mode	An IP Security protocol that offers optimal security using six packets to establish an IP Security connection.
ISAKMP quick mode	An IP Security protocol that is used for refreshing security association information.
jump server	A computer which is used to manage sensitive or critical resources in a separate security domain. Also known as a jump host or jump box.
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. 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.
lockable commercial cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
logical access controls	ICT measures used to control access to ICT systems and their information—this could involve using user identifications and authenticators such as passwords.
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 or malicious software (malware)	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	The occurrence of malicious code infecting a system. Example methods of malicious code infection include viruses, worms and Trojans. Malicious code infection is a cyber security incident.

TERM	MEANING
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 hardware that is 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 so the data cannot be retrieved or reconstructed.
metadata	Information that describes data. This can include how the data was created, the time and date of creation, the author of the data and the location on a network where the data was created.
mobile device	A portable computing or communications device with information storage capability that can be used from a non–fixed location. Mobile devices include mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers and other portable Internet–connected devices.
Multifunction Devices	The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality in the one device. These devices are often designed to connect to computer and telephone networks simultaneously.
Multilevel Security CDS	Multilevel Security CDS allow access to data at multiple classifications and releasability levels based on authorisation where each data unit is individually marked according to a defined security policy.
need–to–know	The principle to restrict an individual's access to only the information that they require to fulfil their role.
network access control	Policies used 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 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.
network protection device	A sub–class of network device used specifically to protect a network. For example, a firewall.

TERM	MEANING
no–lone zone	An area in which personnel are not permitted to be left alone such that all actions are witnessed by at least one other person.
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	Any information generated by Australian government agencies and contracted providers that is not publicly available, including sensitive and security classified information.
OpenPGP Message Format	An open–source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
patch	A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other program deficiencies and improving the usability or performance of the software.
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 Secrecy	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, such as a Keyboard–Video–Mouse (KVM) switch.
privileged user	A user who can alter or circumvent system security protections. This can also apply to 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 sensitive or classified information to indicate the security measures that need to be applied to the information to ensure that it is appropriately protected.

TERM	MEANING
Protective Security Policy Framework	Produced by the Attorney–General's Department, the *Protective Security Policy Framework* sets out the Australian Government's protective security requirements for the protection of its people, information and assets (replaced the PSM).
public domain information	Unclassified information authorised for unlimited public access or circulation, such as publications and websites.
public network infrastructure	Network infrastructure that an agency has no or limited control over, for example the Internet.
Public Switched Telephone Network	A public network where voice is communicated using analog communications.
public system	A system that processes, stores or communicates only unclassified information that has been authorised for release into the public domain.
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	Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.
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 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 that originates from outside an agency network and enters the network through a gateway, including over the Internet.
removable media	Storage media that can be easily removed from a system and is designed for removal, for example USB flash drives or optical media.
risk	The chance of something happening that will affect objectives—it is measured in terms of event likelihood and consequence.
risk acceptance	An informed decision to accept risk.
risk analysis	The systematic process to understand the nature, and deduce the level of risk.

TERM	MEANING
risk appetite	Statements that communicate the expectations of an agency's senior management about the agency's risk tolerance—these criteria help an agency identify risk and prepare appropriate treatments, and provide a benchmark against which the success of mitigations can be measured.
risk management	The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
risk mitigation	Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk.
residual risk	The remaining level of risk after risk treatments have been implemented.
seconded foreign national	A representative of a foreign government on exchange or long–term posting.
secured space	An area that has been certified to the physical security requirements for a Zone 2 to Zone 5 area as defined in the *Australian Government Physical Security Management Protocol*.
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 files between workstations.
security association	A collection of connection–specific parameters containing information about a one–way connection in IP Security that is required for each protocol used.
security association lifetimes	The duration security association information is valid for.
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 committee is chaired by ASIO and reports to the Protective Security Policy Committee.
security domain(s)	A system or collection of systems operating under a security policy that defines the classification and releasability of the information processed in the domain. It can be exhibited as a classification, a community of interest or releasability within a certain classification.
Security Executive	A member of the Senior Executive Service who is responsible for protective security.

TERM	MEANING
security of information arrangement	A formal arrangement between the Australian Government and a foreign government on the protection of classified information exchanged between the two parties. Details of security of information arrangements can be obtained from the Attorney–General's Department.
security posture	The level of security risk to which a system is exposed. A system with a strong security posture is exposed to a low level of security risk while a system with a weak security posture is exposed to a high level of security risk.
security risk	Any event that could result in the compromise, loss of integrity or unavailability of official information or resources, or harm to people measured in terms of its probability and consequences.
Security Risk Management Plan	A plan that identifies security risks and appropriate risk treatments.
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.
sensitive information	Either unclassified or classified information identified as requiring extra protections (e.g. compartmented or Dissemination Limiting Marker information).
server	A computer (including mainframes) that provides services to users or other systems. For example, a file server, email server or database server.
softphone	A software application that allows a workstation to act as a Voice over Internet Protocol (VoIP) phone, using either a built–in or an externally connected microphone and speaker (e.g. Skype).
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.
split tunnelling	Functionality that allows personnel to access both a public network and a Virtual Private Network connection at the same time, such as an agency system and the Internet.
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 Standard Operating Environment can be used for servers, workstations, laptops and mobile devices.

TERM	MEANING
Standard Operating Procedures	Instructions for operation to ensure a system maintains compliance with its SSP. For example, an approved data transfer process.
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 owner	The person responsible for a resource.
system classification	The classification of a system is the highest classification of information which the system is approved to store or process.
System Security Plan	A plan documenting the security controls and procedures for a system.
target of evaluation	The functions of a product subject to evaluation under a scheme such as the Common Criteria.
technical surveillance counter–measures	The process of surveying facilities 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 is used for point–to–point communication over a distance. This includes digital and IP telephony.
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 ICT equipment	ICT equipment that has been specifically designed to minimise TEMPEST emanations.
threat	Any circumstance or event with the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.
traffic flow filter	A device that has been configured to automatically filter and control the form of data.
transfer CDS	An information security system that facilitates the transfer of information, in one or multiple directions (low to high or high to low), between different security domains.
transport mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an IP payload.
Trusted Operating Environment	An operating environment provides assurance that a reasonable effort has been made to secure an operating system such that it presents a reduced security risk to an agency's information and systems.

TERM	MEANING
trusted source	A person or system formally identified as being capable of reliably producing information meeting certain defined parameters, such as a maximum data classification and reliably reviewing information produced by others to confirm compliance with certain defined parameters.
tunnel mode	An IP Security mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unclassified information	Information that is assessed as not requiring a classification. Unclassified information with a dissemination limiting marker is known as sensitive information while unclassified information without a dissemination limiting marker is authorised for release into the public domain.
unsecured space	An area that has not been certified to physical security requirements to allow for the processing of classified information.
user	An entity authorised to access an information system.
validation	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled.
verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
Virtual Local Area Network (VLAN)	Network devices and ICT equipment grouped logically based on resources, security or business requirements instead of the physical location of the devices and equipment.
Virtual Private Network (VPN)	A virtual private network (VPN) is a private data network that makes use of a networking infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. VPNs may use encryption to protect traffic.
Virtualisation	Simulation of a hardware platform, application, operating system, storage device or network resource; upon which other software runs.
volatile media	A type of media, such as RAM, which gradually loses its information when power is removed.
vulnerability	In the context of information security, a vulnerability is a weakness in system security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

TERM	MEANING
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.
Wi–Fi Protected Access	Certifications of the implementations of protocols designed to replace Wired Equivalent Privacy. They refer to components of the 802.11 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 on 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.

References

This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest baseline comprising the latest release, 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/ or the ASD public website at http://www.asd.gov.au.

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

TOPIC	DOCUMENTATION	AUTHOR
Archiving of information	*The Archives Act (1983)*	National Archives of Australia (NAA)
	Administrative Functions Disposal Authority—Revised 2010	NAA
	General Disposal Authority for Encrypted Records Created in Online Security Processes	NAA
Bluetooth security	NIST SP 800–121, *Guide to Bluetooth Security*	National Institute of Standards and Technology (NIST)
Business continuity	HB 221:2004, *Business Continuity Management*	Standards Australia
	HB 292:2006, *A practitioners guide to business continuity management*	Standards Australia
	HB 293:2006, *Executive guide to business continuity management*	Standards Australia
Cabinet information	*Cabinet Handbook, Security and Handling of Cabinet Documents*	Department of Prime Minister and Cabinet
Cable security	ACSI 61, *Guidelines for the Installation of Communications and Information Processing Equipment and Systems*	ASD
Cloud computing	*Cloud Computing Security Considerations*	ASD
Communications security roles and responsibilities	ACSI 53, *Communications Security Handbook*	ASD
Communications security incident reporting	ACSI 107, *Reporting and Evaluating Communications Security Incidents*	ASD
Cross Domain Solutions	*Guide to the Secure Configuration of Cross Domain Solutions*	ASD
Diffie–Hellman	*New Directions in Cryptography, IEEE Transactions on Information Theory*	W. Diffie, M.E. Hellman
Emanation security	ACSI 71, *A Guide to the Assessment of Electromagnetic Security in Military and High–risk Environments*	ASD

TOPIC	DOCUMENTATION	AUTHOR
Enterprise Mobility	*Risk Management of Enterprise Mobility including Bring Your Own Device (BYOD)*	ASD
Information and records management for ICT systems	*Australian Government Recordkeeping Metadata Standard V2.0*	NAA
	ISO 16175–1:2010, *Principles and functional requirements for records in electronic office environments—Part 1: Overview and statement of principles*	International Organization for Standardization (ISO)
	ISO 16175–2:2011, *Principles and functional requirements for records in electronic office environments—Part 2: Guidelines and functional requirements for digital records management systems*	ISO
	ISO 16175–3:2010, *Principles and functional requirements for records in electronic office environments—Part 3: Guidelines and functional requirements for records in business systems*	ISO
Information security management	*Australian Government Information Security Management Protocol*	Attorney–General's Department (AGD)
	ISO/IEC 27000:2009, *Information technology—Security techniques—Information security management systems—Overview and vocabulary*	ISO / International Electrotechnical Commission (IEC)
	AS/NZS ISO/IEC 27001:2006, *Information technology—Security techniques—Information security management systems—Requirements*	Standards Australia
	AS/NZS ISO/IEC 27002:2006, *Information technology—Security techniques—Code of practice for information security management*	Standards Australia
	ISO/IEC 27003:2010, *Information technology—Security techniques—Information security management systems implementation guidance*	ISO/IEC
	ISO/IEC 27004:2009, *Information technology—Security techniques—Information security management—Measurement*	ISO/IEC
IP Version 6	*A Strategy for the Implementation of IPv6 in Australian Government*	AGIMO
Key management—high grade	ACSI 105, *Cryptographic Controlling Authorities and Keying Material Management*	ASD

TOPIC	DOCUMENTATION	AUTHOR
Management of electronic records that may be used as evidence	HB 171:2003, *Guidelines for the management of IT evidence*	Standards Australia
Media sanitisation	*Data Remanence in Semiconductor Devices*	Peter Gutmann
	Reliably Erasing Data From Flash–Based Solid State Drives	M. Wei, L.M. Grupp, F.E. Spada, S. Swanson
Open Systems Interconnection	ISO/IEC 7498–1:1994, *Information Technology—Open Systems Interconnection: The Basic Model*	ISO/IEC
Personnel security	*Australian Government Personnel Security Management Protocol*	AGD
Physical security	*Australian Government Physical Security Management Protocol*	AGD
Privacy requirements	*The Privacy Act (1988)*	AGD
Protective security	*Australian Government Protective Security Policy Framework*	AGD
Risk management	AS/NZS ISO 31000:2009, *Risk Management—Principles and guidelines*	Standards Australia
	HB 327:2010, *Communicating and consulting about risk (Companion to AS/NZS ISO 31000:2009)*	Standards Australia
	ISO/IEC Guide 73, *Risk Management—Vocabulary—Guidelines for use in Standards*	ISO/IEC
	ISO/IEC 27005:2008, *Information technology—Security techniques—Information security risk management*	ISO/IEC
	HB 167:2006, *Security risk management*	Standards Australia
	HB 231:2004, *Information security risk management guidelines*	Standards Australia
	NIST SP 800–30, *Risk Management Guide for Information Technology Systems*	National Institute of Standards and Technology (NIST)

Index

Numbers

A

B

C

D

E

F

G

H

I

N

O

P

R

S

T

U

V

W

X

asd.gov.au

ASD | REVEAL THEIR SECRETS—PROTECT OUR OWN