Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

APRIL 2021

cyber.gov.au

Table of Contents

ACSC Australian Cyber Security Centre

Using the Australian Government Information Security Manual

Executive summary

Purpose

The purpose of the ***Australian Government Information Security Manual*** (ISM) is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats.

Intended audience

The ISM is intended for Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), cyber security professionals and information technology managers.

Authority

The ISM represents the considered advice of the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under section 7(1)(ca) of the ***Intelligence Services Act 2001***.

The ACSC also provides cyber security advice in the form of consumer guides, Australian Communications Security Instructions and other cyber security-related publications. In these cases, device and application-specific advice may take precedence over the advice in the ISM.

Legislation and legal considerations

Organisations are not required as a matter of law to comply with the ISM, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply. Furthermore, the ISM does not override any obligations imposed by legislation or law. Finally, if the ISM conflicts with legislation or law, the latter takes precedence.

While the ISM contains examples of when legislation or laws may be relevant for organisations, there is no comprehensive consideration of such issues. When designing, operating and decommissioning systems, organisations are encouraged to familiarise themselves with legislation such as the ***Archives Act 1983***, ***Privacy Act 1988*** and ***Telecommunications (Interception and Access) Act 1979***.

Cyber security principles

The purpose of the cyber security principles within the ISM is to provide strategic guidance on how organisations can protect their systems and information from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond. Organisations should be able to demonstrate that the cyber security principles are being adhered to within their organisation.

Cyber security guidelines

The purpose of the cyber security guidelines within the ISM is to provide practical guidance on how organisations can protect their systems and information from cyber threats. These cyber security guidelines cover governance, physical security, personnel security, and information and communications technology security matters. Organisations should consider the cyber security guidelines that are relevant to each of the systems that they operate.

Further information

The complete ISM, including all supporting materials and changes documents, is constantly being reviewed and updated. The latest release can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

Additional cyber security-related publications from the ACSC can be found at https://www.cyber.gov.au/acsc/view-all-content/publications.

Applying a risk-based approach to cyber security

Using a risk management framework

The risk management framework used by the ISM draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, ***Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy***. Within this risk management framework, the identification of security risks and selection of security controls can be undertaken using a variety of risk management standards, such as International Organization for Standardization (ISO) 31000:2018, ***Risk management – Guidelines***. Broadly, the risk management framework used by the ISM has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system.

Define the system

Determine the type, value and security objectives for the system based on an assessment of the impact if it were to be compromised.

When embarking upon the design of a system, the type, value and security objectives for the system, based on confidentiality, integrity and availability requirements, should be determined. This will ultimately guide activities such as selecting and tailoring security controls to meet those security objectives and determining the level of residual risk that will be accepted before the system is authorised to operate.

For organisations that handle government information, the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF) provides guidance within Table 1 (***Business Impact Levels tool – Assessing damage to the national interest, organisations or individuals***) of their ***Sensitive and classified information*** policy to assist in determining the impact of information compromise.

For organisations that do not handle government information, security controls marked as OFFICIAL and OFFICIAL: Sensitive can be used for a baseline level of protection while those marked as PROTECTED can be used for an increased level of protection.

Following the determination of the type and value of a system, along with its security objectives, a description of the system and its characteristics should be documented in the system's system security plan.

Select security controls

Select security controls for the system and tailor them to achieve desired security objectives.

Each cyber security guideline discusses security risks associated with the topic it covers. Paired with these discussions are security controls that the ACSC considers to provide efficient and effective mitigations based on the security objectives for a system.

While security risks and security controls are discussed in the cyber security guidelines, and act as a security control baseline, these should not be considered an exhaustive list for a specific activity or technology. As such, the cyber security guidelines provide an important input into each organisation's risk identification and risk treatment activities however do not represent the full extent of such activities.

While the cyber security guidelines can assist with risk identification and risk treatment activities, organisations will still need to undertake their own risk analysis and risk evaluation activities due to the unique nature of each system, its operating environment and the organisation's risk tolerances.

Following the selection and tailoring of security controls for a system, they should be recorded along with the details of their planned implementation in the system's system security plan annex. In addition, and as appropriate, security controls should also be recorded in both the system's incident response plan and continuous monitoring plan.

Implement security controls

Implement security controls within the system and its operating environment.

Once suitable security controls have been identified and agreed upon for a system, they should be implemented. In doing so, the details of their actual implementation, if different from their planned implementation, should be documented in the system's system security plan annex.

Assess security controls

Assess security controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.

In conducting a security assessment, it is important that assessors and system owners first agree to the scope, type and extent of assessment activities, which may be documented in a security assessment plan, such that any risks associated with the security assessment can be appropriately managed. To a large extent, the scope of the security assessment will be determined by the type of system and security controls that have been implemented for the system and its operating environment.

For TOP SECRET systems, including sensitive compartmented information systems, security assessments can be undertaken by ASD assessors (or their delegates). While for SECRET and below systems, security assessments can be undertaken by an organisation's own assessors or Information Security Registered Assessors Program (IRAP) assessors. In all cases, assessors should hold an appropriate security clearance and have an appropriate level of experience and understanding of the type of system they are assessing.

At the conclusion of a security assessment, a security assessment report should be produced outlining the scope of the security assessment, the system's strengths and weaknesses, security risks associated with the operation of the system, the effectiveness of the implementation of security controls, and any recommended remediation actions. This will assist in performing any initial remediation actions as well as guiding the development of the system's plan of action and milestones.

Authorise the system

Authorise the system to operate based on the acceptance of the security risks associated with its operation.

Before a system can be granted authorisation to operate, sufficient information should be provided to the authorising officer in order for them to make an informed risk-based decision as to whether the security risks associated with its operation are acceptable or not. This information should take the form of an authorisation package that includes the system's system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.

In some cases, the security risks associated with a system's operation will be acceptable and it will be granted authorisation to operate; however, in other cases the security risks associated with operation of a system may be unacceptable. In such cases, the authorising officer may request further work, and potentially another security assessment, be undertaken by the system owner. In the intervening time, the authorising officer may choose to grant authorisation to operate but with constraints placed on the system's use. Finally, if the authorising officer deems the security risks to be unacceptable regardless of any potential constraints on the system's use, they may deny

authorisation to operate until such time that sufficient remediation actions, if possible, have been completed to an acceptable standard.

For TOP SECRET systems, and systems that process, store or communicate sensitive compartmented information, the authorising officer is Director-General ASD or their delegate. While for SECRET and below systems, the authorising officer is an organisation's CISO or their delegate.

For multinational and multi-organisation systems, the authorising officer should be determined by a formal agreement between the parties involved. While for commercial providers providing services to organisations, the authorising officer is the CISO of the supported organisation or their delegate.

In all cases, the authorising officer should have an appropriate level of seniority and understanding of security risks they are accepting on behalf of their organisation. In cases where an organisation does not have a CISO, the authorising officer could be a Chief Security Officer, a CIO or other senior executive within the organisation.

Monitor the system

Monitor the system, and associated cyber threats, security risks and security controls, on an ongoing basis.

Regular monitoring of cyber threats, security risks and security controls associated with a system and its operating environment, as outlined in a continuous monitoring plan, is essential to maintaining its security posture. In doing so, specific events may necessitate additional risk management activities. Such events may include:

- changes in security policies relating to the system
- detection of new or emerging cyber threats to the system or its operating environment
- the discovery that security controls for the system are not as effective as planned
- a major cyber security incident involving the system
- major architectural changes to the system.

Following the implementation or modification of any security controls as a result of risk management activities, another security assessment should be completed. In doing so, the system's authorisation package should be updated. This in turn allows the authorising officer to make an informed risk-based decision as to whether the security risks associated with the system's operation are still acceptable, and whether to grant ongoing authorisation to operate.

Further information

Further information on the use of protective markings can be found in AGD's PSPF, ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.

Further information on various risk management frameworks and practices can be found in:

- Department of Finance's, ***Commonwealth Risk Management Policy***, at https://www.finance.gov.au/government/comcover/commonwealth-risk-management-policy
- AGD's PSPF, ***Security planning and risk management*** policy, at https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/Pages/default.aspx
- ISO 31000:2018, ***Risk management – Guidelines***, at https://www.iso.org/standard/65694.html
- ISO Guide 73:2009, ***Risk management – Vocabulary***, at https://www.iso.org/standard/44651.html
- International Electrotechnical Commission 31010:2019, ***Risk management – Risk assessment techniques***, at https://www.iso.org/standard/72140.html

- ISO 27005:2018, ***Information technology – Security techniques – Information security risk management***, at https://www.iso.org/standard/75281.html
- NIST SP 800-30 Rev. 1, ***Guide for Conducting Risk Assessments***, at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- NIST SP 800-37 Rev. 2, ***Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy***, at https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

The IRAP website lists the range of activities IRAP assessors are authorised to perform. This information is available at https://www.cyber.gov.au/acsc/view-all-content/programs/irap.

Cyber Security Principles

The cyber security principles

Purpose of the cyber security principles

The purpose of the cyber security principles is to provide strategic guidance on how organisations can protect their systems and information from cyber threats. These cyber security principles are grouped into four key activities: govern, protect, detect and respond.

- **Govern:** Identifying and managing security risks.
- **Protect:** Implementing security controls to reduce security risks.
- **Detect:** Detecting and understanding cyber security events.
- **Respond:** Responding to and recovering from cyber security incidents.

Govern principles

- **G1:** A Chief Information Security Officer provides leadership and oversight of cyber security.
- **G2:** The identity and value of systems, applications and information is determined and documented.
- **G3:** The confidentiality, integrity and availability requirements of systems, applications and information is determined and documented.
- **G4:** Security risk management processes are embedded into organisational risk management frameworks.
- **G5:** Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life.

Protect principles

- **P1:** Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.
- **P2:** Systems and applications are delivered and supported by trusted suppliers.
- **P3:** Systems and applications are configured to reduce their attack surface.
- **P4:** Systems and applications are administered in a secure, accountable and auditable manner.
- **P5:** Security vulnerabilities in systems and applications are identified and mitigated in a timely manner.
- **P6:** Only trusted and supported operating systems, applications and computer code can execute on systems.
- **P7:** Information is encrypted at rest and in transit between different systems.
- **P8:** Information communicated between different systems is controlled, inspectable and auditable.
- **P9:** Information, applications and configuration settings are backed up in a secure and proven manner on a regular basis.
- **P10:** Only trusted and vetted personnel are granted access to systems, applications and data repositories.
- **P11:** Personnel are granted the minimum access to systems, applications and data repositories required for their duties.

- **P12:** Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories.
- **P13:** Personnel are provided with ongoing cyber security awareness training.
- **P14:** Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

Detect principles

- **D1:** Cyber security events and anomalous activities are detected, collected, correlated and analysed in a timely manner.

Respond principles

- **R1:** Cyber security incidents are identified and reported both internally and externally to relevant bodies in a timely manner.
- **R2:** Cyber security incidents are contained, eradicated and recovered from in a timely manner.
- **R3:** Business continuity and disaster recovery plans are enacted when required.

Maturity modelling

When implementing the cyber security principles, organisations can use the following maturity model to assess the implementation of either individual principles, groups of principles or the cyber security principles as a whole. The five levels in the maturity model are:

- **Incomplete:** The cyber security principles are either partially implemented or not implemented.
- **Initial:** The cyber security principles are implemented, but in a poor or ad hoc manner.
- **Developing:** The cyber security principles are sufficiently implemented, but on a project-by-project basis.
- **Managing:** The cyber security principles are established as standard business practices and robustly implemented throughout the organisation.
- **Optimising:** A deliberate focus on optimisation and continual improvement exists for the implementation of the cyber security principles throughout the organisation.

Guidelines for Cyber Security Roles

Chief Information Security Officer

Required skills and experience

The role of the Chief Information Security Officer (CISO) requires a combination of technical and soft skills, such as business acumen, leadership, communications and relationship building. Additionally, CISOs must adopt a continuous approach to learning and up-skilling in order to maintain pace with the cyber threat landscape and new technologies. It is expected that CISOs show innovation and imagination in conceiving and delivering cyber security strategies for their organisations.

Providing cyber security leadership and guidance

To provide cyber security leadership and guidance within organisations, it is important that each organisation appoints a CISO.

Security Control: 0714; Revision: 5; Updated: Oct-20; Applicability: O, P, S, TS
A CISO is appointed to provide cyber security leadership and guidance for their organisation.

Overseeing the cyber security program

The CISO within an organisation is typically responsible for providing strategic-level guidance for their organisation's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation. They are likely to work with a Chief Security Officer, a Chief Information Officer and other senior executives within their organisation.

Security Control: 1478; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees their organisation's cyber security program and ensures their organisation's compliance with cyber security policy, standards, regulations and legislation.

Security Control: 1617; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
The CISO regularly reviews and updates their organisation's cyber security program to ensure its relevance in addressing cyber threats and harnessing business and cyber security opportunities.

Security Control: 0724; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO implements cyber security measurement metrics and key performance indicators for their organisation.

Coordinating cyber security

The CISO is responsible for ensuring the alignment of cyber security and business objectives within their organisation. To achieve this, they should facilitate communication between cyber security and business stakeholders. This includes translating cyber security concepts and language into business concepts and language as well as ensuring that business teams consult with cyber security teams to determine appropriate security measures when planning new business projects. Additionally, as the CISO is responsible for the development of the strategic-level cyber security program, they are best placed to advise projects on the strategic direction of cyber security.

Security Control: 0725; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key business and ICT executives, which meets formally and on a regular basis.

Security Control: 0726; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO coordinates security risk management activities between cyber security and business teams.

Reporting on cyber security

The CISO is responsible for directly reporting cyber security matters to their organisation's senior executive and/or Board. Reporting should cover:

- the organisation's security risk profile
- the status of key systems and any outstanding security risks
- any planned cyber security uplift activities
- any recent cyber security incidents
- expected returns on cyber security investments.

Reporting on cyber security matters should be structured by business functions, regions or legal entities and support a consolidated view of the organisation's cyber security risks.

It is important that the CISO is able to translate cyber security risks into operational risks for the organisation, including financial and legal risks, in order to enable more holistic conversations about the organisation's risks.

Security Control: 0718; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO reports directly to their organisation's senior executive and/or Board on cyber security matters.

Overseeing incident response activities

To ensure the CISO is able to accurately report to their organisation's senior executive and/or Board on cyber security matters, it is important they are fully aware of all cyber security incidents within their organisation.

The CISO is also responsible for overseeing their organisation's response to cyber security incidents, including how internal teams respond and communicate with each other during an incident. In the event of a major cyber security incident, the CISO should be prepared to step into a crisis management role. They should understand how to bring clarity to the situation and communicate effectively with internal and external stakeholders.

Security Control: 0733; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO is fully aware of all cyber security incidents within their organisation.

Security Control: 1618; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees their organisation's response to cyber security incidents.

Contributing to business continuity and disaster recovery planning

The CISO is responsible for contributing to the development and maintenance of their organisation's business continuity and disaster recovery plan, with the aim to improve business resilience and ensure the continued operation of critical business processes. Other senior executives may also be responsible for contributing to the development and maintenance of the business continuity and disaster recovery plan.

Security Control: 0734; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO contributes to the development and maintenance of a business continuity and disaster recovery plan for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.

Developing a cyber security communications strategy

To facilitate broad security cultural change across their organisation, the CISO should act as a thought leader continually communicating their strategy and vision. A communication strategy can be helpful in achieving this. Communications should be tailored to different parts of the organisation and be topical for the intended audience.

Security Control: 0720; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
The CISO develops and maintains a cyber security communications strategy for their organisation.

Working with suppliers and service providers

The CISO is responsible for ensuring that a consistent vendor management process is applied across their organisation, from discovery through to ongoing management. As supplier and service provider relationships come with additional security risks for their organisation, the CISO should assist personnel with assessing cyber supply chain risks and understand the security impacts of entering into contracts with suppliers and service providers.

Security Control: 0731; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees cyber supply chain risk management activities for their organisation.

Receiving and managing a dedicated cyber security budget

Receiving and managing a dedicated cyber security budget will ensure the CISO has sufficient access to funding to support their cyber security program, including cyber security uplift activities and responding to cyber security incidents.

Security Control: 0732; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO receives and manages a dedicated cyber security budget for their organisation.

Overseeing cyber security personnel

The CISO is responsible for the cyber security workforce within their organisation, including plans to attract, train and retain cyber security personnel in order to ensure that sufficient resources are in place to perform cyber security functions. CISOs should delegate relevant tasks to cyber security managers and other personnel as required and provide them with adequate authority and resources to perform their duties.

Security Control: 0717; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees the management of cyber security personnel within their organisation.

Overseeing cyber security awareness raising

To ensure personnel are actively contributing to the security posture of their organisation, a cyber security awareness training program should be developed. As the CISO is responsible for cyber security within their organisation, they should oversee the development and operation of the program.

Security Control: 0735; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees the development and operation of their organisation's cyber security awareness training program.

System owners

System ownership and oversight

System owners are responsible for ensuring the secure operation of their systems; however, system owners may delegate the day-to-day management and operation of their systems to system managers.

Security Control: 1071; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Each system has a designated system owner.

Security Control: 1525; Revision: 1; Updated: Jan-21; Applicability: O, P, S, TS
System owners register each system with its authorising officer.

Protecting systems and their resources

Broadly, the risk management framework used by the ***Australian Government Information Security Manual*** has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the

system and monitor the system. System owners are responsible for the implementation of this six step risk management framework for each of their systems.

Security Control: 1633; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners determine the type, value and security objectives for each system based on an assessment of the impact if it were to be compromised.

Security Control: 1634; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners select security controls for each system and tailor them to achieve desired security objectives.

Security Control: 1635; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners implement identified security controls within each system and its operating environment.

Security Control: 1636; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners ensure security controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.

Security Control: 0027; Revision: 4; Updated: Jan-21; Applicability: O, P, S, TS
System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.

Security Control: 1526; Revision: 1; Updated: Jan-21; Applicability: O, P, S, TS
System owners monitor each system, and associated cyber threats, security risks and security controls, on an ongoing basis.

Annual reporting of system security status

Annual reporting on the security status of their systems to their authorising officers (e.g. by providing outcomes of any vulnerability scans and penetration tests) can assist authorising officers in maintaining awareness of the security posture of systems.

Security Control: 1587; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
System owners report the security status of each system to its authorising officer at least annually.

Further information

Further information on using the six step risk management framework can be found in ***Using the Australian Government Information Security Manual***.

Further information on monitoring systems and their operating environments can be found in the ***Guidelines for System Monitoring***.

Guidelines for Cyber Security Incidents

Detecting cyber security incidents

Cyber security events

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

Cyber security incidents

A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.

Cyber resilience

Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.

Detecting cyber security incidents

One of the core elements of detecting and investigating cyber security incidents is the availability of appropriate data sources. Fortunately, many data sources can be extracted from existing systems without requiring specialised capabilities.

The following table describes some of the data sources that organisations can use for detecting and investigating cyber security incidents.

Data Source	Description
Domain Name System logs	Can assist in identifying attempts to resolve malicious domains or Internet Protocol (IP) addresses which can indicate an exploitation attempt or successful compromise.
Email server logs	Can assist in identifying users targeted with spear-phishing emails. Can also assist in identifying the initial vector of a compromise.
Operating system event logs	Can assist in tracking process execution, file/registry/network activity, authentication events, operating system created security alerts and other activity.
Security software and appliance logs	Can assist in the identification of anomalous or malicious activity which can indicate an exploitation attempt or successful compromise.

Virtual Private Network and remote access logs	Can assist in identifying unusual source addresses, times of access and logon/logoff times associated with malicious activity.
Web proxy logs	Can assist in identifying Hypertext Transfer Protocol-based vectors and malware communication traffic.

Intrusion detection and prevention policy

Establishing an intrusion detection and prevention policy can increase the likelihood of detecting, and subsequently preventing, malicious activity on networks and systems. In doing so, an intrusion detection and prevention policy will likely cover the following:

- methods of network-based intrusion detection and prevention used
- methods of host-based intrusion detection and prevention used
- guidelines for reporting and responding to detected intrusions
- resources assigned to intrusion detection and prevention activities.

Security Control: 0576; Revision: 7; Updated: Aug-19; Applicability: O, P, S, TS
An intrusion detection and prevention policy is developed and implemented.

Trusted insider program

As a trusted insider's system access and knowledge of business processes often makes them harder to detect, establishing a trusted insider program can assist organisations to detect and respond to trusted insider threats before they occur, or limit damage if they do occur. In doing so, organisations will likely obtain the most benefit by logging and analysing the following user activities:

- rapid and numerous file copying or changes
- unauthorised or excessive use of removable media
- connecting devices capable of data storage (e.g. mobile devices and digital cameras) to systems
- unusual system usage outside of business hours
- data access or printing which is excessive compared to the normal baseline for a user or their peers
- data transfers to unauthorised cloud computing services or webmail
- use of unauthorised Virtual Private Networks, file transfer applications or anonymity networks.

Security Control: 1625; Revision: 0; Updated: Nov-20; Applicability: O, P, S, TS
A trusted insider program is developed and implemented.

Security Control: 1626; Revision: 0; Updated: Nov-20; Applicability: O, P, S, TS
Legal advice is sought regarding the development and implementation of a trusted insider program.

Access to sufficient data sources and tools

Successful detection of cyber security incidents is often based around trained cyber security personnel with access to sufficient data sources complemented by tools supporting both manual and automated analysis. As such, it is important that during system design and development activities, functionality is added to systems to ensure that sufficient data sources can be provided to cyber security personnel to assist with the detection and remediation of cyber security incidents.

Security Control: 0120; Revision: 5; Updated: May-20; Applicability: O, P, S, TS
Cyber security personnel have access to sufficient data sources and tools to ensure that systems can be monitored for key indicators of compromise.

Further information

Further information on detecting cyber security incidents can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Further information on establishing and operating a trusted insider program can be found in the Carnegie Mellon University's Software Engineering Institute's ***Common Sense Guide to Mitigating Insider Threats*** publication at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644.

Managing cyber security incidents

Cyber security incident register

The purpose of recording cyber security incidents in a register is to highlight their type and frequency so that corrective action can be taken. This information, along with information on the costs of any remediation activities, can also be used as an input to risk assessments and vulnerability management activities.

Security Control: 0125; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
A cyber security incident register is maintained with the following information:

- *the date the cyber security incident occurred*
- *the date the cyber security incident was discovered*
- *a description of the cyber security incident*
- *any actions taken in response to the cyber security incident*
- *to whom the cyber security incident was reported.*

Handling and containing data spills

When a data spill occurs, organisations should inform information owners and restrict access to the information. In doing so, affected systems can be powered off, have their network connectivity removed or have additional access controls applied to the information. It should be noted though that powering off systems could destroy information that would be useful for forensic investigations. Furthermore, users should be made aware of appropriate actions to take in the event of a data spill such as not deleting, copying, printing or emailing the information.

Security Control: 0133; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
When a data spill occurs, information owners are advised and access to the information is restricted.

Handling and containing malicious code infections

Taking immediate remediation steps after the discovery of malicious code can minimise the time and cost spent eradicating and recovering from the infection. As a priority, all infected systems and media should be isolated to prevent the infection from spreading further. Once isolated, infected systems and media can be scanned by antivirus software to potentially remove the infection. It is important to note though, a complete system restoration from a known good backup or rebuild may be the only reliable way to ensure that malicious code can be truly eradicated.

Security Control: 0917; Revision: 7; Updated: Oct-19; Applicability: O, P, S, TS
When malicious code is detected, the following steps are taken to handle the infection:

- *the infected systems are isolated*

- *all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary*
- *antivirus software is used to remove the infection from infected systems and media*
- *if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.*

Allowing targeted cyber intrusions to continue

When a targeted cyber intrusion is detected, organisations may wish to allow the intrusion to continue for a short period of time in order to understand its extent. Organisations allowing a targeted cyber intrusion to continue on a system should establish with their legal advisors whether the actions are breaching the ***Telecommunications (Interception and Access) Act 1979***.

Security Control: 0137; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Legal advice is sought before allowing targeted cyber intrusion activity to continue on a system for the purpose of collecting further information or evidence.

Security Control: 1609; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
System owners are consulted before allowing targeted cyber intrusion activity to continue on a system for the purpose of collecting further information or evidence.

Post-incident analysis

Post-incident analysis after a targeted cyber intrusion can assist in determining whether an adversary has been removed from a system. This can be achieved, in part, by conducting a full network traffic capture for at least seven days. Organisations should then be able to identify anomalous behaviour that may indicate whether the adversary has persisted on the system or not.

Security Control: 1213; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Post-incident analysis is performed for successful targeted cyber intrusions; this includes storing full network traffic for at least seven days after a targeted cyber intrusion.

Integrity of evidence

When gathering evidence following any form of cyber security incident, it is important that its integrity is maintained. Even though an investigation may not directly lead to a law enforcement agency prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

If the Australian Cyber Security Centre (ACSC) is requested to assist in investigations, the ACSC requests that no actions which could affect the integrity of evidence be carried out before the ACSC becomes involved.

Security Control: 0138; Revision: 4; Updated: Aug-20; Applicability: O, P, S, TS
The integrity of evidence gathered during an investigation is maintained by investigators:

- *recording all of their actions*
- *creating checksums for all evidence*
- *copying evidence onto media for archiving*
- *maintaining a proper chain of custody.*

Further information

Further information on incident response plans can be found in the system-specific security documentation section of the ***Guidelines for Security Documentation***.

Further information on event logging, including retention periods, can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Further information on handling and managing data spills can be found in the ACSC's ***Data Spill Management Guide*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/data-spill-management-guide.

Further information on responding to cyber security incidents can be found in the ACSC's ***Preparing for and Responding to Cyber Security Incidents*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/preparing-and-responding-cyber-security-incidents.

Reporting cyber security incidents

Reporting cyber security incidents

Reporting cyber security incidents, including unplanned outages, to an organisation's Chief Information Security Officer (CISO), or one of their delegates, as soon as possible after they occur or are discovered provides senior management with the opportunity to assess damage to systems and their organisation, and to take remedial action if necessary, including seeking advice from the ACSC.

Security Control: 0123; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Cyber security incidents are reported to an organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.

Security Control: 0141; Revision: 4; Updated: Jul-20; Applicability: O, P, S, TS
Service providers report all cyber security incidents to the organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.

Security Control: 1433; Revision: 2; Updated: Jul-20; Applicability: O, P, S, TS
Organisations and service providers maintain 24x7 contact details for each other in order to report cyber security incidents.

Security Control: 1434; Revision: 2; Updated: Jul-20; Applicability: O, P, S, TS
Organisations and service providers provide each other with additional out-of-band contact details for use when normal communication channels fail.

Reporting cyber security incidents to the ACSC

The ACSC uses the cyber security incident reports it receives as the basis for providing assistance to organisations. Cyber security incident reports are also used by the ACSC to identify trends and maintain an accurate threat environment picture. The ACSC utilises this understanding to assist in the development of new or updated cyber security advice, capabilities and techniques to better prevent and respond to evolving cyber threats. Organisations are recommended to internally coordinate their reporting of cyber security incidents to the ACSC.

Security Control: 0140; Revision: 6; Updated: May-19; Applicability: O, P, S, TS
Cyber security incidents are reported to the ACSC.

Further information

Further information on reporting cyber security incidents to the ACSC is available at https://www.cyber.gov.au/acsc/report.

Guidelines for Outsourcing

Information technology and cloud services

Information technology services

Information technology services encompass business process services, application processes and infrastructure services. The range of information technology services that can be outsourced is extensive.

Cloud services

The terminology and definitions used in this section for cloud services are consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, ***The NIST Definition of Cloud Computing***. This section also applies to cloud services that have a payment model which differs to the NIST pay-per-use measured service characteristic.

Cyber supply chain risk management

As part of cyber supply chain risk management activities, organisations should consider the security risks that may arise as systems, software and hardware are being designed, built, stored, delivered, installed, operated, maintained or decommissioned. This includes identifying and managing jurisdictional, governance, privacy and security risks associated with the use of suppliers and service providers. For example, outsourced information technology or cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge. Additionally, use of offshore services introduces jurisdictional risks as foreign countries' laws could change with little warning. Finally, foreign owned service providers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers.

Furthermore, during the earliest possible stage of procurement processes, organisations should consider the security risks that a particular supplier or service provider may introduce to their systems. In doing so, it is important that organisations preference suppliers and service providers that have demonstrated a commitment to secure-by-design practices and have a strong track record of transparency and maintaining the security of their own systems, services and cyber supply chains. Finally, in some cases, a shared responsibly model which clearly defines the responsibilities of suppliers, service providers and their customers can be highly beneficial.

Security Control: 1631; Revision: 0; Updated: Dec-20; Applicability: O, P, S, TS
Components and services relevant to the security of systems are identified and understood.

Security Control: 1452; Revision: 3; Updated: Dec-20; Applicability: O, P, S, TS
Before obtaining components and services relevant to the security of systems, a review of suppliers and service providers (including their country of origin) is performed to assess the potential increase to systems' security risk profile, including by identifying those that are high risk.

Security Control: 1567; Revision: 1; Updated: Dec-20; Applicability: O, P, S, TS
Suppliers and service providers identified as high risk are not used.

Security Control: 1568; Revision: 1; Updated: Dec-20; Applicability: O, P, S, TS
Components and services relevant to the security of systems are chosen from suppliers and service providers that have made a commitment to secure-by-design practices.

Security Control: 1632; Revision: 0; Updated: Dec-20; Applicability: O, P, S, TS
Components and services relevant to the security of systems are chosen from suppliers and service providers that have a strong track record of transparency and maintaining the security of their own systems, services and cyber supply chains.

Security Control: 1569; Revision: 1; Updated: Dec-20; Applicability: O, P, S, TS
A shared responsibility model is created, documented and shared between suppliers, service providers and their customers in order to articulate the security responsibilities of each party.

Outsourced gateway services

Commercial and government gateway services selected by the Australian Cyber Security Centre (ACSC) will need to undergo regular security assessments to determine their security posture and security risks associated with their use.

Security Control: 0100; Revision: 10; Updated: Jul-20; Applicability: O, P
Commercial and government gateway services selected by the ACSC undergo a joint security assessment by ACSC and Information Security Registered Assessors Program (IRAP) assessors at least every 24 months.

Outsourced cloud services

Outsourcing can be a cost-effective option for providing cloud services, as well as potentially delivering a superior service; however, it can also affect an organisation's security risk profile. Ultimately, organisations will still need to decide whether a particular outsourced cloud service represents an acceptable risk and, if appropriate to do so, authorise it for their own use.

Cloud service providers and their cloud services will need to undergo regular security assessments to determine their security posture and security risks associated with their use. Following an initial security assessment, subsequent security assessments should focus on any new cloud services that are being offered as well as any security-related changes that have occurred since the previous security assessment.

Security Control: 1637; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
An outsourced cloud services register is maintained and regularly audited.

Security Control: 1638; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
Outsourced cloud services registers contain the following for each outsourced cloud service:

- *cloud service provider's name*
- *cloud service's name*
- *purpose for using the cloud service*
- *sensitivity or classification of information involved*
- *due date for the next security assessment of the cloud service*
- *point of contact for users of the cloud service*
- *point of contact for the cloud service provider.*

Security Control: 1570; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
Cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.

Security Control: 1529; Revision: 1; Updated: Jul-20; Applicability: S, TS
Only community or private clouds are used for outsourced cloud services.

Contractual security requirements

Obligations for protecting the confidentiality, integrity and availability of information are no different when using an outsourced information technology or cloud service than using an in-house service. As such, contractual arrangements between an organisation and a service provider should address how security risks will be managed. However, in some cases an organisation may require information technology or cloud services to be used before all security requirements

have been implemented by the service provider. In such cases, contractual arrangements should include appropriate timeframes for the implementation of security requirements and break clauses if these are not achieved.

In addition, although information ownership resides with an organisation, this can become less clear in some circumstances, such as when legal action is taken and a service provider is asked to provide access to, or information from, their assets. To mitigate the likelihood of information being unavailable or compromised, organisations can document the types of information and its ownership through contractual arrangements.

Furthermore, organisations may make the decision to move from their current service provider for strategic, operational or governance reasons. This may include scenarios such as changing to another service provider, moving to a different service with the same service provider or moving back to an on-premises solution. In many cases, transferring information and functionality between old and new services or systems will be desired. Service providers can assist organisations by ensuring information is as portable as possible and that as much information can be exported as possible. As such, information should be stored in a documented format, preferably an open standard, noting that undocumented or proprietary formats may make it more difficult for organisations to perform backup, service migration or service decommissioning activities.

Finally, to ensure that organisations are given sufficient time to download their information or move to another service provider should a service provider cease offering a particular service, a one month notification period should be documented in contractual arrangements.

Security Control: 1395; Revision: 4; Updated: Jul-20; Applicability: O, P, S, TS
Service providers provide an appropriate level of protection for any official, sensitive or classified information entrusted to them or their services.

Security Control: 0072; Revision: 6; Updated: Jul-20; Applicability: O, P, S, TS
Security requirements associated with the confidentiality, integrity and availability of information entrusted to a service provider are documented in contractual arrangements.

Security Control: 1571; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
The right to audit security controls associated with the protection of information and services is specified in contractual arrangements.

Security Control: 1451; Revision: 2; Updated: Jul-20; Applicability: O, P, S, TS
Types of information and its ownership is documented in contractual arrangements.

Security Control: 1572; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
The regions or availability zones where information will be processed, stored and communicated is documented in contractual arrangements.

Security Control: 1573; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
Access to all logs relating to an organisation's information and services are specified in contractual arrangements.

Security Control: 1574; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
Information entrusted to a service provider is stored in a portable manner that allows organisations to perform backups, service migration or service decommissioning without any loss of information.

Security Control: 1575; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements.

Access to systems and information by service providers

To perform their contracted duties, service providers may need to access an organisation's systems and information. However, without proper security controls in place, this access could leave organisations' systems vulnerable – especially when such access occurs from outside of Australian borders. As such, organisations should ensure that their systems and information are not accessed or administered by service providers unless such requirements, and

associated measures to control such requirements, are documented in contractual arrangements. In doing so, it is important that sufficient measures are also in place to detect and record any unauthorised access, such as customer support representatives or platform engineers accessing an organisation's encryption keys. In such cases, the service provide should immediately report the cyber security incident to organisations and make available all logs pertaining to the unauthorised access.

Security Control: 1073; Revision: 4; Updated: Jul-20; Applicability: O, P, S, TS
An organisation's systems and information are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

Security Control: 1576; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
If an organisation's systems or information are accessed or administered by a service provider in an unauthorised manner, organisations are immediately notified.

Further information

Further information on the definition of cloud computing can be found in NIST SP 800-145, ***The NIST Definition of Cloud Computing***, at https://csrc.nist.gov/publications/detail/sp/800-145/final.

The ACSC's list of certified gateways is available at https://www.cyber.gov.au/acsc/view-all-content/programs/irap/asd-certified-gateways.

The ACSC's guidance on conducting security assessments for cloud service providers and their cloud services is available at https://www.cyber.gov.au/acsc/government/cloud-security-guidance.

The whole-of-government policy on secure cloud computing can be found in the Digital Transformation Agency's ***Secure Cloud Strategy*** publication at https://www.dta.gov.au/our-projects/secure-cloud-strategy.

Further information on outsourced information technology and cloud services can be found in the Attorney-General's Department's ***Protective Security Policy Framework***, ***Security governance for contracted goods and service providers*** policy, at https://www.protectivesecurity.gov.au/governance/security-governance-for-contracted-service-providers/Pages/default.aspx.

Further information on the ACSC's Managed Service Provider Partner Program can be found at https://www.cyber.gov.au/acsc/view-all-content/programs/msp-partner-program-msp3.

Further information on cyber supply chain risk management can be found in the ACSC's ***Cyber Supply Chain Risk Management*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management and the ***Identifying Cyber Supply Chain Risks*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/identifying-cyber-supply-chain-risks.

Further information on supply chain integrity can be found in NIST SP 800-161, ***Supply Chain Risk Management Practices for Federal Information Systems and Organizations***, at https://csrc.nist.gov/publications/detail/sp/800-161/final.

Guidelines for Security Documentation

Development and maintenance of security documentation

Cyber security strategy

A cyber security strategy sets out an organisation's guiding principles, objectives and priorities for cyber security, typically over a three to five year period. In addition, a cyber security strategy may also cover an organisation's threat environment, cyber security initiatives (an action plan) or investments the organisation plans to make as part of its cyber security program. Without a cyber security strategy, organisations risk failing to adequately plan for and manage security and business risks within their organisation.

Security Control: 0039; Revision: 4; Updated: May-19; Applicability: O, P, S, TS
A cyber security strategy is developed and implemented for the organisation.

Approval of security documentation

If security documentation is not approved, personnel will have difficulty ensuring appropriate policies, processes and procedures are in place. Having approval not only assists in the implementation of policies, processes and procedures, it also ensures personnel are aware of cyber security issues and security risks.

Security Control: 0047; Revision: 4; Updated: May-19; Applicability: O, P, S, TS
Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system's authorising officer.

Maintenance of security documentation

Threat environments are dynamic. If security documentation is not kept up-to-date to reflect the current threat environment, security controls and processes may cease to be effective. In such a situation, resources could be devoted to areas that have reduced effectiveness or are no longer relevant.

Security Control: 0888; Revision: 5; Updated: May-19; Applicability: O, P, S, TS
Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Communication of security documentation

It is important that once security documentation has been approved, either initially or following any changes, it is published and communicated to all stakeholders. If security documentation is not communicated to stakeholders they will be unaware of what policies and procedures have been implemented for systems and their use.

Security Control: 1602; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Security documentation, including notification of subsequent changes, is communicated to all stakeholders.

Further information

Further information on intrusion detection and prevent policy can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on cyber security incident registers can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on ICT equipment and media registers can be found in the ***Guidelines for Physical Security***.

Further information on authorised Radio Frequency devices for SECRET and TOP SECRET area registers can be found in the ***Guidelines for Physical Security***.

Further information on cable registers can be found in the ***Guidelines for Communications Infrastructure***.

Further information on cable labelling process and procedures can be found in the ***Guidelines for Communications Infrastructure***.

Further information on telephone systems usage policy can be found in the ***Guidelines for Communications Systems***.

Further information on fax machine and multifunction device usage policy can be found in the ***Guidelines for Communications Systems***.

Further information on mobile device management policy and mobile device usage policy, as well as mobile device emergency sanitisation process and procedures, can be found in the ***Guidelines for Enterprise Mobility***.

Further information on ICT equipment management policy, as well as ICT equipment sanitisation and disposal processes and procedures, can be found in the ***Guidelines for ICT Equipment***.

Further information on media management policy and removable media usage policy, as well as media sanitisation, destruction and disposal processes and procedures, can be found in the ***Guidelines for Media***.

Further information on system administration process and procedures can be found in the ***Guidelines for System Management***.

Further information on patch management process and procedures can be found in the ***Guidelines for System Management***.

Further information on software registers can be found in the ***Guidelines for System Management***.

Further information on change management process and procedures can be found in the ***Guidelines for System Management***.

Further information on digital preservation policy, as well as data backup and restoration processes and procedures, can be found in the ***Guidelines for System Management***.

Further information on event logging policy, as well as event log auditing process and procedures, can be found in the ***Guidelines for System Monitoring***.

Further information on database registers can be found in the ***Guidelines for Database Systems***.

Further information on email usage policy can be found in the ***Guidelines for Email***.

Further information on network device registers can be found in the ***Guidelines for Networking***.

Further information on web usage policy can be found in the ***Guidelines for Gateways***.

Further information on data transfer process and procedures can be found in the ***Guidelines for Data Transfers***.

System-specific security documentation

System-specific security documentation

System-specific security documentation, such as the system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones, support the accurate and consistent application of policies, processes and procedures for systems. As such, it is important that they are developed by personnel with a good understanding of security matters, the technologies being used and the business requirements of the organisation.

System-specific security documentation may be presented in a number of formats including dynamic content such as wikis, intranets or other forms of document repositories. Furthermore, depending on the documentation framework used, details common to multiple systems could be consolidated into higher level security documentation.

System security plan

The system security plan provides a description of a system and includes an annex that describes the security controls that have been identified and implemented for the system.

There can be many stakeholders involved in defining a system security plan. This can include representatives from:

- cyber security teams within the organisation
- project teams who deliver the capability (including contractors)
- support teams who operate and support the capability
- owners of information to be processed, stored or communicated by the system
- users for whom the capability is being developed.

Security Control: 0041; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
Systems have a system security plan that includes a description of the system and an annex that covers both security controls from this document (based on the system's classification, functionality and technologies) and any additional security controls that have been identified for the system.

Incident response plan

Having an incident response plan 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 prevent the cyber security incident from escalating, restore any impacted system or information, and preserve any evidence.

Security Control: 0043; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Systems have an incident response plan that covers the following:

- *guidelines on what constitutes a cyber security incident*
- *the types of incidents likely to be encountered and the expected response to each type*
- *how to report cyber security incidents, internally to the organisation and externally to the Australian Cyber Security Centre (ACSC)*
- *other parties which need to be informed in the event of a cyber security incident*
- *the authority, or authorities, responsible for investigating and responding to cyber security incidents*
- *the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency, the ACSC or other relevant authority*
- *the steps necessary to ensure the integrity of evidence relating to a cyber security incident*
- *system contingency measures or a reference to such details if they are located in a separate document.*

Continuous monitoring plan

A continuous monitoring plan can assist organisations in proactively identifying, prioritising and responding to security vulnerabilities. Measures to monitor and manage security vulnerabilities in systems can also provide organisations with a wealth of valuable information about their exposure to cyber threats, as well as assisting them to determine security risks associated with the operation of their systems. Undertaking continuous monitoring activities is important as cyber threats and the effectiveness of security controls will change over time.

Three types of continuous monitoring activities are vulnerability assessments, vulnerability scans and penetration tests. A vulnerability assessment typically consists of a review of a system's architecture or an in-depth hands-on assessment while a vulnerability scan involves using software tools to conduct automated scans. In each case, the goal is to identify

as many security vulnerabilities as possible. A penetration test however is designed to exercise real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical system components or information. Regardless of the continuous monitoring activities chosen, they should be conducted by suitably skilled personnel independent of the system being assessed. Such personnel can be internal to an organisation or a third party. This ensures that there is no conflict of interest, perceived or otherwise, and that the activities are undertaken in an objective manner.

Security Control: 1163; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
Systems have a continuous monitoring plan that includes:

- *conducting vulnerability scans for systems at least monthly*
- *conducting vulnerability assessments or penetration tests for systems at least annually*
- *analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls*
- *using a risk-based approach to prioritise the implementation of identified mitigations.*

Security assessment report

At the conclusion of a security assessment for a system, a security assessment report should be produced by the assessor. This will assist the system owner in performing any initial remediation actions as well as guiding the development of the system's plan of action and milestones.

Security Control: 1563; Revision: 0; Updated: May-20; Applicability: O, P, S, TS
At the conclusion of a security assessment for a system, a security assessment report is produced by the assessor and covers:

- *the scope of the security assessment*
- *the system's strengths and weaknesses*
- *security risks associated with the operation of the system*
- *the effectiveness of the implementation of security controls*
- *any recommended remediation actions.*

Plan of action and milestones

At the conclusion of a security assessment for a system, and the production of a security assessment report by the assessor, a plan of action and milestones should be produced by the system owner. This will assist with tracking any of the system's identified weaknesses and recommended remediation actions following the security assessment.

Security Control: 1564; Revision: 0; Updated: May-20; Applicability: O, P, S, TS
At the conclusion of a security assessment for a system, a plan of action and milestones is produced by the system owner.

Guidelines for Physical Security

Facilities and systems

Certification and accreditation authorities

Information on the certification and accreditation authorities for physical security are outlined in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Entity facilities*** policy.

Facilities containing systems

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 a facility.

Deployable platforms should meet physical security requirements as per any other system. Notably, physical security certification authorities dealing with deployable platforms may have specific requirements that supersede the security controls in these guidelines. As such, personnel should contact their 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.

Security Control: 0810; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Any facility containing a system, including a deployable system, is certified and accredited to at least the sensitivity or classification of the system.

Server rooms, communications rooms and security containers

The second layer in the protection of systems is the use of a higher Security Zone or secure room for a server room or communications room while the final layer is the use of lockable commercial cabinets or security containers. All layers are designed to limit access to people without the appropriate authorisation to access systems at a facility.

Security Control: 1053; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Servers and network devices are secured in server rooms or communications rooms that meet the requirements for a Security Zone or secure room suitable for their sensitivity or classification.

Security Control: 1530; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Servers and network devices are secured in lockable commercial cabinets or security containers suitable for their sensitivity or classification taking into account protection afforded by the Security Zone or secure room they reside in.

Security Control: 0813; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Server rooms, communications rooms and security containers are not left in unsecured states.

Security Control: 1074; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

Network infrastructure

While physical security can provide a degree of protection to information communicated over network infrastructure, organisations can have reduced control over information when it is communicated over network infrastructure in areas not authorised for the processing of such information. For this reason, it is important that information communicated over network infrastructure outside of areas in which it is authorised to be processed is appropriately encrypted.

Security Control: 0157; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Information communicated over network infrastructure in areas not authorised for the processing of such information is encrypted as if it was communicated through unsecured spaces.

Controlling physical access to network devices

Adequate physical protection should be provided to network devices, especially those in public areas, to prevent an adversary physically damaging a network device with the intention of interrupting services.

Physical access to network devices can also allow an adversary to reset devices to factory default settings by pressing a physical reset button, connecting a serial interface to a device or connecting directly to a device to bypass any access controls. Resetting a network device 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.

Security Control: 1296; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Physical security controls are implemented to protect network devices, especially those in public areas, from physical damage or unauthorised access.

Preventing observation by unauthorised people

The inside of facilities without sufficient perimeter security are often exposed to observation through windows. Ensuring systems and information are not visible through windows will assist in reducing this security risk. This can be achieved by using blinds or curtains on windows.

Security Control: 0164; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Unauthorised people are prevented from observing systems, in particular, workstation displays and keyboards.

Further information

Further information on encryption can be found in the ***Guidelines for Cryptography***.

Further information on physical security for Security Zones, secure rooms and security containers can be found in AGD's PSPF, ***Entity facilities*** policy, at https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx.

ICT equipment and media

ICT equipment and media register

Maintaining and regularly auditing a register of authorised ICT equipment and media can assist organisations in both tracking legitimate assets and determining whether unauthorised assets have been introduced into a system or its operating environment.

Security Control: 0336; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment and media register is maintained and regularly audited.

Security Control: 0159; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
All ICT equipment and media are accounted for on a regular basis.

Securing ICT equipment and media

ICT equipment and media needs to be secured when not in use. This can be achieved by implementing one of the following approaches:

- securing ICT equipment and media in an appropriate security container or secure room
- using ICT equipment without hard drives and sanitising memory at shut down
- encrypting hard drives of ICT equipment and sanitising memory at shut down
- sanitising memory of ICT equipment at shut down and removing and securing any hard drives.

If none of the above approaches are feasible, organisation may wish to minimise the potential impact of not securing ICT equipment when not in use. This can be achieved by preventing sensitive or classified information from being stored on hard drives (e.g. by storing user profiles and documents on network shares), removing temporary user data at logoff, scrubbing virtual memory at shut down, and sanitising memory at shut down. It should be noted though that there is no guarantee that such measures will always work effectively or will not be bypassed due to circumstances such as an unexpected loss of power. Therefore, hard drives in such cases will retain their sensitivity or classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal.

Security Control: 0161; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
ICT equipment and media are secured when not in use.

Further information

Further information on ICT equipment and media can be found in the fax machines and multifunction devices section of the ***Guidelines for Communications Systems*** as well as in the ***Guidelines for ICT Equipment*** and ***Guidelines for Media***.

Further information on the encryption of media can be found in the ***Guidelines for Cryptography***.

Further information on the storage of ICT equipment can be found in AGD's PSPF, ***Physical security for entity resources*** policy, at https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx.

Wireless devices and Radio Frequency transmitters

Radio Frequency devices

Many RF devices, such as mobile devices, can pose a security risk to organisations when they are capable of picking up and recording or transmitting background conversations. In highly classified environments, it is important that organisations understand the security risks associated with the introduction of RF devices and should maintain a register of those that have been authorised for use in such environments.

Security Control: 1543; Revision: 1; Updated: Aug-19; Applicability: S, TS
An authorised RF devices for SECRET and TOP SECRET areas register is maintained and regularly audited.

Security Control: 0225; Revision: 2; Updated: Sep-18; Applicability: S, TS
Unauthorised RF devices are not brought into SECRET and TOP SECRET areas.

Security Control: 0829; Revision: 4; Updated: Mar-19; Applicability: S, TS
Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.

Bluetooth and wireless keyboards

While there have been a number of revisions to the Bluetooth protocol that have made incremental improvements to its security over time, there have also been trade-offs that have limited these improvements, such as maintaining backward compatibility with earlier versions of the protocol. While newer versions of the Bluetooth protocol have addressed many of its historical weaknesses, it still provides inadequate security for the communication of sensitive or classified information. As such, sensitive or classification information communicated using Bluetooth will need to be limited to within RF screened buildings.

Security Control: 1058; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Bluetooth and wireless keyboards are not used unless in an RF screened building.

Infrared keyboards

When using infrared keyboards with 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.

Security Control: 0222; Revision: 2; Updated: Sep-18; Applicability: O, P
When using infrared keyboards, infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.

Security Control: 0223; Revision: 4; Updated: Sep-18; Applicability: S
When using infrared keyboards, the following activities are prevented:

- *line of sight and reflected communications travelling into unsecured spaces*
- *multiple infrared keyboards for different systems being used in the same area*
- *other infrared devices being used in the same area*
- *infrared keyboards operating in areas with unprotected windows.*

Security Control: 0224; Revision: 4; Updated: Sep-18; Applicability: TS
When using infrared keyboards, the following activities are prevented:

- *line of sight and reflected communications travelling into unsecured spaces*
- *multiple infrared keyboards for different systems being used in the same area*
- *other infrared devices being used in the same area*
- *infrared keyboards operating in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.*

Wireless RF pointing devices

As many wireless RF pointing devices used Bluetooth, they along with other wireless RF pointing devices can pose an unacceptable emanation security risk, unless used in an RF screened building.

Security Control: 0221; Revision: 2; Updated: Sep-18; Applicability: TS
Wireless RF pointing devices are not used in TOP SECRET areas unless used in an RF screened building.

Further information

Further information on the use of mobile devices can be found in the ***Guidelines for Enterprise Mobility***.

Further information on the use of Bluetooth devices with mobile devices can be found in the mobile device management section of the ***Guidelines for Enterprise Mobility***.

Further information on wireless networks can be found in the wireless networks section of the ***Guidelines for Networking***.

Guidelines for Personnel Security

Cyber security awareness training

Providing cyber security awareness training

Organisations should ensure that ongoing cyber security awareness training is provided to all personnel in order to assist them in understanding their security responsibilities. The content of cyber security awareness training will depend on the objectives of the organisation; however, personnel with responsibilities beyond that of a standard user will require tailored content to meet their needs.

Security Control: 0252; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
Cyber security awareness training is undertaken annually by all personnel and covers:

- *the purpose of the cyber security awareness training*
- *security appointments and contacts within the organisation*
- *authorised use of systems and their resources*
- *protection of systems and their resources*
- *reporting of cyber security incidents and suspected compromises of systems and their resources.*

Security Control: 1565; Revision: 0; Updated: Jun-20; Applicability: O, P, S, TS
Tailored privileged user training is undertaken annually by all privileged users.

Reporting suspicious contact via online services

Online services such as email, internet forums, instant messaging apps and direct messaging on social media can all be used by an adversary in an attempt to elicit information from personnel. As such, personnel should be advised of what constitutes suspicious contact via online services and how to report it.

Security Control: 0817; Revision: 4; Updated: Jan-20; Applicability: O, P, S, TS
Personnel are advised of what suspicious contact via online services is and how to report it.

Posting work information to online services

Personnel should be advised to take special care not to post work information to online services unless authorised to do so, especially in internet forums and on social media. Even information that appears to be benign in isolation could, along with other information, have a considerable security impact. In addition, to ensure that personal opinions of individuals are not interpreted as official policy, personnel should be advised to maintain separate work and personal accounts for online services, especially when using social media.

Security Control: 0820; Revision: 5; Updated: Jan-20; Applicability: O, P, S, TS
Personnel are advised to not post work information to unauthorised online services and to report cases where such information is posted.

Security Control: 1146; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Personnel are advised to maintain separate work and personal accounts for online services.

Posting personal information to online services

Personnel should be advised that any personal information they post to online services, such as social media, could be used by an adversary to develop a detailed profile of their lifestyle in order to build a relationship with them. This

relationship could then be used to attempt to elicit information or influence them to undertake specific actions, such as opening malicious emails or visiting malicious websites. Furthermore, encouraging personnel to use the privacy settings of online services can minimise who can view their information and interactions on such services.

Security Control: 0821; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.

Sending and receiving files via online services

When personnel send and receive files via online services, such as instant messaging apps and social media, they often bypass security controls put in place to detect and quarantine malicious code. Advising personnel to only send and receive files via authorised online services will ensure files are appropriately protected and scanned for malicious code.

Security Control: 0824; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Personnel are advised not to send or receive files via unauthorised online services.

Further information

Further information on email usage policy can be found in the email usage section of the ***Guidelines for Email***.

Further information on web usage policies can be found in the web proxies section of the ***Guidelines for Gateways***.

Further information on detecting socially engineered messages be found in the Australian Cyber Security Centre (ACSC)'s ***Detecting Socially Engineered Messages*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/detecting-socially-engineered-messages.

Further information on the use of social media can be found in the ACSC's ***Security Tips for Social Media and Social Networking Apps*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-social-media-and-social-networking-apps.

Further information on the sanitisation of documents before posting them to authorised online services can be found in the ACSC's ***An Examination of the Redaction Functionality of Adobe Acrobat Pro DC 2017*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/examination-redaction-functionality-adobe-acrobat-pro-dc-2017.

Access to systems and their resources

Security clearances

Where these guidelines refer to security clearances, it applies to Australian security clearances or security clearances from a foreign government which are formally recognised by Australia.

System access requirements

Ensuring that the requirements for access to systems and their resources are documented and agreed upon helps determine if personnel have the appropriate authorisations, security clearances and need-to-know to access a system and its resources. Types of users for which access requirements should be documented include standard users, privileged users, foreign users and contractors.

Security Control: 0432; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
Each system's system security plan specifies any requirements for access to the system and its resources.

Security Control: 0434; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS
Personnel undergo appropriate employment screening, and where necessary hold an appropriate security clearance, before being granted access to a system and its resources.

Security Control: 0435; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
Personnel receive any necessary briefings before being granted access to a system and its resources.

User identification

Having uniquely identifiable users ensures accountability for access to systems and their resources. Furthermore, where systems process, store or communicate Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) information, and foreign nationals have access to such systems, it is important that foreign nationals are identified as such.

Security Control: 0414; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
Personnel granted access to a system and its resources are uniquely identifiable.

Security Control: 0415; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

Security Control: 1583; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Personnel who are contractors are identified as such.

Security Control: 0975; Revision: 7; Updated: Aug-19; Applicability: O, P, S, TS
Personnel who are foreign nationals are identified as such, including by their specific nationality.

Security Control: 0420; Revision: 9; Updated: Sep-20; Applicability: S, TS
Where systems process, store or communicate AUSTEO, AGAO or REL information, personnel who are foreign nationals are identified as such, including by their specific nationality.

Standard access to systems

Personnel seeking access to systems, applications and data repositories should have a genuine business requirement verified by their manager. Once a requirement to access a system is established, personnel should be given only the privileges that they need to undertake their duties.

Security Control: 0405; Revision: 5; Updated: Sep-19; Applicability: O, P, S, TS
Standard access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1503; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Standard access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

Security Control: 1566; Revision: 0; Updated: Jun-20; Applicability: O, P, S, TS
The use of standard accounts, and any activities undertaken with them, are monitored and audited.

Standard access to systems by foreign nationals

Due to the extra sensitivities associated with AUSTEO, AGAO and REL information, foreign access to such information is strictly controlled.

Security Control: 0409; Revision: 6; Updated: Sep-20; Applicability: S, TS
Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO or REL information unless effective security controls are in place to ensure such information is not accessible to them.

Security Control: 0411; Revision: 5; Updated: Aug-19; Applicability: S, TS
Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO information unless effective security controls are in place to ensure such information is not accessible to them.

Privileged access to systems

Privileged users are considered to be those which can alter or circumvent a system's security measures. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security measures. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.

Privileged users are often targeted by adversaries as they can potentially give full access to systems. As such, ensuring that privileged users do not have the ability to read emails, browse the web or obtain files via online services, such as instant messaging or social media, minimises opportunities for their accounts to be compromised.

Security Control: 1507; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1508; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

Security Control: 0445; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.

Security Control: 1509; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The use of privileged accounts, and any activities undertaken with them, are monitored and audited.

Security Control: 1175; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Privileged access to systems by foreign nationals

As privileged accounts often have the ability to bypass security controls on a system, it is strongly encouraged that foreign nationals are not given privileged access to systems, particularly those that process, store or communicate AUSTEO, AGAO or REL information.

Security Control: 0448; Revision: 6; Updated: Sep-19; Applicability: O, P, S, TS
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems, applications and data repositories.

Security Control: 0446; Revision: 4; Updated: Sep-20; Applicability: S, TS
Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO or REL information.

Security Control: 0447; Revision: 3; Updated: Aug-19; Applicability: S, TS
Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO information.

Suspension of access to systems

Removing or suspending access to systems, applications and data repositories can prevent them from being accessed when there is no longer a legitimate business requirement for their use, such as when personnel change duties, leave the organisation or are detected undertaking malicious activities.

Security Control: 0430; Revision: 7; Updated: Sep-19; Applicability: O, P, S, TS
Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.

Security Control: 1591; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Access to systems, applications and data repositories is removed or suspended as soon as practicable when personnel are detected undertaking malicious activities.

Security Control: 1404; Revision: 2; Updated: Sep-19; Applicability: O, P, S, TS
Access to systems, applications and data repositories is removed or suspended after one month of inactivity.

Recording authorisation for personnel to access systems

Retaining records of system account requests will assist in maintaining personnel accountability. This is needed 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 last reviewed.

Security Control: 0407; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
A secure record is maintained for the life of each system covering:

- *all personnel authorised to access the system, and their user identification*
- *who provided authorisation for access*
- *when access was granted*
- *the level of access that was granted*
- *when access, and the level of access, was last reviewed*
- *when the level of access was changed, and to what extent (if applicable)*
- *when access was withdrawn (if applicable).*

Temporary access to systems

Under strict circumstances, temporary access to systems, applications or data repositories may be granted to personnel who lack an appropriate security clearance or briefings. In such circumstances, personnel should have their access controlled in such a way that they only have access to information they require to undertake their duties.

Security Control: 0441; Revision: 6; Updated: Sep-19; Applicability: O, P, S, TS
When personnel are granted temporary access to a system, effective security controls are put in place to restrict their access to only information required for them to undertake their duties.

Security Control: 0443; Revision: 3; Updated: Sep-18; Applicability: S, TS
Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.

Emergency access to systems

It is important that organisations do not lose access to systems. As such, organisations should always have a method for gaining access during emergencies. Typically, such emergencies would occur where access to systems cannot be gained via normal authentication processes (e.g. due to misconfigurations of authentication services, misconfigurations of security settings or due to a cyber security incident). In these situations, a break glass account (also known as an emergency access account) can be used to gain access. As break glass accounts generally have the highest level of privileges available for systems, extreme care should be taken to both protect them and to monitor for any signs of compromise or abuse.

When break glass accounts are used, actions undertaken will not be directly attributable to an individual, and systems may not generate audit logs. As such, additional activities need to be taken in order to ensure a system's integrity. In doing so, organisations should ensure that configuration changes made using a break glass account are identified and documented using configuration management processes. This includes documenting the individual using the break

glass account, the reason for using the break glass account and the reason for any configuration changes made to a system.

As the custodian of each break glass account should be the only party who knows the account's credentials, credentials will need to be changed and tested by custodians after the authorised access by another party. Modern password managers that support automated credential changes and testing can assist in reducing the administrative overheads of such activities.

Security Control: 1610; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
A method of emergency access to systems is documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Security Control: 1611; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are only used when normal authentication processes cannot be used.

Security Control: 1612; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are only used for specific authorised activities.

Security Control: 1613; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are monitored and audited for unauthorised use or modification.

Security Control: 1614; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass account credentials are changed by the account custodian after they are accessed by any other party.

Security Control: 1615; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Break glass accounts are tested after credentials are changed.

Control of Australian systems

Due to extra sensitivities associated with AUSTEO and AGAO systems, it is essential that control of such systems is maintained by Australian citizens working for the Australian Government and that such systems can only be accessed from facilities under the sole control of the Australian Government.

Security Control: 0078; Revision: 4; Updated: Sep-18; Applicability: S, TS
Systems processing, storing or communicating AUSTEO or AGAO information remain at all times under the control of an Australian national working for or on behalf of the Australian Government.

Security Control: 0854; Revision: 4; Updated: Sep-18; Applicability: S, TS
Access to AUSTEO or AGAO information from systems not under the sole control of the Australian Government is prevented.

Further information

Further information on access to government resources, including temporary access, can be found in the Attorney-General's Department's ***Protective Security Policy Framework***, ***Access to information*** policy, at https://www.protectivesecurity.gov.au/information/access-to-information/Pages/default.aspx.

Guidelines for Communications Infrastructure

Cabling infrastructure

Applicability

The security controls in this section apply to new cabling infrastructure installations or upgrades. Organisations do not need to retrofit existing cabling infrastructure to align with these security controls.

This section is applicable to all domestic facilities. For deployable platforms or facilities outside of Australia, consult the emanation security section of these guidelines.

Implementation scenarios

This section provides common security controls for non-shared government facilities, shared government facilities and shared non-government facilities:

- A non-shared government facility is where the entire facility and personnel are cleared to the highest level of information processed in the facility.
- A shared government facility is where the facility and personnel are cleared at different levels.
- A shared non-government facility is where the facility is shared by government organisations and non-government organisations.

Specific security controls for any of the above scenarios will be identified as such.

Cable sheaths and conduits

A cable's protective sheath is not considered to be a conduit. However, for fibre-optic cables with subunits, the fibre-optic cable's outer protective sheath is considered to be a conduit.

Cable connector types

The same cable connector types can be used for all systems within a facility regardless of their sensitivity or classification.

Cabling infrastructure standards

Cabling infrastructure should be installed by an endorsed cable installer to the relevant Australian Standards to ensure personnel safety and system availability.

Security Control: 0181; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Cabling infrastructure is installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority.

Use of fibre-optic cables

Fibre-optic cables do not produce, nor are influenced by, electromagnetic emanations; thereby offering the highest degree of protection from electromagnetic emanation effects. Also, fibre-optic cables are more difficult to tap than copper cables.

Security Control: 1111; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Fibre-optic cables are used for cabling infrastructure instead of copper cables.

Cable register

Maintaining and regularly auditing cable registers allow installers and inspectors to trace cables for malicious or accidental changes or damage. In doing so, cable registers should track all cable management changes throughout the life of a system.

Security Control: 0211; Revision: 5; Updated: Jan-21; Applicability: O, P, S, TS
A cable register is maintained and regularly audited.

Security Control: 0208; Revision: 5; Updated: Mar-21; Applicability: O, P, S, TS
Cable registers contain the following information:

- *cable identifier*
- *cable colour*
- *sensitivity/classification*
- *source*
- *destination*
- *site/floor plan diagram*
- *seal numbers (if applicable).*

Cable labelling process and procedures

A well documented and followed cable labelling process, and supporting cable labelling procedures, makes cable auditing and fault finding easier.

Security Control: 0206; Revision: 5; Updated: Aug-19; Applicability: O, P, S, TS
A cable labelling process, and supporting cable labelling procedures, is developed and implemented.

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.

Security Control: 1096; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Labelling building management cables

All facilities will contain cabling to support building management functions, such as: security systems, fire detection systems, building management systems, audio/visual systems, operational technology sensors and lighting. As building management cables may use colours such as red for fire alarms (as per Australian Standards), it is important that such cables are appropriately labelled.

Security Control: 1639; Revision: 0; Updated: Mar-21; Applicability: O, P, S, TS
Building management cables are labelled with their purpose in black writing on a yellow background, with a minimum size of 2.5 cm x 1 cm, and attached at five-metre intervals.

Labelling cables for foreign systems in Australian facilities

Labelling cables for foreign systems in Australian facilities helps prevent unintended cross-patching of Australian and foreign systems.

Security Control: 1640; Revision: 0; Updated: Mar-21; Applicability: O, P, S, TS
Cables for foreign systems installed in Australian facilities are labelled at inspection points.

Cable colours

The use of designated cable colours can provide an easy way to distinguish highly classified systems from other systems. For example, while TOP SECRET and SECRET cables have designated colours, cables for PROTECTED and below systems may be any colour (except for those reserved for highly classified systems). In addition, cable colours for PROTECTED and below systems may be the same colour (e.g. blue).

Security Control: 0926; Revision: 8; Updated: Mar-21; Applicability: O, P, S, TS
The cable colours in the following table are used.

System	*Cable Colour*
TOP SECRET	*Red*
SECRET	*Salmon pink*
PROTECTED	*Any colour (except red or salmon pink)*
OFFICIAL	*Any colour (except red or salmon pink)*

Cable colour non-conformance

In certain circumstances it may not be possible to use the correct cable colours. Therefore, organisations should band cables with the appropriate colour and ensure that the cable bands are easily visible at inspection points. In doing so, it is important that cable bands are robust enough to 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.

Security Control: 1216; Revision: 2; Updated: Mar-21; Applicability: S, TS
Cables with non-conformant cable colouring are both banded with the appropriate colour and labelled at inspection points.

Cable inspectability

The ability to inspect cabling infrastructure is necessary to detect illicit tampering or degradation.

Security Control: 1112; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
In non-shared government facilities, cables are inspectable at a minimum of five-metre intervals.

Security Control: 1118; Revision: 1; Updated: Sep-18; Applicability: O, P, S
In non-TOP SECRET areas of shared government facilities, cables are inspectable at a minimum of five-metre intervals.

Security Control: 1119; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
In TOP SECRET areas of shared government facilities, cables are fully inspectable for their entire length.

Security Control: 1126; Revision: 1; Updated: Sep-18; Applicability: O, P, S
In non-TOP SECRET areas of shared non-government facilities, cables are inspectable at a minimum of five-metre intervals.

Security Control: 0184; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
In TOP SECRET areas of shared non-government facilities, cables are fully inspectable for their entire length.

Cable groups

Cable groups provide a method of sharing conduits and cable reticulation systems.

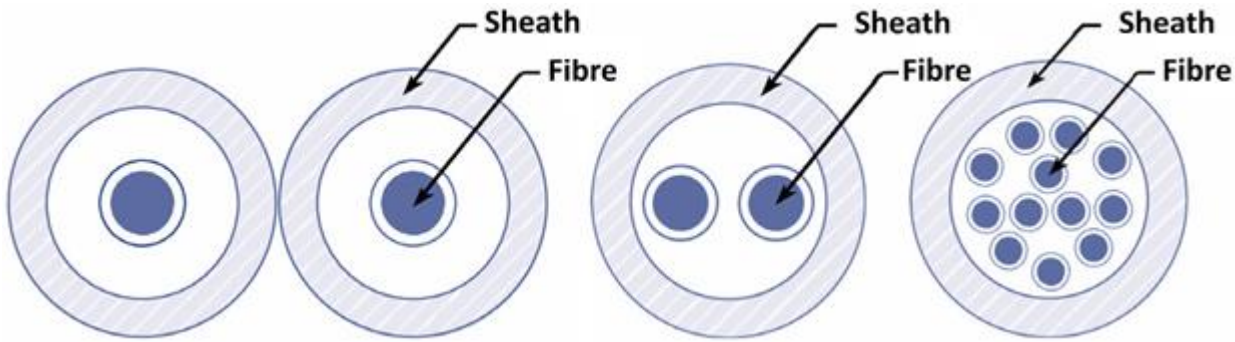
Security Control: 0187; Revision: 6; Updated: Mar-21; Applicability: O, P, S, TS
The cable groups in the following table are used.

Cable Group	*System*
1	*OFFICIAL*
	PROTECTED
2	*SECRET*
3	*TOP SECRET*

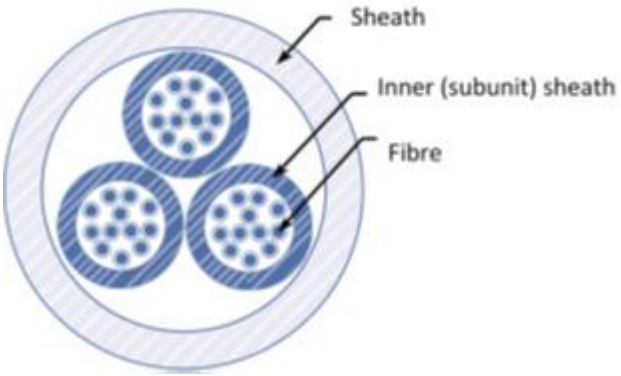
Fibre-optic cables sharing a common conduit

Fibre-optic cables of various cable groups can share a common conduit to reduce costs; however, various cable groups can't share a common sheath unless they belong to different subunits.

Security Control: 0189; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
With fibre-optic cables, the fibres in the sheath only carry a single cable group.



Security Control: 0190; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
With fibre-optic cables contains subunits, each subunit only carries a single cable group; however, each subunit can carry a different cable group.



Common cable reticulation systems

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

Security Control: 1114; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Cable groups sharing a common cable reticulation system have a dividing partition or a visible gap between the cable groups.

Enclosed cable reticulation systems

In shared non-government facilities, cables should be enclosed in a sealed cable reticulation system to prevent access and enhance cable management.

Security Control: 1130; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
In shared non-government facilities, cables are run in an enclosed cable reticulation system.

Covers for enclosed cable reticulation systems

In shared non-government facilities, clear covers on enclosed cable reticulation systems are a convenient method of maintaining inspection requirements. Having clear covers face inwards increases their inspectability.

Security Control: 1164; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
In shared non-government facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.

Sealing cable reticulation systems and conduits

In shared non-government facilities, Security Construction and Equipment Committee (SCEC) endorsed seals should be used to provide evidence of any tampering or illicit access to cable reticulation systems. In addition, conduits should be sealed with a visible smear of conduit glue to prevent access.

Security Control: 0195; Revision: 5; Updated: Mar-21; Applicability: TS
In shared non-government facilities, uniquely identifiable SCEC endorsed tamper-evident seals are used to seal all removable covers on cable reticulation systems.

Security Control: 0194; Revision: 2; Updated: Sep-18; Applicability: TS
In shared non-government facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and conduit runs connected by threaded lock nuts.

Labelling conduits

Conduit labels should be a specific size and colour to allow for easy identification.

Security Control: 0201; Revision: 3; Updated: Mar-21; Applicability: TS
Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at five-metre intervals and marked as 'TS RUN'.

Cables in walls

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

Security Control: 1115; Revision: 4; Updated: Dec-19; Applicability: O, P, S, TS
Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.

Cables in party walls

In shared non-government facilities, cables should not be run in any 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.

Security Control: 1133; Revision: 2; Updated: Mar-21; Applicability: TS
In shared non-government facilities, cables are not run in party walls.

Wall penetrations

In shared government facilities and shared non-government facilities, penetrating a wall into a lower classified space requires the integrity of the classified spaces to be maintained. As such, all cables should be encased in conduit with no gaps in the wall around the conduit.

Security Control: 1122; Revision: 1; Updated: Sep-18; Applicability: TS
In shared government facilities, where wall penetrations exit into a lower classified space, cables are encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Security Control: 1134; Revision: 1; Updated: Sep-18; Applicability: TS
In shared non-government facilities, where wall penetrations exit into a lower classified space, cables are encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Wall outlet boxes

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

Security Control: 1104; Revision: 3; Updated: Mar-21; Applicability: O, P
Wall outlet boxes have connectors on opposite sides of the wall outlet box if the cable group contains cables belonging to different classifications.

Security Control: 1105; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Different cables groups do not share a wall outlet box.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment of a lower classification to the wrong wall outlet box. In cases were a wall outbox has a cable group containing cables belonging to different classifications, each connector should be individually labelled with its classification.

Security Control: 1095; Revision: 4; Updated: Mar-21; Applicability: O, P, S, TS
Wall outlet boxes denote the classifications, cable identifiers and wall outlet box identifier.

Wall outlet box colours

The use of designated wall outlet box colours can provide an easy way to distinguish highly classified systems from other systems. For example, while TOP SECRET and SECRET wall outlet boxes have designated colours, wall outlet boxes for PROTECTED and below systems may be any colour (except for those reserved for highly classified systems). In addition, wall outlet box colours for PROTECTED and below systems may be the same colour (e.g. white). Ideally, wall outlet boxes should be the same colour that is used for associated cabling infrastructure.

Security Control: 1107; Revision: 4; Updated: Mar-21; Applicability: O, P, S, TS
The wall outlet box colours in the following table are used.

System	Wall Outlet Box Colour
TOP SECRET	Red
SECRET	Salmon pink
PROTECTED	Any colour (except red or salmon pink)
OFFICIAL	Any colour (except red or salmon pink)

Wall outlet box covers

Transparent wall outlet box covers allow for inspection of cable cross-patching and tampering.

Security Control: 1109; Revision: 3; Updated: Dec-19; Applicability: O, P, S, TS
Wall outlet box covers are clear plastic.

Fly lead installation

Keeping the lengths of fibre-optic fly leads to a minimum prevents clutter around desks, prevents damage, and reduces the chance of cross-patching and tampering. If lengths become excessive, fly leads should be treated as cabling infrastructure and run in a conduit or fixed infrastructure such as desk partitioning.

Security Control: 0218; Revision: 5; Updated: Mar-21; Applicability: TS
If fibre-optic fly leads exceeding five metres in length are used to connect wall outlet boxes to ICT equipment, they are run in a protective and easily inspected pathway that is clearly labelled at the ICT equipment end with the wall outlet box's identifier.

Connecting cable reticulation systems to cabinets

Controlling the routing from cable management systems to cabinets can assist in preventing unauthorised modifications and tampering while also providing easy inspection of cables.

Security Control: 1102; Revision: 2; Updated: Mar-21; Applicability: O, P, S
In non-TOP SECRET areas, cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.

Security Control: 1101; Revision: 2; Updated: Mar-21; Applicability: O, P, S, TS
In TOP SECRET areas, cable reticulation systems leading into cabinets in a secure communications or server room are terminated as close as possible to the cabinet.

Security Control: 1103; Revision: 2; Updated: Mar-21; Applicability: O, P, S, TS
In TOP SECRET areas, cable reticulation systems leading into cabinets not in a secure communications or server room are terminated at the boundary of the cabinet.

Terminating cables in cabinets

Having individual or divided cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

Security Control: 1098; Revision: 3; Updated: Mar-21; Applicability: O, P, S
Cables are terminated in individual cabinets; or for small systems, one cabinet with a division plate to delineate cable groups.

Security Control: 1100; Revision: 1; Updated: Sep-18; Applicability: TS

TOP SECRET cables are terminated in an individual TOP SECRET cabinet.

Terminating cable groups on patch panels

Terminating cable groups on different patch panels in cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

Security Control: 0213; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Different cable groups do not terminate on the same patch panel.

Physical separation of cabinets and patch panels

Physical separation between TOP SECRET systems and systems of lower classifications reduces the chance of cross-patching, thereby the possibility of unauthorised personnel gaining access to TOP SECRET systems.

Security Control: 1116; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
There is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.

Security Control: 0216; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
TOP SECRET and non-TOP SECRET patch panels are physically separated by installing them in separate cabinets.

Security Control: 0217; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Where spatial constraints demand patch panels of lower classifications than TOP SECRET be located in the same cabinet as a TOP SECRET patch panel:

- *a physical barrier in the cabinet is provided to separate patch panels*
- *only personnel holding a Positive Vetting security clearance have access to the cabinet*
- *approval from the TOP SECRET system's authorising officer is obtained prior to installation.*

Audio secure spaces

Audio secure spaces are designed to prevent audio conversations from being overheard. The Australian Security Intelligence Organisation (ASIO) should be consulted before any modifications are made to audio secure spaces.

Security Control: 0198; Revision: 2; Updated: Sep-18; Applicability: TS
When penetrating an audio secured space, ASIO is consulted and all directions provided are complied with.

Power reticulation

In both shared government facilities and shared non-government facilities with TOP SECRET systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

Security Control: 1123; Revision: 2; Updated: Sep-18; Applicability: TS
In TOP SECRET areas of shared government facilities, a power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.

Security Control: 1135; Revision: 1; Updated: Sep-18; Applicability: TS
In TOP SECRET areas of shared non-government facilities, a power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.

Further information

Australian Standards for cables can be obtained from the Australian Communications and Media Authority at https://www.acma.gov.au/cabling-standards-and-regulations.

Further information on physical security for Security Zones and secure rooms can be found in the Attorney-General's Department's ***Protective Security Policy Framework***, ***Entity facilities*** policy, at https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx.

Further information on endorsed seals for various sealing requirements is available in the SCEC's ***Security Equipment Evaluated Products List*** at https://www.scec.gov.au/catalogue.

Emanation security

Applicability

This section is only applicable to:

- organisations 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 information.

Emanation security threat assessments in Australia

Obtaining current threat advice from the Australian Cyber Security Centre (ACSC) on potential adversaries, and applying the appropriate counter-measures, is vital to protecting systems from emanation security threats.

Security Control: 0247; Revision: 3; Updated: Sep-18; Applicability: S, TS
System owners deploying systems with Radio Frequency (RF) transmitters inside or co-located with their facility contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.

Security Control: 0248; Revision: 5; Updated: Sep-18; Applicability: O, P, S
System owners deploying systems with RF transmitters that will be co-located with systems of a higher classification contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.

Security Control: 1137; Revision: 2; Updated: Sep-18; Applicability: TS
System owners deploying systems in shared facilities with non-Australian government entities contact the ACSC for an emanation security threat assessment and implement any additional 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. Failing to implement recommended counter-measures and standard operating procedures to reduce threats could result in the platform emanating compromising signals, which if intercepted and analysed, could lead to platform compromise with serious consequences.

Security Control: 0932; Revision: 5; Updated: Sep-18; Applicability: O, P
System owners deploying systems overseas contact the ACSC for emanation security threat advice and implement any additional installation criteria derived from the emanation security threat advice.

Security Control: 0249; Revision: 3; Updated: Sep-18; Applicability: S, TS
System owners deploying systems overseas contact the ACSC for an emanation security threat assessment and implement any additional 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.

Security Control: 0246; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
An emanation security threat assessment is sought as early as possible in a project's life cycle as emanation security controls can have significant cost implications.

Industry and government standards

While ICT equipment in a TOP SECRET area in Australia may not need certification to TEMPEST standards, the ICT equipment still needs to meet applicable industry and government standards.

Security Control: 0250; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Further information

Further information on cables and separation standards, as well as the potential dangers of operating RF transmitters near systems is documented in Australian Communications Security Instruction (ACSI) 61 D.

Further information on conducting an emanation security threat assessment is documented in ACSI 71 D.

Guidelines for Communications Systems

Telephone systems

Telephone systems usage policy

All non-secure telephone systems are subject to interception. Accidentally or maliciously revealing sensitive or classified information over a public telephone network can lead to the compromise of such information.

Security Control: 1078; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A telephone systems usage policy is developed and implemented.

Personnel awareness

As there is a potential for unintended disclosure of information when using telephone systems, it is important that personnel are made aware of what they can discuss on particular telephone systems, as well as security risks associated with the use of non-secure telephone systems in sensitive or classified areas.

Security Control: 0229; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Personnel are advised of the permitted sensitivity or classification of information that can be discussed over both internal and external telephone systems.

Security Control: 0230; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Personnel are advised of security risks posed by non-secure telephone systems 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 sensitivity or classification of information that can be discussed will assist in reducing the likelihood of unintended disclosure of information.

Security Control: 0231; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
When permitting different levels of conversation for different kinds of connections, telephone systems give a visual indication of what kind of connection has been made.

Protecting conversations

When sensitive or classified conversations are to be held using telephone systems, the conversation needs to be appropriately protected through the use of encryption.

Security Control: 0232; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.

Cordless telephone systems

Cordless telephone systems have minimal transmission security and are susceptible to interception. Using cordless telephone systems can result in disclosure of information to an unauthorised party through interception.

Security Control: 0233; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Cordless telephone systems are not used for sensitive or classified conversations.

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 number of security risks. However, if an organisation is able to reduce security risks through the use of an audio secure room that is secured during conversations, then they may be used.

Security Control: 0235; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in a room rated as audio secure, the room is audio secure during conversations and only personnel involved in discussions are present in the room.

Off-hook audio protection

Providing off-hook security minimises the chance of background conversations being accidentally coupled into handsets, headsets and speakerphones. Limiting the time an active microphone is open minimises this security risk.

Security Control: 0236; Revision: 4; Updated: Sep-18; Applicability: O, P
In PROTECTED areas, off-hook audio protection features are used on all telephones that are not authorised for the transmission of PROTECTED information.

Security Control: 0931; Revision: 5; Updated: Dec-20; Applicability: O, P, S
In SECRET areas, push-to-talk handsets or push-to-talk headsets are used on all telephones that are not authorised for the transmission of SECRET information.

Security Control: 0237; Revision: 4; Updated: Dec-20; Applicability: O, P, S, TS
In TOP SECRET areas, push-to-talk handsets or push-to-talk headsets are used on all telephones that are not authorised for the transmission of TOP SECRET information.

Further information

Further information on Internet Protocol (IP) telephony can be found in the video conferencing and Internet Protocol telephony section of these guidelines.

Further information on mobile phones can be found in the ***Guidelines for Enterprise Mobility***.

Further information on encryption can be found in the ***Guidelines for Cryptography***.

Video conferencing and Internet Protocol telephony

Video conferencing and Internet Protocol telephony gateways

Where a video conferencing or IP telephony network is connected to another video conferencing or IP telephony network belonging to a different security domain the gateways section of the ***Guidelines for Gateways*** applies.

Where an analog telephone network, such as the Public Switched Telephone Network (PSTN), is connected to a data network the gateways section of the ***Guidelines for Gateways*** does not apply.

Video conferencing and Internet Protocol telephony infrastructure hardening

Hardening can be applied to video conferencing units, handsets, software and servers in order to reduce their attack surface. For example, by ensuring that a Session Initiation Protocol (SIP) server:

- has a fully patched operating system
- has fully patched software
- runs only required services

- uses encrypted non-replayable authentication
- applies 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 Virtual Local Area Network (VLAN) to reach the server.

Security Control: 1562; Revision: 0; Updated: Dec-19; Applicability: O, P, S, TS
Video conferencing and IP telephony infrastructure is hardened.

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 traffic) 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 to be deployed for video conferencing, IP telephony and data traffic. Organisations are encouraged to implement one firewall that is video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

Security Control: 0546; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Where a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video or voice-aware firewall is used.

Protecting video conferencing and Internet Protocol telephony traffic

Video conferencing and IP telephony traffic is vulnerable to eavesdropping but can be protected with encryption. When encrypting video conferencing and IP telephony traffic, voice control signalling can be protected using Transport Layer Security 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.

Security Control: 0547; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Video conferencing and IP telephony signalling and data is encrypted.

Establishment of secure signalling and data protocols

Use of secure signalling and data protocols protect against eavesdropping, some types of denial of service, person-in-the-middle attacks and call spoofing attacks.

Security Control: 0548; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Video conferencing and IP telephony functions are established using secure signalling and data protocols.

Video conferencing unit and Internet Protocol phone authentication

Blocking unauthorised or unauthenticated devices by default will reduce the likelihood of unauthorised access to a video conferencing or IP telephony network.

Security Control: 0554; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.

Security Control: 0553; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.

Security Control: 0555; Revision: 3; Updated: Dec-19; Applicability: O, P, S, TS
Authentication and authorisation is used for all actions on an IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.

Security Control: 0551; Revision: 7; Updated: Jan-20; Applicability: O, P, S, TS
IP telephony is configured such that:

- *IP phones authenticate themselves to the call controller upon registration*
- *auto-registration is disabled and only authorised devices are allowed to access the network*
- *unauthorised devices are blocked by default*
- *all unused and prohibited functionality is disabled.*

Security Control: 1014; Revision: 5; Updated: Sep-18; Applicability: S, TS
Individual logins are used for IP phones.

Traffic separation

Video conferencing and IP telephony networks should be logically or physically separated from other networks to ensure availability and sufficient quality of service.

Security Control: 0549; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.

Security Control: 0556; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
Workstations are not 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.

Internet Protocol phones in public areas

IP phones in public areas may give an adversary the opportunity to exploit them for social engineering purposes (since the call may appear to be internal) or to access poorly protected voicemail boxes.

Security Control: 1015; Revision: 6; Updated: Dec-19; Applicability: O, P, S, TS
Traditional analog phones are used in public areas.

Security Control: 0558; Revision: 5; Updated: Dec-19; Applicability: O, P, S, TS
If IP phones are used in public areas, their ability to access data networks, voicemail and directory services are prevented.

Microphones and webcams

Microphones (including headsets and Universal Serial Bus [USB] handsets) and webcams can pose a security risk in classified areas. An adversary can email or host a malicious application on a compromised website and use social engineering techniques to convince users into installing the application on their workstation. Such malicious applications may then activate microphones or webcams that are attached to the workstation to act as remote listening and recording devices.

Security Control: 0559; Revision: 4; Updated: Sep-18; Applicability: O, P, S
Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.

Security Control: 1450; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.

Developing a denial of service response plan

Telephony is considered a critical service for any organisation. A denial of service response plan will assist in responding to a video conferencing and IP telephony denial of service, signalling floods, and established call teardown and RTP data floods.

Resources and services that can be used to monitor for signs of a denial of service can 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.

Security Control: 1019; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS
A denial of service response plan is developed and implemented that includes:

- *how to identify signs of a denial of service*
- *how to identify the source of a denial of service*
- *how capabilities can be maintained during a denial of service*
- *what actions can be taken to clear a denial of service.*

Further information

Further information on the use of telephones and telephone systems can be found in the telephone systems section of these guidelines.

Further information on the use of mobile devices can be found in the ***Guidelines for Enterprise Mobility***.

Further information on encryption can be found in the ***Guidelines for Cryptography***.

Further information on firewalls and gateways can be found in the ***Guidelines for Gateways***.

Further information on the use of web conferencing solutions can be found in the Australian Cyber Security Centre (ACSC)'s ***Web Conferencing Security*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/web-conferencing-security.

Fax machines and multifunction devices

Using cryptographic equipment with fax machines and multifunction devices

Specific information regarding the process and procedures for sending classified fax messages using High Assurance Cryptographic Equipment can be requested from the ACSC.

Fax machine and multifunction device usage policy

As fax machines and multifunction devices (MFDs) are a potential source of cyber security incidents, it is important that organisations develop a policy governing their use.

Security Control: 0588; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
A fax machine and MFD usage policy is developed and implemented.

Sending fax messages

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a 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 classified fax message the device will continue attempting to send the fax message even

if it has been disconnected from cryptographic equipment and connected directly to the PSTN. In such cases, the fax machine could send the classified fax message in the clear causing a data spill.

Security Control: 1092; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.

Security Control: 0241; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure or the PSTN.

Receiving fax messages

While the communications path between fax machines and MFDs may be appropriately protected, personnel should still be aware of who has a need to know of the information 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.

Security Control: 1075; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The sender of a fax message makes arrangements for the receiver to collect the fax message as soon as possible after it is received and notify the sender if the fax message does not arrive in an agreed amount of time.

Connecting multifunction devices to networks

As networked MFDs are considered to be devices that reside on a network, they should have security controls (e.g. authentication and auditing measures) of a similar strength to other devices on the network.

Security Control: 0590; Revision: 5; Updated: Dec-19; Applicability: O, P, S, TS
Security controls for MFDs connected to a network are of a similar strength to those for other devices on the network.

Connecting multifunction devices to both networks and digital telephone systems

When an MFD is connected to both a network and a digital telephone system, the MFD can act as a bridge between the two. The digital telephone system therefore needs to operate at the same sensitivity or classification as the network.

Security Control: 0245; Revision: 5; Updated: Dec-19; Applicability: O, P, S, TS
A direct connection from an MFD to a digital telephone system is not enabled unless the digital telephone system is authorised to operate at the same sensitivity or classification as the network to which the MFD is connected.

Copying documents on multifunction devices

As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel should 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.

Security Control: 0589; Revision: 5; Updated: Dec-19; Applicability: O, P, S, TS
MFDs connected to networks are not used to copy documents above the sensitivity or classification of the connected network.

Observing fax machine and multifunction device use

Placing fax machines and MFDs in public areas can help reduce the likelihood of any suspicious use going unnoticed.

Security Control: 1036; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Fax machines and MFDs are located in areas where their use can be observed.

Further information

Further information on encryption can be found in the ***Guidelines for Cryptography***.

Further information on MFDs communicating via network gateways can be found in the ***Guidelines for Gateways***.

Guidelines for Enterprise Mobility

Mobile device management

Types of mobile devices

These guidelines describe the use of mobile devices such as laptops, mobile phones and tablets.

Mobile device management policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that a mobile device management policy is developed to ensure that they are protected in an appropriate manner.

Security Control: 1533; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A mobile device management policy is developed and implemented.

Security Control: 1195; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
A Mobile Device Management solution is used to ensure mobile device management policy is applied to all mobile devices.

Security Control: 0687; Revision: 5; Updated: Sep-18; Applicability: TS
Mobile devices do not process, store or communicate TOP SECRET information unless explicitly approved by the ACSC to do so.

Privately-owned mobile devices

If organisations choose to allow personnel to use privately-owned mobile devices to access their organisation's systems or information, they should ensure that the devices do not present an unacceptable security risk. Information on security risks, and recommended security controls, for allowing the use of privately-owned mobile devices are discussed in the ACSC's ***Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*** publication.

Security Control: 1400; Revision: 4; Updated: Aug-20; Applicability: O, P
Personnel accessing official or classified systems or information using a privately-owned mobile device use an ACSC approved platform, a security configuration in accordance with ACSC guidance, and have enforced separation of official and classified information from any personal information.

Security Control: 0694; Revision: 5; Updated: Aug-20; Applicability: S, TS
Privately-owned mobile devices do not access highly classified systems or information.

Seeking legal advice for privately-owned mobile devices

Allowing privately-owned mobile devices to access an organisation's systems or information can increase liability risk. Organisations should seek legal advice to ascertain whether this scenario affects compliance with relevant legislation (e.g. compliance with government data retention laws in the ***Archives Act 1983***), and also consider whether the increased liability risks are acceptable to the organisation. Risks will be dependent on each organisation's mobile device usage policy and its implementation.

Security Control: 1297; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
Legal advice is sought prior to allowing privately-owned mobile devices to access official or classified systems or information.

Organisation-owned mobile devices

If organisations choose to issue personnel with mobile devices to access their organisation's systems or information, they should ensure that the devices do not present an unacceptable security risk. Information on security risks, and recommended security controls, for allowing the use of organisation-owned mobile devices are discussed in the ACSC's ***Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*** publication.

Security Control: 1482; Revision: 3; Updated: Aug-20; Applicability: O, P, S, TS
Personnel accessing official or classified systems or information using an organisation-owned mobile device use an ACSC approved platform with a security configuration in accordance with ACSC guidance.

Mobile device storage encryption

Encrypting the internal storage and removable media of mobile devices will lessen security risks associated with a lost or stolen device as it will present a significant challenge to an adversary looking to gain easy access to information stored on the device.

Security Control: 0869; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
All information on mobile devices is encrypted using at least an Australian Signals Directorate Approved Cryptographic Algorithm.

Mobile device communications encryption

If appropriate encryption is not available, mobile devices communicating sensitive or classified information present a security risk to such information. Encrypting communications, regardless of the protocol used (e.g. Bluetooth, infrared, Wi-Fi, 3G/4G/5G or other wireless protocols) is the only way to have any assurances that the information is protected.

Security Control: 1085; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Mobile devices used to communicate sensitive or classified information over public network infrastructure use encryption approved for communicating such information over public network infrastructure.

Mobile device Bluetooth functionality

Bluetooth provides inadequate security for information that is passed between mobile devices and other Bluetooth devices. As such, Bluetooth is not suitable for use with highly classified mobile devices. Furthermore, as Bluetooth has a number of known weaknesses which can potentially be exploited, the range of Bluetooth communications for all other mobile devices should be limited.

Security Control: 1202; Revision: 1; Updated: Sep-18; Applicability: O, P
The range of Bluetooth communications between mobile devices and other Bluetooth devices is restricted to less than 10 metres by using class 2 or class 3 Bluetooth devices.

Security Control: 0682; Revision: 4; Updated: Sep-18; Applicability: S, TS
Bluetooth functionality is not enabled on highly classified mobile devices.

Mobile device Bluetooth pairing

To mitigate security risks associated with pairing mobile devices with other Bluetooth devices, Bluetooth version 2.1 introduced secure simple pairing and extended inquiry response. Secure simple pairing improved the pairing experience for Bluetooth devices and introduced a form of public key cryptography while extended inquiry response provided more information during the inquiry procedure to allow for better filtering of Bluetooth devices.

In addition to using Bluetooth devices that support at least Bluetooth version 2.1, personnel should consider the location and manner in which they pair Bluetooth devices. For example, by avoiding pairing devices in public locations.

Security Control: 1196; Revision: 1; Updated: Sep-18; Applicability: O, P

Mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.

Security Control: 1200; Revision: 3; Updated: Sep-18; Applicability: O, P
Bluetooth pairing is performed using Bluetooth version 2.1 or later.

Security Control: 1198; Revision: 1; Updated: Sep-18; Applicability: O, P
Bluetooth pairing is performed in a manner such that connections are only made between intended Bluetooth devices.

Security Control: 1199; Revision: 1; Updated: Sep-18; Applicability: O, P
Bluetooth pairings are removed from mobile devices when there is no longer a requirement for their use.

Configuration control

Poorly controlled mobile devices are more vulnerable to compromise and provide an adversary with a potential access point into systems. Although organisations may initially provide secure mobile devices, the state of security may degrade over time. The security of mobile devices should be audited regularly to ensure their integrity.

Security Control: 0863; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Mobile devices prevent personnel from installing or uninstalling applications once provisioned.

Security Control: 0864; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS
Mobile devices prevent personnel from disabling or modifying security functions once provisioned.

Maintaining mobile device security

It is important that mobile devices are regularly tested to ensure that they meet organisation-defined security configurations and that patches are being applied.

Security Control: 1365; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Mobile carriers that are able to provide timely security updates for mobile devices are used.

Security Control: 1366; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Mobile devices are able to accept security updates from mobile carriers as soon as they become available.

Connecting mobile devices to the internet

During the time mobile devices are connected to the internet for web browsing they are directly exposed to targeted cyber intrusions originating from the internet. Should web browsing be required, best practice involves establishing a Virtual Private Network (VPN) connection and browsing the web though an organisation's internet gateway.

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 targeted cyber intrusions from such networks. Disabling split tunnelling may not be achievable on all mobile devices. Organisations can refer to the relevant ACSC guidance for mobile devices on how to manage security risks associated with split tunnelling.

Security Control: 0874; Revision: 4; Updated: Sep-18; Applicability: O, P
Web browsing from mobile devices is conducted through an organisation's internet gateway rather than via a direct connection to the internet.

Security Control: 0705; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When accessing an organisation system via a VPN connection, split tunnelling is disabled.

Further information

Further information on the use of mobile devices can be found in the mobile device usage section of these guidelines.

Further information on using Bluetooth to communicate sensitive or classified information can be found in the wireless devices and Radio Frequency transmitters section of the ***Guidelines for Physical Security***.

Further information on the use of encryption to reduce storage and physical transfer requirements is detailed in the cryptographic fundamentals section of the ***Guidelines for Cryptography***.

Further information on ACSC approved platforms can be found on the ***Evaluated Products List*** at https://www.cyber.gov.au/acsc/view-all-content/epl-products.

Further information on allowing the use of privately-owned devices by personnel to access their organisation's systems and information can be found in the ACSC's ***Bring Your Own Device for Executives*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/bring-your-own-device-executives.

Further information and specific guidance on enterprise mobility can be found in the ACSC's ***Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/risk-management-enterprise-mobility-including-bring-your-own-device.

Further information on securely configuring mobile devices can be found in the following ACSC publications:

- ***Security Configuration Guide – Apple iOS 14 Devices*** at https://www.cyber.gov.au/acsc/view-all-content/publications/security-configuration-guide-apple-ios-14-devices
- ***Security Configuration Guide – Samsung Galaxy S10, S20 and Note 20 Devices*** at https://www.cyber.gov.au/acsc/view-all-content/publications/security-configuration-guide-samsung-galaxy-s10-s20-and-note-20-devices
- ***Security Configuration Guide – Viasat Mobile Dynamic Defense*** at https://www.cyber.gov.au/acsc/view-all-content/publications/security-configuration-guide-viasat-mobile-dynamic-defense.

Further information on configuring personal mobile devices can be found in the ACSC's ***Security Tips for Personal Devices*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-personal-devices.

Further information on Bluetooth security can be found in National Institute of Standards and Technology Special Publication 800-121 Rev. 2, ***Guide to Bluetooth Security***, at https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final.

Mobile device usage

Mobile device usage policy

Since mobile devices routinely leave the office environment, and the protection it affords, it is important that organisations develop a mobile device usage policy governing their use.

Security Control: 1082; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A mobile device usage policy is developed and implemented.

Personnel awareness

Mobile devices can have both a voice and data component capable of processing or communicating information. In such cases, personnel should know the sensitivity or classification of information that mobile devices have been approved to process, store and communicate.

Security Control: 1083; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.

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.

Security Control: 0240; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Paging, Multimedia Message Service, Short Message Service or instant messaging apps are not used to communicate sensitive or classified information.

Using mobile devices in public spaces

Personnel should be aware of the environment they use mobile devices in to view or communicate sensitive or classified information, especially in public areas such as public transport, transit lounges and coffee shops. In such locations personnel taking care to ensure information is not observed or conversations are overheard will assist in maintaining the confidentiality of their organisation's information. In some cases, privacy filters can be applied to the screen of a mobile device to prevent onlookers from reading content off its screen.

Security Control: 0866; Revision: 4; Updated: Apr-19; Applicability: O, P, S, TS
Sensitive or classified information is not viewed or communicated in public locations unless care is taken to reduce the chance of conversations being overheard or the screen of a mobile device being observed.

Security Control: 1145; Revision: 3; Updated: Sep-18; Applicability: S, TS
Privacy filters are applied to the screens of highly classified mobile devices.

Maintaining control of mobile devices

As mobile devices are portable in nature, and can be easily lost or stolen, it is strongly advised that personnel do not leave mobile devices unattended when being actively used.

Security Control: 0871; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS
Mobile devices are kept under continual direct supervision when being actively used.

Security Control: 0870; Revision: 3; Updated: Apr-19; Applicability: O, P, S, TS
Mobile devices are carried or stored in a secured state when not being actively used.

Carrying mobile devices

As mobile devices used outside the office will be carried through areas not authorised to process the information stored on them, carrying them in a secured state (i.e. encryption is active when they are not in use) will decrease the likelihood of accidental or deliberate compromise of information. Depending on the type of mobile device, the effectiveness of encrypting its 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.

Security Control: 1084; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
If unable to apply encryption to mobile devices that is suitable for them to be carried through areas not authorised to process the information stored on them, they are physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.

Mobile device emergency sanitisation process and procedures

The sanitisation of mobile devices in emergency situations can assist in reducing the potential for compromise of information by an adversary. This may be achieved through the use of a remote wipe capability or a cryptographic key zeroise or sanitisation function if present.

Security Control: 0701; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS

A mobile device emergency sanitisation process, and supporting mobile device emergency sanitisation procedures, is developed and implemented.

Security Control: 0702; Revision: 4; Updated: Aug-19; Applicability: S, TS
If a cryptographic zeroise or sanitise function is provided for cryptographic keys on highly classified mobile devices, the function is used as part of the mobile device emergency sanitisation process.

Before travelling overseas with mobile devices

Personnel travelling overseas with mobile devices face additional security risks compared to travelling domestically, especially when travelling to high/extreme risk countries. As such, appropriate precautions should be taken. Personnel should also be aware that when they leave Australian borders they also leave behind any expectations of privacy.

Security Control: 1298; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Personnel are advised of privacy and security risks when travelling overseas with mobile devices.

Security Control: 1554; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
If travelling overseas with mobile devices to high/extreme risk countries, personnel are:

- *issued with newly provisioned accounts and devices from a pool of dedicated travel devices which are used solely for work-related activities*
- *advised on how to apply and inspect tamper seals to key areas of devices*
- *advised to avoid taking any personal devices, especially if rooted or jailbroken.*

Security Control: 1555; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
Before travelling overseas with mobile devices, personnel take the following actions:

- *record all details of the devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers*
- *update all applications and operating systems*
- *remove all non-essential accounts, applications and data*
- *apply security configuration settings, such as lock screens*
- *configure remote locate and wipe functionality*
- *enable encryption, including for any media used*
- *backup all important data and configuration settings.*

While travelling overseas with mobile devices

Personnel lose control of mobile devices and media any time they are not on their person. This includes when placing mobile devices and media in checked-in luggage or leaving them in hotel rooms (including hotel room safes). In addition, allowing untrusted people to access mobile devices provides an opportunity for them to be tampered with.

Security Control: 1299; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Personnel take the following precautions when travelling overseas with mobile devices:

- *never leaving devices or media unattended for any period of time, including by placing them in checked-in luggage or leaving them in hotel safes*
- *never storing credentials with devices that they grant access to, such as in laptop bags*
- *never lending devices to untrusted people, even if briefly*
- *never allowing untrusted people to connect other devices or media to their devices, including for charging*

- *never using designated charging stations, wall outlet charging ports or chargers supplied by untrusted people*
- *avoiding connecting devices to open or untrusted Wi-Fi networks*
- *using an approved Virtual Private Network to encrypt all device communications*
- *using encrypted mobile applications for communications instead of using foreign telecommunication networks*
- *disabling any communications capabilities of devices when not in use, such as cellular data, wireless, Bluetooth and Near Field Communication*
- *avoiding reuse of media once used with other parties' devices or systems*
- *ensuring any media used for data transfers are thoroughly checked for malicious code beforehand*
- *never using any gifted devices, especially media, when travelling or upon returning from travelling.*

Security Control: 1088; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Personnel report the potential compromise of mobile devices, media or credentials to their organisation as soon as possible, especially if they:

- *provide credentials, decrypt devices or have devices taken out of sight by foreign government officials*
- *have devices or media stolen that are later returned*
- *loose devices or media that are later found*
- *observe unusual behaviour of devices.*

After travelling overseas with mobile devices

Following overseas travel with mobile devices, personnel should take appropriate precautions to ensure that their devices don't pose an undue security risk to their organisation's systems and information. In most cases, sanitising and resetting mobile devices, including all media used with them, will be sufficient; however, upon returning from high/extreme risk countries, additional precautions will likely be needed.

Security Control: 1300; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Upon returning from travelling overseas with mobile devices, personnel take the following actions:

- *sanitise and reset devices, including all media used with them*
- *decommission any physical credentials that left their possession during their travel*
- *report if significant doubt exists as to the integrity of any devices following their travel.*

Security Control: 1556; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
If returning from travelling overseas with mobile devices to high/extreme risk countries, personnel take the following additional actions:

- *reset user credentials used with devices, including those used for remote access to their organisation's systems*
- *monitor accounts for any indicators of compromise, such as failed login attempts.*

Further information

Further information on the management of mobile devices can be found in the mobile device management section of these guidelines.

Further information on using mobile devices in highly classified areas can be found in the wireless devices and Radio Frequency transmitters section of the ***Guidelines for Physical Security***.

Further information on travelling overseas with mobile devices can be found in the ACSC's ***Travelling Overseas with Electronic Devices*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/travelling-overseas-with-electronic-devices.

Further information on security briefcases can be found in the Australian Security Intelligence Organisation (ASIO)'s Security Equipment Guide-005, ***Briefcases for the Carriage of Security Classified Information***, from the Protective Security Policy GovTEAMS community or ASIO by email.

Further information on approved multi-use satchels, pouches and transit bags can be found in the Security Construction and Equipment Committee's ***Security Equipment Evaluated Products List*** at https://www.scec.gov.au/catalogue.

Guidelines for Evaluated Products

Evaluated product acquisition

Evaluated products

An evaluated product provides a level of assurance in its security functionality that an unevaluated product does not. To assist in providing this assurance, the Australian Signals Directorate (ASD) performs product evaluations through the following programs:

- ASD Cryptographic Evaluation (ACE) program, for products used to protect classified information.
- High Assurance Evaluation program, for products used to protect highly classified information.

The Australian Cyber Security Centre (ACSC) also certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria, as part of the Australasian Information Security Evaluation Program (AISEP).

For organisations seeking to procure evaluated products, the ***Evaluated Products List*** contains a list of products that have been evaluated through the ACE program or the High Assurance Evaluation program while the ***Certified Products List*** contains a list of products that have been certified in accordance with the Common Criteria.

Protection Profiles

A Protection Profile (PP) is a technology-specific document that defines the security functions that must be included in a Common Criteria certified product to mitigate specific cyber threats. PPs can be published by a recognised Common Criteria Recognition Arrangement (CCRA) scheme or by the CCRA body itself. PPs published by the CCRA body are referred to as collaborative PPs.

The ACSC recognises all PPs listed on the Common Criteria website in addition to those listed on the ACSC's website. Where a PP does not exist, an evaluation based on an Evaluation Assurance Level (EAL) may be accepted. Such evaluations are capped at EAL2+ as this represents the best balance between completion time and meaningful security assurance gains.

Evaluation documentation

Organisations choosing to use Common Criteria certified products can determine their suitability by reviewing their evaluation documentation. This includes the security target and certification report.

Products that are undergoing a Common Criteria evaluation will not have published evaluation documentation. However, documentation can be obtained from the ACSC if a product is being evaluated through the AISEP. For a product that is in evaluation through a foreign scheme, the product's vendor can be contacted directly for further information.

Evaluated product selection

A Common Criteria evaluation is traditionally conducted at a specified EAL; however, evaluations against a PP exist outside of this scale. Notably, while products evaluated against a PP will fulfil the Common Criteria EAL requirements, the EAL number will not be published.

Security Control: 0280; Revision: 7; Updated: Sep-19; Applicability: O, P, S, TS
If procuring an evaluated product, a product that has completed a PP-based evaluation is selected in preference to one that has completed an EAL-based evaluation.

Delivery of evaluated products

It is important that organisations ensure that products they purchase are the actual products that are delivered. In the case of evaluated products, if the product delivered differs from an evaluated version then the assurance gained from the evaluation may not necessarily apply.

Packaging and delivery practices can vary greatly from product to product. For most evaluated products, standard commercial packaging and delivery practices are likely to be sufficient. However, in some cases more secure packaging and delivery practices, including tamper-evident seals and secure transportation, may be required. In the case of the digital delivery of evaluated products, vendor-supplied checksums can often be used to ensure the integrity of software that was delivered.

Security Control: 0285; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.

Security Control: 0286; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
When procuring high assurance ICT equipment, the ACSC is contacted for any equipment-specific delivery procedures.

Further information

Further information on the ACE program is available at https://www.cyber.gov.au/acsc/view-all-content/programs/asd-cryptographic-evaluation-program.

Further information on the High Assurance Evaluation program is available at https://www.cyber.gov.au/acsc/view-all-content/programs/high-assurance-evaluation-program.

Further information on the AISEP is available at https://www.cyber.gov.au/acsc/view-all-content/programs/australasian-information-security-evaluation-program.

The ***Evaluated Products List*** is available at https://www.cyber.gov.au/acsc/view-all-content/epl-products.

The ***Certified Products List*** is available at https://commoncriteriaportal.org/products/.

Evaluated product usage

Evaluated configuration

An evaluated product is considered to be operating in an evaluated configuration if:

- functionality that it uses was in the scope of the 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 evaluation documentation.

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 in its certification report.

Patching evaluated products

In the majority of cases, the latest patched version of an evaluated product will be more secure than an older unpatched version. While the application of patches will not normally place an evaluated product into an unevaluated configuration, some vendors may include new functionality, which has not been evaluated, with their patches. In such

cases, organisations should use their judgement to determine whether this deviation from the evaluated configuration constitutes additional security risk or not.

Installation and configuration of evaluated products

Product evaluation provides assurance that a product's security functionality will work as expected when operating in a clearly defined configuration. The scope of the evaluation specifies the security functionality that can be used and how a product is to be configured and operated. Using an evaluated product in an unevaluated configuration could result in the introduction of security vulnerabilities that were not considered as part of the product's evaluation.

For Common Criteria certified products, information is available from vendors regarding its installation, configuration, administration and operation. Additional information is also available in its evaluation documentation. For high assurance ICT equipment, installation and configuration guidance can be obtained from the ACSC.

Security Control: 0289; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Evaluated products are installed, configured, administered and operated in accordance with vendor guidance and evaluation documentation.

Security Control: 0290; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
High assurance ICT equipment is installed, configured, administered and operated in accordance with guidance produced by the ACSC.

Use of high assurance ICT equipment in unevaluated configurations

Given the value of the information being protected by high assurance ICT equipment, it should always be operated in an evaluated configuration.

Security Control: 0292; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
High assurance ICT equipment is only operated in an evaluated configuration.

Further information

Further information on the use of ICT equipment can be found in the ***Guidelines for ICT Equipment***.

Further information on patching can be found in the system patching section of the ***Guidelines for System Management***.

Guidelines for ICT Equipment

ICT equipment usage

ICT equipment management policy

Since ICT equipment is capable of processing, storing or communicating sensitive or classified information, it is important that an ICT equipment management policy is developed and implemented to ensure that ICT equipment, and the information it processes, stores or communicates, is protected in an appropriate manner.

Security Control: 1551; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment management policy is developed and implemented.

Classifying ICT equipment

The purpose of classifying ICT equipment it to acknowledge the sensitivity or classification of information that it is approved for processing, storing or communicating.

Classifying ICT equipment also assists in ensuring that the appropriate sanitisation, destruction and disposal processes are followed at the end of its life.

Security Control: 0293; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment is classified based on the highest sensitivity or classification of information that it is approved for processing, storing or communicating.

Labelling ICT equipment

Applying protective markings to ICT equipment assists to reduce the likelihood that a user will accidentally input information into it that it is not approved for processing, storing or communicating.

While text-based protective markings are typically used for labelling ICT equipment, there may be circumstances where colour-based protective markings or other marking schemes need to be used instead. In such cases, the marking scheme will need to be documented and personnel will need to be trained in its use.

Security Control: 0294; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment, with the exception of high assurance ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.

Labelling high assurance ICT equipment

High assurance ICT equipment often has tamper-evident seals placed on its external surfaces. To assist users in noticing changes to these seals, and to prevent functionality being degraded, organisations should limit the use of labels on high assurance ICT equipment.

Security Control: 0296; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The Australian Cyber Security Centre (ACSC)'s approval is sought before applying labels to external surfaces of high assurance ICT equipment.

Handling ICT equipment

As ICT equipment can often retain sensitive or classified information, it will need to be handled, and subsequently protected, as per the sensitivity or classification of information that it displays, processes, stores or communicates. However, applying encryption to media within ICT equipment may reduce the requirements for storage and physical

transfer. Any reduction in requirements needs to be based on the original sensitivity or classification of information residing on media within the ICT equipment and the level of assurance in the encryption software being used to encrypt the media.

Security Control: 1599; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
ICT equipment is handled in a manner suitable for its sensitivity or classification.

Further information

Further information on classifying and labelling of media can be found in the media usage section of the ***Guidelines for Media***.

Further information on the use of protective markings can be found in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.

ICT equipment maintenance and repairs

Maintenance and repairs of high assurance ICT equipment

Due to the nature of high assurance ICT equipment, it is important that that ACSC's approval is sought before any maintenance or repair work is undertaken.

Security Control: 1079; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The ACSC's approval is sought before undertaking any repairs to high assurance ICT equipment.

On-site maintenance and repairs

Making unauthorised repairs to ICT equipment could impact its integrity. As such, using cleared technicians to maintain and repair ICT equipment on-site is considered the most secure approach. This ensures that if information is disclosed during the course of maintenance or repairs, the technicians are aware of the requirements to protect such information.

Organisations choosing to use uncleared technicians to maintain or repair ICT equipment should be aware of the requirement for cleared personnel to escort uncleared technicians during maintenance or repair activities.

Security Control: 0305; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
Maintenance and repairs of ICT equipment is carried out on-site by an appropriately cleared technician.

Security Control: 0307; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the ICT equipment and associated media is sanitised before maintenance or repair work is undertaken.

Security Control: 0306; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician is escorted by someone who:

- *is appropriately cleared and briefed*
- *takes due care to ensure that information is not disclosed*
- *takes all responsible measures to ensure the integrity of the ICT equipment*
- *has the authority to direct the technician*
- *is sufficiently familiar with the ICT equipment to understand the work being performed.*

Off-site maintenance and repairs

Organisations choosing to have ICT equipment maintained or repaired off-site should be aware of requirements for the external company's facilities to be approved to do so based on the sensitivity or classification of the ICT equipment.

Organisations choosing to have ICT equipment maintained or repaired off-site can sanitise the ICT equipment prior to transport, and subsequent maintenance or repair activities, to lower (depending on the types of media involved) its physical transfer and storage requirements.

Security Control: 0310; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment maintained or repaired off-site is done so in accordance with the physical transfer and storage requirements for the sensitivity or classification of the ICT equipment.

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.

Security Control: 0944; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment maintained or repaired off-site is treated as per the requirements for the sensitivity or classification of the area that the ICT equipment will be returned to.

Inspection of ICT equipment following maintenance and repairs

Following the maintenance or repair of ICT equipment (either on-site or off-site), it is important that the ICT equipment is inspected to ensure that it retains its approved software configuration and that no unauthorised modifications (either accidental or deliberate) have been made by technicians.

Security Control: 1598; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Following maintenance or repair activities for ICT equipment, the ICT equipment is inspected to confirm it retains its approved software configuration and that no unauthorised modifications have taken place.

Further information

Further information on the sanitisation of ICT equipment can be found in the ICT equipment sanitisation and disposal section of these guidelines.

Further information on the sanitisation of media can be found in the media sanitisation section of the ***Guidelines for Media***.

Further information on the storage and transfer of ICT equipment can be found in AGD's PSPF, ***Physical security for entity resources*** policy, at https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx.

ICT equipment sanitisation and disposal

ICT equipment sanitisation and disposal processes and procedures

When disposing of ICT equipment, any media in the ICT equipment should be sanitised in situ or removed and sanitised separately. Once any media has been sanitised or removed, ICT equipment can be considered sanitised. As such, the ICT equipment can then be declassified and formally authorised for release into the public domain. However, if media cannot be sanitised or removed, the ICT equipment will need to be destroyed in its entirety.

In addition, removing labels and markings indicating the classification, codewords, caveats, owner, system or network details as part of the disposal process will ensure ICT equipment does not display indications of its prior use and draw undue attention.

Media typically found in ICT equipment includes:

- electrostatic memory devices, such as laser printer cartridges used in multifunction devices (MFDs)
- non-volatile magnetic memory, such as hard disks
- non-volatile semiconductor memory, such as flash cards and solid state drives
- volatile memory, such as random-access memory sticks.

Security Control: 0313; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment sanitisation process, and supporting ICT equipment sanitisation procedures, is developed and implemented.

Security Control: 1550; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment disposal process, and supporting ICT equipment disposal procedures, is developed and implemented.

Security Control: 0311; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
When disposing of ICT equipment containing media, the ICT equipment is sanitised by sanitising the media within the ICT equipment, removing the media from the ICT equipment or destroying the ICT equipment in its entirety.

Security Control: 1217; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Labels and markings indicating the classification, codewords, caveats, owner, system, network, or any other marking that can associate the ICT equipment with its original use, are removed prior to disposal.

Security Control: 0316; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Following sanitisation, destruction or declassification, a formal administrative decision is made to handle ICT equipment, or its waste, as 'publicly releasable' before it is released into the public domain.

Sanitisation and disposal of highly sensitive ICT equipment

The ACSC provides specific advice on how to securely dispose of high assurance ICT equipment and ICT equipment designed or modified to meet TEMPEST standards. In addition, ICT equipment located overseas that has processed or stored Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) material can have more severe consequences for Australian interests if not sanitised and disposed of appropriately.

Security Control: 0315; Revision: 6; Updated: Dec-20; Applicability: O, P, S, TS
When disposing of high assurance ICT equipment, it is destroyed prior to its disposal.

Security Control: 0321; Revision: 3; Updated: Dec-20; Applicability: O, P, S, TS
When disposing of ICT equipment that has been designed or modified to meet TEMPEST standards, the ACSC is contacted for requirements relating to its secure disposal.

Security Control: 1218; Revision: 2; Updated: Oct-19; Applicability: S, TS
ICT equipment, including associated media, that is located overseas and has processed or stored AUSTEO or AGAO information is sanitised in situ.

Security Control: 0312; Revision: 4; Updated: Sep-18; Applicability: S, TS
ICT equipment, including associated media, that is located overseas and has processed or stored AUSTEO or AGAO information that cannot be sanitised in situ is returned to Australia for destruction.

Sanitisation and disposal of printers and multifunction devices

When sanitising and disposing of printers and MFDs, the printer cartridge or MFD print drum should be sanitised in addition to the sanitisation or removal of any media. This can be achieved by printing random text with no blank areas

on each colour printer cartridge or MFD print drum. In addition, transfer rollers and platens can become imprinted with text and images over time and should be destroyed if any images have been retained. Finally, any paper jammed in the paper path should be removed.

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 should be destroyed.

Security Control: 0317; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.

Security Control: 1219; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner which cannot be removed or if a print is visible on the image transfer roller.

Security Control: 1220; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Printer and MFD platens are inspected and destroyed if any images are retained on the platen.

Security Control: 1221; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.

Security Control: 0318; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.

Security Control: 1534; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Printer ribbons in printers and MFDs are removed and destroyed.

Sanitising televisions and computer monitors

All types of televisions and computer monitors are capable of retaining information if mitigation measures are not taken during their lifetime. Cathode Ray Tube monitors and plasma screens can be affected by burn-in while Liquid Crystal Display screens can be affected by image persistence.

Televisions and computer monitors can be visually inspected by turning up the brightness and contrast to their maximum level to determine if any information has been burnt into or persists on the screen. If burn-in or image persistence is removed by this activity, televisions and computer monitors can be considered sanitised allowing them to be declassified and formally authorised for release into the public domain. However, if burn-in or persistence is not removed through these measures, televisions and computer monitors cannot be sanitised and should 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 should be destroyed.

Security Control: 1076; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Televisions and computer monitors with minor burn-in or image persistence are sanitised by displaying a solid white image on the screen for an extended period of time.

Security Control: 1222; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Televisions and computer monitors that cannot be sanitised are destroyed.

Sanitising network devices

Routers, switches, network interface cards and firewalls contain memory that is used in their operation. This memory can often retain network configuration information such as passwords, encryption keys and certificates. The correct method to sanitise a network device will depend on the configuration of the device and the type of memory within the device. Device-specific guidance provided by the ACSC, or vendor sanitisation guidance, should be consulted to determine the most appropriate method to remove information from a network device's memory.

Security Control: 1223; Revision: 4; Updated: Nov-19; Applicability: O, P, S, TS
Memory in network devices is sanitised using the following processes, in order of preference:

- *following device-specific guidance provided by the ACSC*
- *following vendor sanitisation guidance*
- *loading a dummy configuration file, performing a factory reset and then reinstalling firmware.*

Sanitising fax machines

Fax machines store information such as phone number directories and pages ready for transmission. In addition to the sanitisation or removal of any media within fax machines, the memory should be cleared and any paper jammed in the paper path should be removed.

Security Control: 1225; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The paper tray of the fax machine is removed, and a fax message with a minimum length of four pages is transmitted, before the paper tray is re-installed to allow a fax summary page to be printed.

Security Control: 1226; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Fax machines are checked to ensure no pages are trapped in the paper path due to a paper jam.

Further information

Further information on the sanitisation, destruction and disposal of media can be found in the ***Guidelines for Media***.

Guidelines for Media

Media usage

Media management policy

Since media is capable of storing sensitive or classified information, it is important that a media management policy is developed and implemented to ensure that all types of media, and the information it stores, is protected in an appropriate manner. In many cases, an organisation's media management policy will be closely tied to their removable media usage policy.

Security Control: 1549; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
A media management policy is developed and implemented.

Removable media usage policy

Establishing a removable media usage policy can decrease the likelihood and consequence of accidental data spills and information loss or theft. In doing so, a removable media usage policy will likely cover the following:

- permitted uses of removable media
- permitted types of removable media
- requirements for removable media registration
- requirements for removable media labelling
- requirements for the protection of removable media
- requirements for the reporting of lost or stolen removable media
- requirements for the sanitisation or destruction of removable media at the end of its life.

Security Control: 1359; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
A removable media usage policy is developed and implemented.

Classifying media

Media that is not correctly classified could be stored and handled inappropriately or accessed by personnel who do not have appropriate security clearances.

Security Control: 0323; Revision: 6; Updated: Apr-21; Applicability: O, P, S, TS
Media is classified to the highest sensitivity or classification of information stored on the media, unless the media has been classified to a higher sensitivity or classification.

Reclassifying media

Some activities will necessitate a change to the sensitivity or classification of media. For example, when rewritable media is connected to a system with a higher sensitivity or classification than the media and the system lacks a mechanism through which read-only access can be ensured, when rewritable media is sanitised, or when information stored on media is subject to a sensitivity or classification change.

Security Control: 0325; Revision: 6; Updated: Apr-21; Applicability: O, P, S, TS
Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured.

Security Control: 0330; Revision: 4; Updated: Apr-21; Applicability: O, P, S, TS
In order to reclassify media to a lower sensitivity or classification, the media is sanitised (unless the media is read-only) and a formal administrative decision (in consultation with information owners) is made to reclassify the media.

Handling media

As media can be easily misplaced or stolen, measures should be put in place to protect information stored on it. Furthermore, applying encryption to media may reduce the requirements for storage and handling. Any reduction in requirements needs to be based on the original sensitivity or classification of the media and the level of assurance in the encryption software being used to encrypt the media.

Security Control: 0831; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Media is handled in a manner suitable for its sensitivity or classification.

Security Control: 1059; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Media is encrypted with at least an Australian Signals Directorate Approved Cryptographic Algorithm.

Labelling media

Labelling media helps personnel to identify its sensitivity or classification and ensure that appropriate measures are applied to its storage, handling and usage.

While text-based protective markings are typically used for labelling media, there may be circumstances where colour-based protective markings or other marking schemes need to be used instead. In such cases, the marking scheme will need to be documented and personnel will need to be trained in its use.

Security Control: 0332; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Media, with the exception of internally mounted fixed media within ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.

Connecting media to systems

Some operating systems provide functionality to automatically execute software that resides on media. While this functionality was designed with a legitimate purpose in mind (e.g. automatically loading a graphical user interface to browse the contents of the media or to install software) it can also be used for malicious purposes. For example, an adversary 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 for permission.

Device access control software allows control over media that can be connected to systems and how operating systems interact with it. For example, it can prevent information from being read from media, software being executed from media and/or information being written to media. Disabling connection ports in software can also assist in preventing operating systems from interacting with media.

Media can be prevented from connecting to systems by physical means such as using wafer seals or applying epoxy. If physical means are used to prevent media connecting to systems, processes and procedures covering detection and reporting are needed in order to respond to attempts to bypass these measures.

Security Control: 1600; Revision: 1; Updated: Apr-21; Applicability: O, P, S, TS
Media is sanitised before it is used for the first time.

Security Control: 1642; Revision: 0; Updated: Apr-21; Applicability: O, P, S, TS
Media is sanitised before it is reused in a different security domain.

Security Control: 0337; Revision: 5; Updated: Apr-21; Applicability: O, P, S, TS

Media is only used with systems that are authorised to process, store or communicate the sensitivity or classification of the media.

Security Control: 0341; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Any automatic execution features for media are disabled in the operating system of systems.

Security Control: 0342; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Unauthorised media is prevented from connecting to systems via the use of device access control software, disabling connection ports or by physical means.

Security Control: 0343; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Media is prevented from being written to via the use of device access control software if there is no business requirement for its use.

Using media for data transfers

Organisations transferring data between systems belonging to different security domains are strongly encouraged to use write-once media. When done properly (e.g. using non-rewritable compact discs that have been finalised) this will ensure that information from the destination system cannot be accidently transferred, or maliciously exfiltrated, onto the media used for the data transfer and then onto another system, such as the original source system. Alternatively, if suitable write-once media is not used, the destination system should have a mechanism through which read-only access can be ensured (e.g. via a read-only device or hardware write-blocker). However, the use of read-only mechanisms is not immune to failure or compromise, therefore, rewritable media should still be sanitised following each data transfer.

It is important to note that for PROTECTED and below non-volatile flash memory media it will be possible to sanitise and reclassify the media after a data transfer to allow it to be connected to lower classified systems again. This is not possible for SECRET and above non-volatile flash memory media as the media cannot be reclassified to a lower classification following sanitisation.

Security Control: 0347; Revision: 5; Updated: Apr-21; Applicability: O, P, S, TS
When transferring data manually between two systems belonging to different security domains, write-once media is used unless the destination system has a mechanism through which read-only access can be ensured.

Security Control: 0947; Revision: 6; Updated: Apr-21; Applicability: O, P, S, TS
When transferring data manually between two systems belonging to different security domains, rewritable media is sanitised after each data transfer.

Further information

Further information on accounting for and storing media can be found in the ICT equipment and media section of the ***Guidelines for Physical Security***.

Further information on labelling ICT equipment can be found in the ICT equipment usage section of the ***Guidelines for ICT Equipment***.

Further information on reducing storage and physical transfer requirements can be found in the cryptographic fundamentals section of the ***Guidelines for Cryptography***.

Further information on using media to transfer data between systems can be found in the ***Guidelines for Data Transfers***.

Further information on the use of protective markings can be found in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.

Further information on the storage and transfer of media can be found in AGD's PSPF, ***Physical security for entity resources*** policy, at https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx.

Media sanitisation

Media in ICT equipment

ICT equipment will often contain devices that are quite small and may not be immediately recognisable as memory. Examples of these include M.2 or Mini-Serial Advanced Technology Attachment (mSATA) devices. When sanitising M.2 or mSATA devices, the method for non-volatile flash memory media sanitisation applies. Generally, if a device offers persistent storage of information, it is likely that the method for non-volatile flash memory media sanitisation will apply.

Hybrid hard drives

When sanitising hybrid hard drives, separate the non-volatile magnetic media from the circuit board containing non-volatile flash memory media and sanitise each separately.

Solid state drives

When sanitising solid state drives, the method for sanitising non-volatile flash memory media applies.

Media that cannot be sanitised

When attempts to sanitise media are unsuccessful, the only way to provide assurance that all information has been erased is to destroy the media. Additionally, some types of media cannot be sanitised and therefore should be destroyed.

Media sanitisation process and procedures

Sanitising media prior to reuse in a different environment ensures that information is not inadvertently accessed by unauthorised personnel or otherwise insufficiently protected.

Using approved methods provides a level of assurance that no information will be left on media. The methods described in these guidelines are designed not only to prevent common information recovery practices 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 was completed successfully.

Security Control: 0348; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
A media sanitisation process, and supporting media sanitisation procedures, is developed and implemented.

Volatile media sanitisation

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to the time recommended in research into preventing the recovery of the contents of volatile media.

If read back cannot be achieved following the overwriting of media contents, or information persists on the media, destroying the media is the only way to provide complete assurance information no longer persists.

Security Control: 0351; Revision: 5; Updated: Sep-18; Applicability: O, P
Volatile media is sanitised by removing power from the media for at least 10 minutes or by overwriting all locations on the media with a random pattern followed by a read back for verification.

Security Control: 0352; Revision: 3; Updated: Sep-18; Applicability: S, TS
Volatile media is sanitised by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification, and then followed by removing power from the media for at least 10 minutes.

Treatment of volatile media following sanitisation

Published literature suggests that short-term remanence effects are likely in volatile media. Data retention times have been reported to be measured in minutes at normal room temperatures and up to hours in extreme cold. Furthermore, 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 retains its classification following sanitisation.

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.

Security Control: 0835; Revision: 3; Updated: Sep-18; Applicability: TS
Following sanitisation, highly classified volatile media retains its classification if it stored static data for an extended period of time, or had data repeatedly stored on 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 media are normally not visible to an operating system or a computer's basic input/output system. Therefore, any sanitisation of the readable sectors of media will not overwrite these hidden sectors leaving any data contained in these locations untouched. Some sanitisation programs include the ability to reset media to their default state removing any host-protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of media during the subsequent sanitisation process.

Modern non-volatile magnetic media automatically reallocates 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 data was stored in a sector that was 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 media, quite often this is due to the sectors no longer meeting expected performance norms and not due to an inability to read/write to them. The Advanced Technology Attachment (ATA) secure erase command was built into the firmware of post-2001 media and is able to access sectors that have been added to the g-list.

Modern non-volatile magnetic media also contain a primary defects table or 'p-list'. The p-list contains a list of bad sectors found during post-production processes. No data is ever stored in sectors on the p-list as they are inaccessible before the media is used for the first time.

Security Control: 1065; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The host-protected area and device configuration overlay table of non-volatile magnetic media is reset prior to sanitisation.

Security Control: 0354; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Non-volatile magnetic media is sanitised by booting from separate media to the media being sanitised and then overwriting the media at least once (or three times if pre-2001 or under 15 Gigabytes) in its entirety with a random pattern followed by a read back for verification.

Security Control: 1067; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
The ATA secure erase command is used where available, in addition to using block overwriting software, to ensure the growth defects table (g-list) is overwritten.

Treatment of non-volatile magnetic media following sanitisation

Due to concerns with the sanitisation of the host-protected area, device configuration overlay table and growth defects table, highly classified non-volatile magnetic media retains its classification following sanitisation.

Security Control: 0356; Revision: 5; Updated: Sep-18; Applicability: S, TS
Following sanitisation, highly classified non-volatile magnetic media retains its classification.

Non-volatile erasable programmable read-only memory media sanitisation

When sanitising non-volatile erasable programmable read-only memory (EPROM), the manufacturer's specification for ultraviolet erasure time should be multiplied by a factor of three to provide an additional level of certainty in the process.

Security Control: 0357; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Non-volatile EPROM media is sanitised by erasing the media 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 read back 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.

Security Control: 0836; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Non-volatile EEPROM media is sanitised 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 erasable and electrically erasable programmable read-only memory media following sanitisation

As little research has been conducted into the ability to recover information from non-volatile EPROM and EEPROM media following sanitisation, highly classified EPROM and EEPROM media retains its classification following sanitisation.

Security Control: 0358; Revision: 5; Updated: Sep-18; Applicability: S, TS
Following sanitisation, highly classified non-volatile EPROM and EEPROM media retains its classification.

Non-volatile flash memory media sanitisation

In non-volatile flash memory media, a technique known as wear levelling ensures that writes are distributed evenly across each memory block. This feature necessitates non-volatile flash memory media being overwritten with a random pattern twice as this helps ensure that all memory blocks are overwritten.

Security Control: 0359; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Non-volatile flash memory media is sanitised 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 non-volatile flash memory media, and potentially bad memory blocks, it is possible that not all memory blocks were written to when attempting to overwrite the non-volatile flash memory media. For this reason, highly classified non-volatile flash memory media retains its classification following sanitisation.

Security Control: 0360; Revision: 5; Updated: Sep-18; Applicability: S, TS
Following sanitisation, highly classified non-volatile flash memory media retains its classification.

Encrypted media sanitisation

When applied appropriately, the use of encryption can provide additional assurance during media sanitisation, reuse and disposal. However, unless otherwise stated in consumer guides for evaluated encryption software, the use of encryption does not reduce the post-sanitisation classification of media.

Security Control: 1464; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Where a consumer guide for evaluated encryption software exists, the sanitisation and post-sanitisation requirements stated in the consumer guide are followed.

Further information

Further information on sanitising ICT equipment can be found in the ICT equipment sanitisation and disposal section of the ***Guidelines for ICT Equipment***.

Further information on recoverability of information from volatile media can be found in the paper ***Data Remanence in Semiconductor Devices*** at https://www.usenix.org/legacy/events/sec01/full_papers/gutmann/gutmann.pdf.

The random-access memory (RAM) testing tool MemTest86 can be obtained from https://www.memtest86.com/.

The graphics card RAM testing tool MemtestG80 and MemtestCL can be obtained from https://simtk.org/projects/memtest.

HDDerase is a freeware tool developed by the Center for Memory and Recording Research at the University of California San Diego. It is capable of calling the ATA secure erase command for non-volatile magnetic media. It is also capable of resetting the host-protected area and the device configuration overlay table information on the media. The tool is available for download from https://cmrr.ucsd.edu/resources/secure-erase.html.

Information on reliably erasing information from solid state drives can be found in the paper ***Reliably Erasing Data From Flash-Based Solid State Drives*** at https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf.

Media destruction

Media destruction process and procedures

Documenting a process and supporting procedures for media destruction will ensure that organisations carry out media destruction in an appropriate and consistent manner.

Security Control: 0363; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A media destruction process, and supporting media destruction procedures, is developed and implemented.

Media that cannot be sanitised

It is not possible to sanitise some types of media while maintaining a level of assurance that no information can be recovered.

Security Control: 0350; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The following media types are destroyed prior to disposal as they cannot be sanitised:

- *microfiche and microfilm*
- *optical discs*
- *programmable read-only memory*
- *read-only memory*
- *other types of media that cannot be sanitised*

- *faulty media that cannot be successfully sanitised.*

Media destruction equipment

When physically destroying media, using approved equipment can provide a level of assurance that that information residing on the media is actually destroyed.

Approved equipment includes destruction equipment listed in the Security Construction and Equipment Committee (SCEC)'s ***Security Equipment Evaluated Products List***, the Australian Security Intelligence Organisation (ASIO)'s Security Equipment Guide (SEG)-009, ***Optical Media Shredders***, and ASIO's SEG-018, ***Destructors***. ASIO's SEG-009 and SEG-018 are available from the Protective Security Policy GovTEAMS community or ASIO by email.

If using degaussers to destroy media, the United States' National Security Agency maintains an ***Evaluated Products List for Magnetic Degaussers***.

Security Control: 1361; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
SCEC or ASIO approved equipment is used when destroying media.

Security Control: 1160; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency are used.

Media destruction methods

The destruction methods given below are designed to ensure that recovery of information is impossible or impractical.

Security Control: 1517; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
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, is used to destroy microfiche and microfilm.

Security Control: 0366; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
One of the methods in the following table is used to destroy media.

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*

Treatment of media waste particles

Following destruction, normal accounting and auditing procedures for media do not apply. However, depending on the destruction method used and the resulting particle size, it may still need to be stored and handled as classified waste.

Security Control: 0368; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
The resulting waste for all destruction methods, except for furnace/incinerator and degausser, is stored and handled as per the following table.

Initial Media Handling	*Screen Aperture Size Particles Can Pass Through*		
	Less Than or Equal to 3 mm	*Less Than or Equal to 6 mm*	*Less Than or Equal to 9 mm*
TOP SECRET	*OFFICIAL*	*SECRET*	*SECRET*
SECRET	*OFFICIAL*	*PROTECTED*	*SECRET*
PROTECTED	*OFFICIAL*	*OFFICIAL*	*OFFICIAL*
OFFICIAL: Sensitive	*OFFICIAL*	*OFFICIAL*	*OFFICIAL*
OFFICIAL	*OFFICIAL*	*OFFICIAL*	*OFFICIAL*

Degaussing magnetic media

Degaussing magnetic media changes the alignment of magnetic domains resulting in information being permanently corrupted.

Coercivity (the resistance of magnetic material to change) varies between magnetic media types and between brands and models of the same type of media. Care is needed when degaussing magnetic media since a degausser of insufficient strength will not be effective. The United States' National Security Agency provides information on the common types of magnetic media and their associated coercivity ratings with their list of evaluated degaussers.

Since 2006, perpendicular magnetic media has been available. As some degaussers are only capable of sanitising longitudinal magnetic media, care needs to be taken to ensure that a suitable degausser is used.

Finally, to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome, product-specific directions provided by degausser manufacturers should be followed.

Security Control: 0361; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
A degausser of sufficient field strength for the coercivity of the magnetic media is used, with the field strength being checked at regular intervals.

Security Control: 0838; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
A degausser capable of the magnetic orientation (longitudinal or perpendicular) of the magnetic media is used.

Security Control: 0362; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Any product-specific directions provided by degausser manufacturers are followed.

Security Control: 1641; Revision: 0; Updated: Mar-21; Applicability: O, P, S, TS

Following destruction of magnetic media using a degausser, the magnetic media is physically damaged by deforming the internal platters by any means prior to disposal.

Supervision of destruction

To verify that media is appropriately destroyed, the process needs to be supervised by at least one person cleared to the sensitivity or classification of the media being destroyed.

Security Control: 0370; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The destruction of media is performed under the supervision of at least one person cleared to the sensitivity or classification of the media being destroyed.

Security Control: 0371; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Personnel supervising the destruction of media supervise the handling of the media to the point of destruction and ensure that the destruction is completed successfully.

Supervision of accountable material destruction

Accountable material is more important than standard media. As such, its destruction should be supervised by at least two personnel who sign a destruction certificate afterwards.

Security Control: 0372; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The destruction of accountable material is performed under the supervision of at least two personnel cleared to the sensitivity or classification of the media being destroyed.

Security Control: 0373; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Personnel supervising the destruction of accountable media supervise the handling of the material to the point of destruction, ensure that the destruction is completed successfully and sign a destruction certificate afterwards.

Outsourcing media destruction

ASIO has approved National Association for Information Destruction AAA certified destruction services with endorsements, as specified in ASIO's Protective Security Circular (PSC)-167, ***External destruction of security classified information***, for the outsourced destruction of media. ASIO's PSC-167 is available from the Protective Security Policy GovTEAMS community or ASIO by email.

Security Control: 0840; Revision: 3; Updated: Sep-18; Applicability: O, P, S
When outsourcing the destruction of media to an external destruction service, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's PSC-167, is used.

Security Control: 0839; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The destruction of TOP SECRET media or accountable material is not outsourced.

Further information

Further information on the destruction of ICT equipment can be found in the ICT equipment sanitisation and disposal section of the ***Guidelines for ICT Equipment***.

The United States' National Security Agency's ***Evaluated Products List for Magnetic Degaussers*** is available at https://www.nsa.gov/Resources/Media-Destruction-Guidance/.

Further information on the SCEC's ***Security Equipment Evaluated Products List*** is available at https://www.scec.gov.au/catalogue.

Media disposal

Media disposal process and procedures

Before media, or its waste, can be released into the public domain it needs to be sanitised, destroyed or declassified. As the compromise of official information still presents a security risk, albeit minor, an appropriate authority needs to formally authorise its release into the public domain.

In addition, removing labels and markings indicating the classification, codewords, caveats, owner, system or network details will ensure media does not display indications of its prior use and draw undue attention following its disposal.

Security Control: 0374; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A media disposal process, and supporting media disposal procedures, is developed and implemented.

Security Control: 0375; Revision: 4; Updated: Apr-21; Applicability: O, P, S, TS
Following sanitisation, destruction or declassification, a formal administrative decision (in consultation with information owners) is made to handle media, or its waste, as 'publicly releasable' before it is released into the public domain.

Security Control: 0378; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Labels and markings indicating the classification, codewords, caveats, owner, system, network, or any other marking that can associate media with its original use, are removed prior to disposal.

Further information

Further information on the disposal of ICT equipment can be found in the ICT equipment sanitisation and disposal section of the ***Guidelines for ICT Equipment***.

Guidelines for System Hardening

Operating system hardening

Standard Operating Environments

Allowing users to setup, configure and maintain their own workstations or servers can create an inconsistent environment where particular workstations or servers are more vulnerable than others. This type of environment can easily allow an adversary to gain an initial foothold on a network. A Standard Operating Environment (SOE) is a standardised implementation of an operation system and applications and is designed to ensure a consistent and secure baseline.

When SOEs are obtained from third parties, such as service providers, there are additional supply chain risks that should be considered, such as the accidental or deliberate inclusion of malicious content or configurations. To reduce the likelihood of such occurrences, organisations should not only obtain their SOEs from trusted sources but also scan them before use to ensure their integrity.

As the configuration of operating environments will naturally change over time (e.g. patches are applied, configurations are changed, and applications are added or removed) it is essential that SOEs are reviewed and updated at least annually to ensure that an updated baseline is maintained.

Security Control: 1406; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
SOEs are used for workstations and servers.

Security Control: 1608; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
SOEs provided by third parties are scanned for malicious content and configurations before being used.

Security Control: 1588; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
SOEs are reviewed and updated at least annually.

Operating system versions

Newer versions of operating systems often introduce improvements in security functionality over older versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of operating systems, especially those no longer supported by vendors, exposes organisations to exploitation techniques that have since been mitigated in newer versions of operating systems.

The x64 (64-bit) versions of Microsoft Windows include additional security functionality that the x86 (32-bit) versions lack. Using x86 (32-bit) versions of Microsoft Windows exposes organisations to exploitation techniques mitigated by x64 (64-bit) versions of Microsoft Windows.

Security Control: 1407; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
The latest version (N), or N-1 version, of an operating system is used for SOEs.

Security Control: 1408; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When developing a Microsoft Windows SOE, the 64-bit version of the operating system is used.

Operating system configuration

When operating systems are deployed in their default state it can easily lead to an unsafe operating environment allowing an adversary to gain an initial foothold on a network. Many options exist within operating systems to allow them to be configured in a secure state to minimise this security risk. The Australian Cyber Security Centre (ACSC) produces guidance to assist in securely configuring various operating systems.

Security Control: 1409; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
ACSC and vendor guidance is implemented to assist in hardening the configuration of operating systems.

Security Control: 0383; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Default operating system accounts are disabled, renamed or have their passphrase changed.

Security Control: 0380; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS
Unneeded operating system accounts, software, components, services and functionality are removed or disabled.

Security Control: 1584; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Standard users are prevented from bypassing, disabling or modifying security functionality of operating systems.

Security Control: 1491; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
Standard users are prevented from running script execution engines in Microsoft Windows, including:

- *Windows Script Host (cscript.exe and wscript.exe)*
- *PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe)*
- *Command Prompt (cmd.exe)*
- *Windows Management Instrumentation (wmic.exe)*
- *Microsoft HTML Application Host (mshta.exe).*

Local administrator accounts

When local administrator accounts are used with common account names and passphrases, it can allow an adversary that compromises these credentials on one workstation or server to easily transfer across a network to other workstations or servers.

Security Control: 1410; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Local administrator accounts are disabled; alternatively, passphrases that are random and unique for each device's local administrator account are used.

Security Control: 1469; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Unique domain accounts with local administrative privileges, but without domain administrative privileges, are used for workstation and server management.

Application management

While the ability to install any application may be a business requirement for users, this privilege can be exploited by an adversary who can email a malicious application, or host it on a compromised website, and use social engineering techniques to convince users into installing it. Even if privileged access is required to install applications, users will often use their privileged access if they believe, or can be convinced that, the requirement to install the application is legitimate. Additionally, if applications are configured to install using elevated privileges, an adversary can exploit this by creating a Windows Installer installation package to create a new account that belongs to the local administrators group. One way to manage this security risk is to allow users to install vetted and approved applications from organisation-managed software repositories or from trusted application marketplaces.

Security Control: 1592; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Users do not have the ability to install unapproved software.

Security Control: 0382; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
Users do not have the ability to uninstall or disable approved software.

Application control

An adversary can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it. Such malicious code often aims to exploit security vulnerabilities in existing applications and does not need to be installed to be successful. Application control can be an extremely effective mechanism in not only preventing malicious code from executing, but also ensuring only approved applications can be installed.

When developing application control rules, defining a list of approved executables (e.g. .exe and .com files), software libraries (e.g. .dll and.ocx files), scripts (e.g. .ps1, .bat, .cmd, .vbs and .js files) and installers (e.g. .msi, .msp and .mst files) from scratch is a more secure method than relying on a list of those currently residing on a workstation or server. Furthermore, it is preferable that organisations define their own approved list of executables, software libraries, scripts and installers rather than relying on lists from application control vendors.

Security Control: 0843; Revision: 8; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 1490; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 0955; Revision: 6; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.

Security Control: 1582; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Cryptographic hash rules, publisher certificate rules and path rules used for application control are validated at least annually.

Security Control: 1471; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
When implementing application control using publisher certificate rules, both publisher names and product names are used.

Security Control: 1392; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
When implementing application control using path rules, file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents (including adding new files) and individual files that are approved to execute.

Security Control: 1544; Revision: 1; Updated: Apr-20; Applicability: O, P, S, TS
Microsoft's latest recommended block rules are implemented to prevent application control bypasses.

Security Control: 0846; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
All users (with the exception of privileged users when performing specific administrative activities) cannot disable, bypass or be exempted from application control.

Security Control: 0957; Revision: 6; Updated: Apr-20; Applicability: O, P, S, TS
Application control is configured to generate event logs for failed execution attempts, including information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.

Enhanced Mitigation Experience Toolkit and exploit protection

An adversary who develops exploits for Microsoft Windows will be more successful in exploiting security vulnerabilities when Microsoft's Enhanced Mitigation Experience Toolkit (EMET) has not been installed. EMET was designed to provide a number of system-wide mitigation measures while also providing application-specific mitigation measures. From Microsoft Windows 10 version 1709 and Microsoft Windows Server 2016 onwards, EMET functionality has been incorporated directly into the operating system as part of exploit protection functionality.

Security Control: 1414; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
If supported, the latest version of Microsoft's EMET is implemented on workstations and servers and configured with both operating system mitigation measures and application-specific mitigation measures.

Security Control: 1492; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
If supported, Microsoft's exploit protection functionality is implemented on workstations and servers.

PowerShell

PowerShell is a powerful scripting language developed by Microsoft to provide an integrated interface for automated system administration, and is an important part of system administrator toolkits due to its ubiquity and the ease with which it can be used to fully control Microsoft Windows environments. However, it is also a dangerous exploitation tool in the hands of an adversary. In order to prevent attacks leveraging security vulnerabilities in earlier PowerShell versions, PowerShell 2.0 and below should be removed from operating systems. Additionally, PowerShell's language mode should be set to Constrained Language Mode to achieve a balance between functionality and security. Finally, logging functionality available in PowerShell, such as module logging, script block logging and transcription, can provide invaluable information for incident responders following cyber security incidents that involved PowerShell being used for malicious purposes.

Security Control: 1621; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell 2.0 and below is removed from operating systems.

Security Control: 1622; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell is configured to use Constrained Language Mode.

Security Control: 1623; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell is configured to use module logging, script block logging and transcription functionality.

Security Control: 1624; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell script block logs are protected by Protected Event Logging functionality.

Host-based Intrusion Prevention System

Many endpoint security solutions rely on signatures to detect malicious code. This approach is only effective when a particular piece of malicious code has already been profiled and signatures are current. Unfortunately, an adversary can create variants of known malicious code, or develop new unseen malicious code, to bypass traditional signature-based detection mechanisms. A Host-based Intrusion Prevention System (HIPS) can use behaviour-based detection schemes to assist in identifying and blocking 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 antivirus vendors.

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

Software firewall

Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from extracting important information, as they generally only control which ports or protocols can be used between different network segments. Many forms of malicious code are designed specifically to take advantage of this by using common protocols such as Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Simple Mail Transfer Protocol and DNS. Software firewalls are more effective than network firewalls as they can control which applications and services can communicate to and from workstations and servers. The in-built Windows firewall should be used to control both inbound and outbound traffic for specific applications.

Security Control: 1416; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.

Antivirus software

When vendors develop software they may not use secure coding practices. An adversary can take advantage of this by developing malicious code to exploit security vulnerabilities that have not been detected and remedied. As significant time and effort is often involved in developing functioning and reliable exploits, an adversary will often reuse their exploits as much as possible. While exploits may be profiled by antivirus vendors, they often remain a viable intrusion method in organisations that do not have any measures in place to detect them.

Security Control: 1417; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Antivirus software is implemented on workstations and servers and configured with:

- *signature-based detection enabled and set to a high level*
- *heuristic-based detection enabled and set to a high level*
- *detection signatures checked for currency and updated on at least a daily basis*
- *automatic and regular scanning configured for all fixed disks and removable media.*

Security Control: 1390; Revision: 2; Updated: Sep-18; Applicability: O, P
Antivirus software has reputation rating functionality enabled.

Device access control software

The use of device access control software to prevent the connection of unauthorised devices (e.g. unapproved smartphones, tablets, Bluetooth devices, wireless devices, 4G/5G dongles) to workstations and servers, via external interfaces such as USB ports, adds value as part of a defence-in-depth approach to the protection of workstations and servers.

It has also been demonstrated that an adversary can connect devices to locked workstations and servers via an external interface that allows Direct Memory Access (DMA), and subsequently gain access to encryption keys in memory. Furthermore, an adversary can read or write any content to memory that they desire. The best defence against this security vulnerability is to disable access to external interfaces that allow DMA. External interfaces that allow DMA include FireWire, ExpressCard and Thunderbolt.

Security Control: 1418; Revision: 2; Updated: Sep-20; Applicability: O, P, S, TS
Device access control software is implemented on workstations and servers to prevent unauthorised devices from being connected.

Security Control: 0345; Revision: 5; Updated: Sep-20; Applicability: O, P, S, TS
External interfaces of workstations and servers that allow DMA are disabled.

Further information

Further information on authenticating users can be found in the authentication hardening section of these guidelines.

Further information on the use of removable media with systems can be found in the media usage section of the ***Guidelines for Media***.

Further information on patching operating systems can be found in the system patching section of the ***Guidelines for System Management***.

Further information on logging and auditing of operating system events can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Further information on securely configuring Microsoft Windows operating systems can be found in the following ACSC publications:

- ***Hardening Microsoft Windows 8.1 Workstations*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-81-workstations
- ***Hardening Microsoft Windows 10 version 1909 Workstations*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-1909-workstations.

Further information on end of support for Microsoft Windows operating systems can be found in the following ACSC publications:

- ***End of Support for Microsoft Windows 7*** at https://www.cyber.gov.au/acsc/view-all-content/publications/end-support-microsoft-windows-7
- ***End of Support for Microsoft Windows 10*** at https://www.cyber.gov.au/acsc/view-all-content/publications/end-support-microsoft-windows-10
- ***End of Support for Microsoft Windows Server 2008 and Windows Server 2008 R2*** at https://www.cyber.gov.au/acsc/view-all-content/publications/end-support-microsoft-windows-server-2008-and-windows-server-2008-r2.

Further information on securely configuring Linux workstations and servers can be found in the ACSC's ***Hardening Linux Workstations and Servers*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-linux-workstations-and-servers.

Further information regarding implementing application control can be found in the ACSC's ***Implementing Application Control*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control.

Microsoft's latest recommended block rules to prevent application control bypasses can be found at https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules.

Further information on Microsoft's EMET is available at https://support.microsoft.com/en-au/help/2458544/the-enhanced-mitigation-experience-toolkit.

Further information on Microsoft's exploit protection functionality is available at https://docs.microsoft.com/en-au/windows/security/threat-protection/microsoft-defender-atp/exploit-protection.

Further information on the use of PowerShell can be found in the ACSC's ***Securing PowerShell in the Enterprise*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/securing-powershell-enterprise.

Further information on implementing PowerShell logging is available at https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html and https://devblogs.microsoft.com/powershell/powershell-the-blue-team/.

Independent testing of different antivirus software and their effectiveness is available at https://www.av-comparatives.org/ and https://av-test.org/en/.

Application hardening

Application selection

When selecting applications it is important that organisations preference vendors that have demonstrated a commitment to secure coding practices and have a strong track record of maintaining the security of their applications. This will assist not only with hardening applications but also increase the likelihood that vendors will release timely patches to remediate any security vulnerabilities in their applications.

Security Control: 0938; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS

Applications are chosen from vendors that have made a commitment to secure development and maintenance practices.

Application versions

Newer versions of applications often introduce improvements in security functionality over older versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of applications, especially key business applications such as office productivity suites (e.g. Microsoft Office), Portable Document Format (PDF) viewers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (e.g. Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .NET Framework), exposes organisations to exploitation techniques that have since been mitigated in newer versions of applications.

Security Control: 1467; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The latest releases of key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms are used when present within SOEs.

Security Control: 1483; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The latest releases of web server software, server applications that store important data, and other internet-accessible server applications are used when present within SOEs.

Hardening application configurations

By default, many applications enable functionality that is not required by users while security functionality may be disabled or set at a lower security level. This is especially risky for key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms that are likely to be targeted by an adversary. To assist in minimising this security risk, the ACSC produces guidance to assist in securely configuring key business applications. Further, to assist in securely configuring their applications, vendors may provide their own security guides.

Security Control: 1412; Revision: 2; Updated: Feb-19; Applicability: O, P, S, TS
ACSC and vendor guidance is implemented to assist in hardening the configuration of Microsoft Office, web browsers and PDF viewers.

Security Control: 1484; Revision: 1; Updated: Jan-19; Applicability: O, P, S, TS
Web browsers are configured to block or disable support for Flash content.

Security Control: 1485; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Web browsers are configured to block web advertisements.

Security Control: 1486; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Web browsers are configured to block Java from the internet.

Security Control: 1541; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS
Microsoft Office is configured to disable support for Flash content.

Security Control: 1542; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Security Control: 1470; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Any unrequired functionality in Microsoft Office, web browsers and PDF viewers is disabled.

Security Control: 1235; Revision: 2; Updated: Apr-19; Applicability: O, P, S, TS
The use of Microsoft Office, web browser and PDF viewer add-ons is restricted to organisation approved add-ons.

Security Control: 1601; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
If supported, Microsoft's Attack Surface Reduction rules are implemented.

Security Control: 1585; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Standard users are prevented from bypassing, disabling or modifying security functionality of applications.

Microsoft Office macros

Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications programming language. A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by users to greatly improve their productivity. However, an adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to sensitive or classified information. To reduce this security risk, organisations should disable or secure their use of Microsoft Office macros.

Security Control: 1487; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.

Security Control: 1488; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macros in documents originating from the internet are blocked.

Security Control: 1489; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macro security settings cannot be changed by users.

Further information

Further information on patching applications can be found in the system patching section of the ***Guidelines for System Management***.

Further information on securely configuring Microsoft Office can be found in the following ACSC publications:

- ***Hardening Microsoft Office 2013*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-office-2013
- ***Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 2016*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-office-365-proplus-office-2019-and-office-2016.

Further information on configuring Microsoft Office macro settings can be found in the ACSC's ***Microsoft Office Macro Security*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security.

Further information on configuring Microsoft Office to block macros in documents originating from the internet can be found at https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/.

Authentication hardening

Account types

When these guidelines refer to authentication hardening, it is equally applicable to all account types. This includes user accounts, privileged accounts, break glass accounts and service accounts.

Authentication types

When these guidelines refer to authentication hardening, it is equally applicable to both interactive authentication and non-interactive authentication.

Authenticating to systems

Before access to a system and its resources is granted to a user, it is essential that they are authenticated. This is typically achieved via multi-factor authentication, such as a username along with biometrics and a password, or via single-factor authentication, such as a username and passphrase.

Security Control: 1546; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
Users are authenticated before they are granted access to a system and its resources.

Multi-factor authentication

Multi-factor authentication uses two or more authentication factors to confirm a user's identity. This may include:

- something a user knows, such as a password
- something a user has, such as a Universal 2nd factor security key, physical one-time password token or smartcard
- something a user is, such as a fingerprint or their facial geometry.

Note, however, that if something a user knows is written down, or typed into a file and stored as plaintext, this becomes something that a user has rather than something a user knows.

Privileged users, positions of trust, users of remote access solutions and users with access to important data repositories are more likely to be targeted by an adversary due to their level of access. For this reason, it is especially important that multi-factor authentication is used for these accounts. In addition, multi-factor authentication is vital to any system administration activities as it can limit the consequences of a compromise by preventing or slowing an adversary's ability to gain unrestricted access to assets. In this regard, multi-factor authentication may be implemented as part of a jump server authentication process rather than performing multi-factor authentication on all critical assets, some of which may not support multi-factor authentication.

When implementing multi-factor authentication, several different authentication factors can be implemented. Unfortunately, some authentication factors, such as those sent via Short Message Service, are more susceptible to compromise by an adversary than others. For this reason, a limited number of authentication factors are recommended for use as part of multi-factor authentication implementations.

The benefit of implementing multi-factor authentication can be diminished when credentials are reused on other systems. For example, when usernames and passwords used as part of multi-factor authentication for remote access are the same as those used for corporate workstations. In such circumstances, if an adversary had compromised the device used for remote access, they could capture the username and password for reuse against a corporate workstation that did not require the use of multi-factor authentication.

Security Control: 0974; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate standard users.

Security Control: 1173; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.

Security Control: 1384; Revision: 3; Updated: Aug-20; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate privileged users each time they perform privileged actions.

Security Control: 1504; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all users of remote access solutions.

Security Control: 1505; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all users when accessing important data repositories.

Security Control: 1401; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS

Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.

Security Control: 1559; Revision: 0; Updated: Oct-19; Applicability: O, P
Passwords used for multi-factor authentication are a minimum of 6 characters.

Security Control: 1560; Revision: 0; Updated: Oct-19; Applicability: S
Passwords used for multi-factor authentication are a minimum of 8 characters.

Security Control: 1561; Revision: 0; Updated: Oct-19; Applicability: TS
Passwords used for multi-factor authentication are a minimum of 10 characters.

Security Control: 1357; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
When multi-factor authentication is implemented, none of the authentication factors on their own can be used for single-factor authentication to another system.

Single-factor authentication

A significant threat to the compromise of user accounts is offline password/passphrase cracking tools. When an adversary gains access to a list of usernames and hashed passwords/passphrases from a system, they can attempt to recover them by comparing the hash of a known password/passphrase with the hashes from the list of hashed passwords/passphrases that they obtained. By finding a match, an adversary will know the password/passphrase associated with a given username. Combined, this often forms a complete set of credentials for an account.

In order to reduce this security risk, organisations should implement multi-factor authentication. Note, while single-factor authentication is no longer considered suitable for protecting sensitive or classified information, it may not be possible to implement on some systems. In such cases, organisations will need to increase the time on average it takes an adversary to compromise a password/passphrase by introducing complexity and continuing to increase its length over time. Such increases in length can be balanced against useability through the use of passphrases rather than passwords. In cases where systems don't support passphrases, and as an absolute last resort, the strongest password length and complexity supported by a system will need to be implemented.

Security Control: 0417; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.

Security Control: 0421; Revision: 6; Updated: Oct-19; Applicability: O, P
Passphrases used for single-factor authentication are a minimum of 14 characters with complexity, ideally as 4 random words.

Security Control: 1557; Revision: 0; Updated: Oct-19; Applicability: S
Passphrases used for single-factor authentication are a minimum of 17 characters with complexity, ideally as 5 random words.

Security Control: 0422; Revision: 6; Updated: Oct-19; Applicability: TS
Passphrases used for single-factor authentication are a minimum of 20 characters with complexity, ideally as 6 random words.

Security Control: 1558; Revision: 1; Updated: Apr-20; Applicability: O, P, S, TS
Passphrases used for single-factor authentication:

- *are not constructed from song lyrics, movies, literature or any other publicly available material*
- *do not form a real sentence in a natural language*
- *are not a list of categorised words.*

Security Control: 1596; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Passphrases used for single-factor authentication can not be used to authenticate to multiple different systems.

Setting and resetting credentials for user accounts

When passwords/passphrases for users are set or reset on their behalf, it is important that they are randomly generated and, following sufficient verification of their identity (e.g. physically presenting themselves and their pass to a service desk or known colleague, or answering a set of challenge-response questions), provided to them via a secure communications channel in order to prevent their compromise. If this is not possible, alternative risk-based measures will need to be implemented.

Security Control: 1227; Revision: 4; Updated: Aug-20; Applicability: O, P, S, TS
Passwords/passphrases set or reset on users' behalf are randomly generated.

Security Control: 1593; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Users provide sufficient evidence to verify their identity when collecting a password/passphrase for their account.

Security Control: 1594; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Passwords/passphrases are provided to users via a secure communications channel or, if not possible, split into parts with part being provided to the user and part provided to the user's supervisor.

Security Control: 1595; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Users that do not set their own initial password/passphrase are required to change it on first use.

Setting and resetting credentials for service accounts

To provide additional security and credential management functionality for service accounts, Microsoft introduced group Managed Service Accounts in Microsoft Windows Server 2012. In doing so, service accounts that are created as group Managed Service Accounts do not require manual credential management by administrators, as the operating system automatically manages the credentials. This ensures that service account credentials are not misplaced or forgotten, and that they are automatically changed on a regular basis.

Security Control: 1619; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
Service accounts are created as group Managed Service Accounts.

Account lockouts

Locking an account after a specified number of failed logon attempts reduces the likelihood of successful password spraying attacks. However, care should be taken as implementing account lockout functionality can increase the likelihood of a denial of service. Alternatively, some systems can be configured to automatically slowdown repeated failed logon attempts rather than locking accounts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful password spraying attacks.

Security Control: 1403; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Accounts are locked out after a maximum of five failed logon attempts.

Security Control: 0431; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Repeated account lockouts are investigated before reauthorising access.

Account unlocks

To reduce the likelihood of social engineering being used to compromise accounts, users should provide sufficient evidence to verify their identity when requesting an account unlock.

Security Control: 0976; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
Users provide sufficient evidence to verify their identity when requesting an account unlock.

Insecure authentication methods

Authentication methods need to resist theft, interception, duplication, forgery, unauthorised access and unauthorised modification. For example, Local Area Network (LAN) Manager and NT LAN Manager authentication methods use weak hashing algorithms. As such, passwords/passphrases used as part of LAN Manager authentication and NT LAN Manager authentication (i.e. NTLMv1, NTLMv2 and NTLM2) can easily be compromised. Instead, organisations should use Kerberos for authentication within Microsoft Windows environments.

Security Control: 1603; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Authentication methods susceptible to replay attacks are disabled.

Security Control: 1055; Revision: 4; Updated: Oct-20; Applicability: O, P, S, TS
LAN Manager and NT LAN Manager authentication methods are disabled.

Security Control: 1620; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
Privileged accounts are members of the Protected Users security group.

Protecting credentials

Storing credentials with a system that it grants access to increases the likelihood of an adversary gaining access to the system. For example, a password/passphrase should never be written down and stuck to a laptop or computer monitor and one-time password tokens should never be left with computers or in laptop bags. Furthermore, obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers.

If storing credentials on a system, sufficient protection should be implemented to prevent them from being compromised as part of a targeted cyber intrusion. For example, credentials can be stored in a password vault rather than in a Microsoft Word or Excel document, credentials stored in a database can be hashed, salted and stretched, or credentials can be stored in a hardware security module.

Finally, asymmetric authentication and secure transmission of credentials reduces the likelihood of an adversary intercepting and using such information to access a system under the guise of a valid user.

Security Control: 0418; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Credentials are stored separately from systems to which they grant access.

Security Control: 1597; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Credentials are obscured as they are entered into systems.

Security Control: 1402; Revision: 5; Updated: Aug-20; Applicability: O, P, S, TS
Stored passwords/passphrases are protected by ensuring they are hashed, salted and stretched.

Security Control: 1590; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Passwords/passphrases are changed if:

- *they are directly compromised*
- *they are suspected of being compromised*
- *they appear in online data breach databases*
- *they are discovered stored in the clear on a network*
- *they are discovered being transferred in the clear across a network*
- *membership of a shared account changes*
- *they have not been changed in the past 12 months.*

Session termination

Implementing measures to automatically terminate user sessions outside of business hours (noting this may differ between different work areas), after an appropriate period of inactivity, and then reboot workstations can assist in both system maintenance activities (such as patching) as well as removing any adversaries that may have compromised a system but failed to gain persistence.

Security Control: 0853; Revision: 1; Updated: Aug-20; Applicability: O, P, S, TS
Outside of business hours, and after an appropriate period of inactivity, user sessions are terminated and workstations are rebooted.

Session and screen locking

Session and screen locking prevents unauthorised access to a system which a user has already been authenticated to access.

Security Control: 0428; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Systems are configured with a session or screen lock that:

- *activates after a maximum of 15 minutes of user inactivity or if manually activated by the user*
- *completely conceals all information on the screen*
- *ensures that the screen does not enter a power saving state before the screen or session lock is activated*
- *requires the user to reauthenticate to unlock the system*
- *denies users the ability to disable the session or screen locking mechanism.*

Logon banner

Displaying a logon banner to users before access is granted to a system reminds them of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- the user's agreement to abide by abovementioned policies
- legal ramifications of violating the abovementioned policies
- details of monitoring and auditing activities
- a point of contact for any questions.

Security Control: 0408; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.

Security Control: 0979; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Legal advice is sought on the exact wording of logon banners.

Further information

Further information on authorisations, security clearances and briefings for system access can be found in the access to systems and their resources section of the ***Guidelines for Personnel Security***.

Further information on restricting administrative privileges can be found in the ACSC's ***Restricting Administrative Privileges*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/restricting-administrative-privileges.

Further information on implementing multi-factor authentication can be found in the ACSC's ***Implementing Multi-Factor Authentication*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication.

Further information creating strong passphrases can be found in the ACSC's ***Creating Strong Passphrases*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases.

Further information on mitigating the use of stolen credentials can be found in the ACSC's ***Mitigating the Use of Stolen Credentials*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/mitigating-the-use-of-stolen-credentials.

A method for randomly generating passphrases can be found at the Electronic Frontier Foundation's website at https://www.eff.org/dice (preferably using five dice rolls and the long word list) while a random five dice roller can be found at https://www.random.org/dice/?num=5.

Virtualisation hardening

Containerisation

Containers allow for versatile deployment of systems, and can be used to quickly scale systems. However, they are still systems that run software and should be treated as any other system. Application of security controls in a containerised environment may take a different form when compared to other types of systems. For example, patching operating systems on workstations may be actioned differently to ensuring that a patched image is being used for a container, however the principle is the same. In general, the same security risks that apply to non-containerised systems would likely apply to containerised systems.

Functional separation between computing environments

Software-based isolation mechanisms are commonly used to share a physical server's hardware among multiple computing environments. The benefits of using software-based isolation mechanisms to share a physical server's hardware include increasing the range of activities that it can be used for and maximising the utilisation of its hardware.

A computing environment could consist of an entire operating system installed in a virtual machine where the isolation mechanism is a hypervisor, as is commonly used in cloud services providing Infrastructure as a Service. Alternatively, a computing environment could consist of an application which uses the shared kernel of the underlying operating system of the physical server where the isolation mechanisms are application containers or application sandboxes, as is commonly used in cloud services providing Platform as a Service. The logical separation of data within a single application, which is commonly used in cloud services providing Software as a Service, is not considered to be the same as multiple computing environments.

An adversary who has compromised a single computing environment, or who legitimately controls a single computing environment, might exploit a misconfiguration or security vulnerability in the isolation mechanism to compromise other computing environments on the same physical server, or compromise the underlying operating system of the physical server.

Security Control: 1460; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that uses secure coding practices and, when security vulnerabilities have been identified, develops and distributes patches in a timely manner.

Security Control: 1604; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS

When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.

Security Control: 1605; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system running on the server is hardened.

Security Control: 1606; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, patches are applied to the isolation mechanism and underlying operating system in a timely manner.

Security Control: 1607; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.

Security Control: 1462; Revision: 1; Updated: Jul-19; Applicability: P
When using a software-based isolation mechanism to share a physical server's hardware, the physical server and all computing environments running on the physical server are of the same classification.

Security Control: 1461; Revision: 3; Updated: Jan-21; Applicability: S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the physical server and all computing environments running on the physical server are of the same classification and within the same security domain.

Further information

Further information on hypervisor security can be found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-125A Rev. 1, ***Security Recommendations for Server-based Hypervisor Platforms***, at https://csrc.nist.gov/publications/detail/sp/800-125a/rev-1/final.

Further information on container security can be found in NIST SP 800-190 ***Application Container Security Guide*** at https://csrc.nist.gov/publications/detail/sp/800-190/final.

Guidelines for System Management

System administration

What is secure system administration

Secure system administration allows organisations to be resilient in the face of targeted cyber intrusions by protecting administrator workstations and accounts from compromise, as well as making adversary movement throughout a network more difficult. If a secure system administration environment withstands a targeted cyber intrusion, incident response will be far more agile, the damage will be limited and remediation work will be completed faster.

Secure system administration of cloud services

Secure system administration of cloud services brings unique challenges when compared to the secure administration of on-premise assets. Notably, responsibility for system administration of cloud services is often shared between service providers and organisations. As the technology stack and secure administration processes implemented by service providers are often opaque to organisations, organisations should consider a service provider's control plane to operate within a different security domain. As such, the security controls below may require adjustment.

Administrative accounts

The use of the same credentials on both an administrator workstation and a user workstation puts the administrator workstation at risk of compromise if the user workstation is compromised. The table below provides clarification on the use of different accounts.

Regular User Account	Unprivileged Administration Account	Privileged Administration Account
Unprivileged account	Unprivileged account	Privileged account
Used for web and email access Used for day-to-day non-administrative tasks	Used for authentication to dedicated administrator workstation Used for authentication to jump server(s)	Used for performance of administration tasks
	Different username and passphrase to regular user account	Different username and passphrase to regular user account

System administration process and procedures

A key component of secure system administration is ensuring that privileged actions are performed using an approved system administration process supported by system administration procedures. This will ensure that privileged actions are undertaken in a repeatable and accountable manner.

Security Control: 0042; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
A system administration process, with supporting system administration procedures, is developed and implemented.

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 administration activities. Providing a physically separate hardened administrator workstation to privileged users, in addition to their workstation used for unprivileged user access, provides greater assurance that privileged activities and credentials will not be compromised.

Using different physical machines is considered the most secure solution to separate workstations; however, a risk-based approach may determine that a virtualisation-based solution is sufficient. In such cases, the unprivileged user environment should be the 'guest' and the administrative environment should be the 'host'.

Security Control: 1380; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Privileged users use a dedicated administrator workstation when performing privileged tasks.

Security Control: 1382; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Privileged users are assigned an unprivileged administration account for authenticating to their dedicated administrator workstations.

Security Control: 1381; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Dedicated administrator workstations used for privileged tasks are prevented from communicating to assets not related to administrative activities.

Security Control: 1383; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All administrative infrastructure including, but not limited to, administrator workstations and jump servers are hardened.

Dedicated administration zones and communication restrictions

Administration security can be improved by segregating administrator workstations from the wider network. This can be achieved a number of ways, such as via the use of Virtual Local Area Networks, firewalls, network access controls and Internet Protocol Security Server and Domain Isolation.

It is recommended that segmentation and segregation be applied regardless of whether privileged users have physically separate administrator workstations or not.

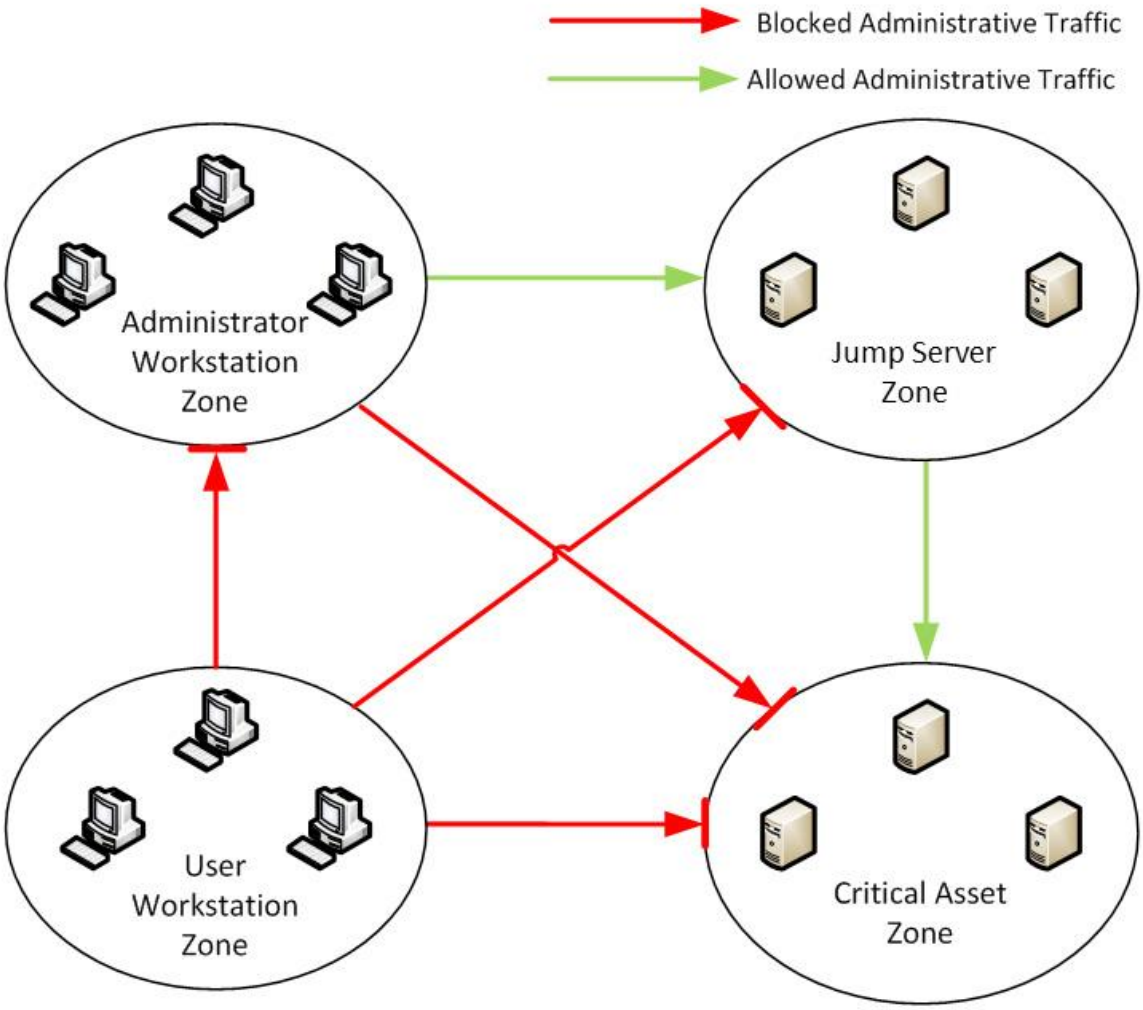
Security Control: 1385; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Administrator workstations are placed into a separate network zone to user workstations.

Restriction of management traffic flows

Limiting the flow of management traffic to only those network elements and segments explicitly required to communicate with each other can reduce the consequences of a network compromise and make it easier to detect if it does occur.

Although 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 will need to send or receive management traffic (such as Remote Desktop Protocol [RDP], Secure Shell [SSH] and similar protocols) to these assets.

The following diagram outlines how management traffic filtering could be implemented between a network comprising different network zones. The only flows of management traffic allowed are those between the 'Administrator Workstation Zone' and the 'Jump Server Zone' as well as 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 network zones.



Security Control: 1386; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Management traffic is only allowed to originate from network zones that are used to administer systems and applications.

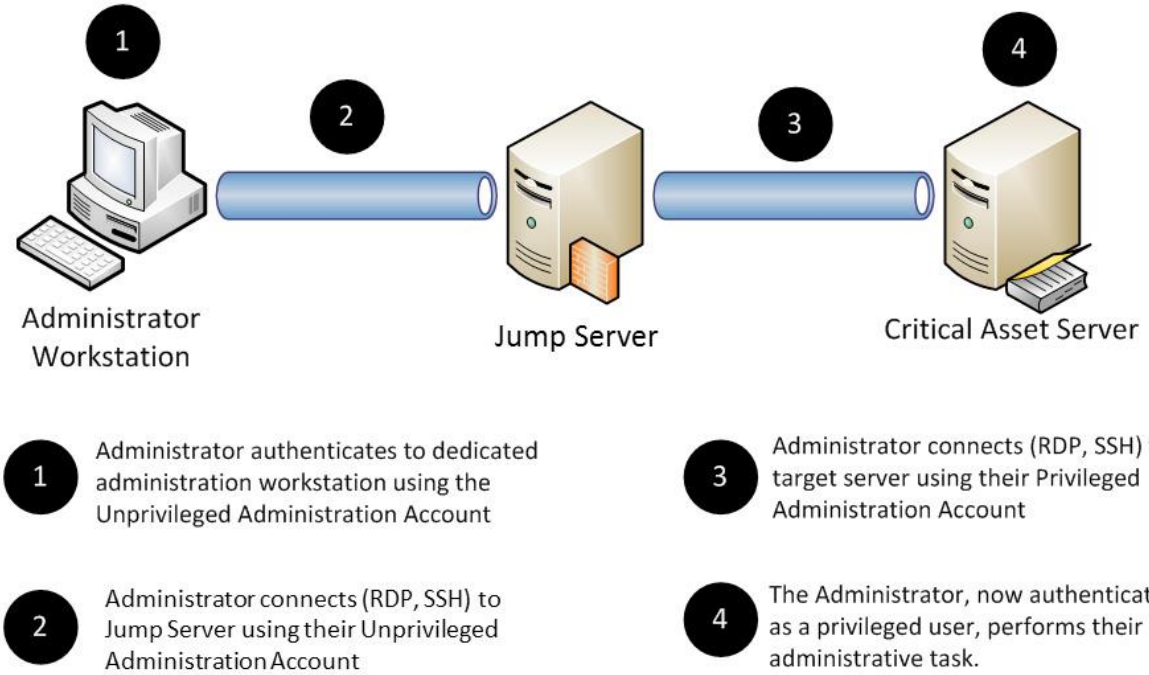
Jump servers

A jump server (also known as a jump host or jump box) is used to manage important or critical resources in a separate security domain. The use of jump servers as a form of 'management proxy' can be an effective way of simplifying and securing privileged 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
- simplified implementation of management traffic filtering
- a focal point for logging, monitoring and alerting.

In a typical scenario, if a privileged user wanted to perform administrative activities they would connect directly to the target server using RDP or SSH. However, in a jump server setup the privileged user would first connect and authenticate to the jump server, then RDP, SSH, or use remote administration tools to access the target server.

When implementing a jump server, it is recommended that organisations implement multi-factor authentication, enforce strict device communication restrictions, and harden administrative infrastructure, otherwise a jump server will yield little security benefit.



Security Control: 1387; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All administrative actions are conducted through a jump server.

Security Control: 1388; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Jump servers are prevented from communicating to assets and sending and receiving traffic not related to administrative activities.

Further information

Further information on the use of privileged accounts can be found in the access to systems and their resources section of the ***Guidelines for Personnel Security***.

Further information on multi-factor authentication for system administration can be found in the authentication hardening section of the ***Guidelines for System Hardening***.

Further information on network segmentation can be found in the network design and configuration section of the ***Guidelines for Networking***.

Further information on secure system administration can be found in the Australian Cyber Security Centre (ACSC)'s ***Secure Administration*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/secure-administration.

Further information on mitigating the use of stolen credentials can be found in the ACSC's ***Mitigating the Use of Stolen Credentials*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/mitigating-the-use-of-stolen-credentials.

Further information can also be found in Microsoft's ***Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, Version 1 and 2*** publication at https://www.microsoft.com/en-au/download/confirmation.aspx?id=36036.

System patching

Patching approaches

Patches for security vulnerabilities are provided by vendors in many forms, such as:

- fixes that can be applied to pre-existing application versions
- fixes incorporated into new applications or drivers that require pre-existing versions to be replaced
- fixes that require the overwriting of firmware on ICT equipment.

When patches are not available

When patches are not available for security vulnerabilities there are a number of approaches that can be undertaken to reduce security risks. In priority order this includes resolving the security vulnerability, preventing exploitation of the security vulnerability, containing the exploitation of the security vulnerability or detecting exploitation of the security vulnerability.

Security vulnerabilities can be resolved by:

- disabling the functionality associated with the security vulnerability
- engaging a software developer to resolve the security vulnerability
- changing to different software or ICT equipment with a more responsive vendor.

Exploitation of security vulnerabilities can be prevented by:

- applying external input sanitisation (if an input triggers the exploit)
- applying filtering or verification on output (if the exploit relates to an information disclosure)
- applying additional access controls that prevent access to the security vulnerability
- configuring firewall rules to limit access to the security vulnerability.

Exploitation of security vulnerabilities can be contained by:

- 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.

Exploitation of security vulnerabilities can be detected by:

- deploying a Host-based Intrusion Prevention System
- monitoring logging alerts
- using other mechanisms for the detection of exploits using the known security vulnerability.

Patch management process and procedures

Applying patches or updates is critical to ensuring the security of applications, drivers, operating systems and firmware in workstations, servers, mobile devices, network devices and all other ICT equipment. To assist in this, information sources should be monitored for information about new patches or updates.

Security Control: 1143; Revision: 7; Updated: Aug-19; Applicability: O, P, S, TS
A patch management process, and supporting patch management procedures, is developed and implemented.

Security Control: 1493; Revision: 1; Updated: Aug-19; Applicability: O, P, S, TS
A software register, including versions and patch histories of applications, drivers, operating systems and firmware for workstations, servers, mobile devices, network devices and all other ICT equipment, is maintained and regularly audited.

When to patch security vulnerabilities

There are multiple information sources that organisations can use to assess the applicability and impact of security vulnerabilities in the context of their environment. This can include information published in vendor security bulletins or in severity ratings assigned to security vulnerabilities using standards such as the Common Vulnerability Scoring System.

Once a patch is released by a vendor, and the associated security vulnerability has been assessed for its applicability and importance, the patch should be deployed in a timeframe that is commensurate with the security risk. Doing so ensures that resources are spent in an effective and efficient manner by focusing effort on the most significant security risks first.

If a patch is released for high assurance ICT equipment, the ACSC will conduct an assessment of the patch and may revise the ICT equipment's usage guidance. Where required, the Australian Signals Directorate will conduct an assessment of any cryptographic security vulnerability and the ACSC may revise usage guidance in the consumer guide or Australian Communications Security Instruction. If a patch for high assurance ICT equipment is approved for deployment, the ACSC will inform organisations of the timeframe in which the patch is to be deployed.

If no patches are immediately available for security vulnerabilities, temporary workarounds may provide the only effective protection until patches become available. These workarounds may be published in conjunction with, or soon after, security vulnerability announcements. Temporary workarounds may include disabling the vulnerable functionality within the operating system, application or device, or restricting or blocking access to the vulnerable service using firewalls or other access controls. The decision as to whether a temporary workaround is implemented should be risk-based, as with patching.

Security Control: 1144; Revision: 9; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

Security Control: 0940; Revision: 8; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 1472; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 1494; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

Security Control: 1495; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 1496; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.

Security Control: 0300; Revision: 6; Updated: Sep-18; Applicability: S, TS
High assurance ICT equipment is only patched with patches approved by the ACSC using methods and timeframes prescribed by the ACSC.

How to patch security vulnerabilities

To ensure that patches are applied consistently across an organisation's workstation and server fleet, it is essential that organisations use a centralised and managed approach. This will assist in ensuring the integrity and authenticity of patches being applied to workstations and servers.

Security Control: 0298; Revision: 7; Updated: Oct-19; Applicability: O, P, S, TS
A centralised and managed approach is used to patch or update applications and drivers.

Security Control: 0303; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
An approach for patching or updating applications and drivers that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

Security Control: 1497; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.

Security Control: 1498; Revision: 1; Updated: Oct-19; Applicability: O, P, S, TS
A centralised and managed approach is used to patch or update operating systems and firmware.

Security Control: 1499; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An approach for patching or updating operating systems and firmware that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

Security Control: 1500; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.

Cessation of support

When applications, operating systems and ICT equipment reach their cessation date for support, organisations will find it increasingly difficult to protect against security vulnerabilities as patches, or other forms of support, will not be made available by vendors. While the cessation date for support for operating systems is generally advised many years in advance by vendors, other applications and ICT equipment may cease to receive support immediately after a newer version is released by a vendor.

Security Control: 0304; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Security Control: 1501; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Further information

Further information on patching evaluated products can be found in the evaluated product usage section of the ***Guidelines for Evaluated Products***.

Further information on what constitutes different levels of security risk for security vulnerabilities can be found in the ACSC's ***Assessing Security Vulnerabilities and Applying Patches*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches.

Further information on patching during change freezes can be found in the ACSC's ***Patching During Change Freezes*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/patching-during-change-freezes.

Change management

Identifying the need for change

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

- identification of security vulnerabilities or cyber threats
- users identifying problems or a need for system enhancements
- upgrades or patches for software or ICT equipment
- vendors notifying the end of life for software or ICT equipment
- the implementation of new software or ICT equipment
- organisational or business process changes
- other continuous improvement activities.

Change management process and procedures

The use of a change management process ensures that changes to systems are made in an accountable manner with appropriate consultation and approval. Furthermore, a change management process provides an opportunity for the security impact of any changes to systems to be considered.

In implementing changes to systems, it is important that change management procedures clearly articulate the steps to be taken for each part of the change management process.

Security Control: 1211; Revision: 3; Updated: Jul-20; Applicability: O, P, S, TS
A change management process, and supporting change management procedures, is developed and implemented covering:

- *identification and documentation of requests for change*
- *approval required for changes to be made*
- *assessment of potential security impacts*
- *notification of any planned disruptions or outages*
- *implementation and testing of approved changes*
- *the maintenance of system and security documentation.*

Data backup and restoration

Digital preservation policy

Developing and implementing a digital preservation policy as part of digital continuity planning can assist in ensuring the long term integrity and availability of important information is maintained. Especially when taking into account the potential for data degradation and media, hardware and software obsolesce.

Security Control: 1510; Revision: 1; Updated: Aug-19; Applicability: O, P, S, TS
A digital preservation policy is developed and implemented.

Data backup and restoration processes and procedures

Having data backup and restoration processes and procedures is an important part of business continuity and disaster recovery planning. Such activities will also form an integral part of an overarching digital preservation policy.

Security Control: 1547; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
A data backup process, and supporting data backup procedures, is developed and implemented.

Security Control: 1548; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
A data restoration process, and supporting data restoration procedures, is developed and implemented.

Performing backups

When performing backups, all important information, software and configuration settings for software, network devices and other ICT equipment should be captured on a daily basis. This will ensure that should a system fall victim to a ransomware attack, important information will not be lost and that business operations will have reduced downtime.

Security Control: 1511; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups of important information, software and configuration settings are performed at least daily.

Backup storage

To mitigate the likelihood of information becoming unavailable due to accidental or malicious deletion of backups, organisations should ensure that backups are protected from unauthorised modification, corruption and deletion. This can be achieved by storing backups offline, ideally at multiple geographically-dispersed locations, or online but in a non-rewritable and non-erasable manner, such as through the use of write once, read many technologies.

Security Control: 1512; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored offline, or online but in a non-rewritable and non-erasable manner.

Security Control: 1513; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored at a multiple geographically-dispersed locations.

Retention periods for backups

To prevent backups from being retained for an insufficient amount of time to allow for the recovery of information, organisations are strongly encouraged to store backups for three months or greater.

Security Control: 1514; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored for three months or greater.

Testing restoration of backups

To ensure that backups can be restored when the need arises, and that any dependencies can be identified and managed, it is important that full restoration of backups has been tested at least once following the implementation of backup technologies and processes. Furthermore, full restoration of backups should be tested each time fundamental information technology changes occur, such as when deploying new backup technologies. In the intervening time, it is important that regular testing in the form of partial restoration of backups is undertaken.

Security Control: 1515; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS
Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Security Control: 1516; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS
Partial restoration of backups is tested on a quarterly or more frequent basis.

Further information

Further information on business continuity can be found in the service continuity for online services section of the ***Guidelines for Networking***.

Further information on preserving digital information can be found on the National Archives of Australia's website at: https://www.naa.gov.au/information-management/store-and-preserve-information/preserving-information/preserving-digital-information/digital-preservation-planning.

Guidelines for System Monitoring

Event logging and auditing

Event logging policy

By developing an event logging policy, taking into consideration any shared responsibilities between organisations and their service providers, an organisation can improve their chances of detecting malicious behaviour on systems and networks. Such an event logging policy would cover events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected.

Security Control: 0580; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS
An event logging policy is developed and implemented.

Centralised logging facility

A centralised logging facility can be used to correlate event logs from multiple sources. This functionality may be provided by a Security Information and Event Management solution.

Security Control: 1405; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
A centralised logging facility is implemented and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs.

Security Control: 0988; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events.

Events to be logged

The following list of events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

Security Control: 0584; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
For any system requiring authentication, logon, failed logon and logoff events are logged.

Security Control: 0582; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
The following events are logged for operating systems:

- *access to important data and processes*
- *application crashes and any error messages*
- *attempts to use special privileges*
- *changes to accounts*
- *changes to security policy*
- *changes to system configurations*
- *Domain Name System (DNS) and Hypertext Transfer Protocol requests*
- *failed attempts to access data and system resources*
- *service failures and restarts*
- *system startup and shutdown*

- *transfer of data to and from external media*
- *user or group management*
- *use of special privileges.*

Security Control: 1536; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The following events are logged for web applications:

- *attempted access that is denied*
- *crashes and any error messages*
- *search queries initiated by users.*

Security Control: 1537; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The following events are logged for databases:

- *access to particularly important information*
- *addition of new users, especially privileged users*
- *any query containing comments*
- *any query containing multiple embedded queries*
- *any query or database alerts or failures*
- *attempts to elevate privileges*
- *attempted access that is successful or unsuccessful*
- *changes to the database structure*
- *changes to user roles or database permissions*
- *database administrator actions*
- *database logons and logoffs*
- *modifications to data*
- *use of executable commands.*

Events log details

For each event logged, sufficient detail needs to be recorded in order for the event log to be useful.

Security Control: 0585; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
For each event logged, the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded.

Event log protection

Effective event log protection and storage, from the time they are created to the time they are destroyed, ensures the integrity, availability and non-repudiation of captured event logs.

Security Control: 0586; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Event logs are protected from unauthorised access, modification and deletion.

Event log retention

Since event logs can contribute to investigations following cyber security incidents, they should ideally be retained for the life of a system, and potentially longer. However, the minimum retention requirement for these records under the National Archives of Australia's ***Administrative Functions Disposal Authority Express Version 2*** publication is seven years.

Security Control: 0859; Revision: 3; Updated: Jan-20; Applicability: O, P, S, TS
Event logs are retained for a minimum of 7 years in accordance with the National Archives of Australia's Administrative Functions Disposal Authority Express Version 2 publication.

Security Control: 0991; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
DNS and proxy logs are retained for at least 18 months.

Event log auditing process and procedures

Auditing of event logs is an integral part of maintaining the security posture of systems. Such activities can help detect and attribute any violations of security policy, including cyber security incidents.

Security Control: 0109; Revision: 6; Updated: Aug-19; Applicability: O, P, S, TS
An event log auditing process, and supporting event log auditing procedures, is developed and implemented covering the scope and schedule of audits, what constitutes a violation of security policy, and actions to be taken when violations are detected, including reporting requirements.

Security Control: 1228; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Events are correlated across event logs to prioritise audits and focus investigations.

Further information

Further information on event logging associated with a cyber security incident can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on event logging and forwarding can be found in the Australian Cyber Security Centre's ***Windows Event Logging and Forwarding*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding.

Further information on retaining event logs can be found in the National Archives of Australia's ***Administrative Functions Disposal Authority Express Version 2*** publication at https://www.naa.gov.au/information-management/records-authorities/types-records-authorities/afda-express-version-2-functions.

Guidelines for Software Development

Application development

Types of application development

These guidelines are applicable to both traditional application development activities as well as mobile application development activities.

Development environments

Segregating development, testing and production environments can limit the spread of malicious code and minimises the likelihood of faulty code in a production environment.

Security Control: 0400; Revision: 5; Updated: Aug-20; Applicability: O, P, S, TS
Development, testing and production environments are segregated.

Security Control: 1419; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Development and modification of software only takes place in development environments.

Security Control: 1420; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Information in production environments is not used in testing or development environments unless the testing or development environments are secured to the same level as the production environments.

Security Control: 1422; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Unauthorised access to the authoritative source for software is prevented.

Secure software design

Threat modelling is an important part of secure software design. Threat modelling identifies at risk components of software, enabling security controls to be identified to reduce security risks.

Security Control: 1238; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Threat modelling and other secure design techniques are used to ensure that threats to software and mitigations to those threats are identified and accounted for.

Secure programming practices

Once a secure software design has been identified, secure programming practices should be followed during software development activities.

Security Control: 0401; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.

Software testing

Software testing can lessen the risk of security vulnerabilities in software being introduced into a production environment. Software testing can be performed using both static testing, such as code analysis, as well as dynamic testing, such as input validation and fuzzing. Vulnerability scanning tools can also assist in the detection of known security vulnerabilities, such as out of date or vulnerable dependencies. Using an independent party for software testing will remove any bias that can occur when a software developer tests their own software.

Security Control: 0402; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Software is tested for security vulnerabilities by software developers, as well as an independent party, before it is used in a production environment.

Vulnerability disclosure program

Implementing a vulnerability disclosure program, based on responsible/coordinated disclosure, can assist organisations, vendors and service providers to improve the security of their products and services as it provides a way for security researchers, customers and members of the public to responsibly notify them of potential security vulnerabilities in a coordinated manner. Furthermore, following the verification and resolution of a reported security vulnerability, it can assist organisations, vendors and service providers in notifying their customers of any security vulnerabilities that have been discovered in their products and services and any recommended security patches, updates or mitigations.

A vulnerability disclosure program should include processes to receive, verify, resolve and report on security vulnerabilities disclosed by both internal and external sources. In support of this, a vulnerability disclosure policy should be made publicly available that covers:

- the purpose of the vulnerability disclosure program
- the types of security research that are allowed
- the types of security research that are not allowed
- how to report potential security vulnerabilities
- the actions that will be taken on receiving notification of potential security vulnerabilities and indicative timeframes for these actions
- any expectations regarding the public disclosure of verified security vulnerabilities
- any recognition finders of verified security vulnerabilities will receive.

Finally, the Australian Cyber Security Centre (ACSC) encourages security researchers, customers and members of the public to responsibility report security vulnerabilities directly with organisations, vendors and service providers. However, the ACSC recognises that this is not always practical, initial attempts at communication may be unsuccessful or the person making the report may not wish to do so directly. In such cases, security vulnerabilities can be reported to the ACSC as an independent coordinator at https://www.cyber.gov.au/acsc/report.

Security Control: 1616; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
A vulnerability disclosure program is implemented to assist with the secure development and maintenance of products and services.

Further information

An example of a secure development life cycle model, known as the Trustworthy Computing Security Development Lifecycle, is available at https://docs.microsoft.com/en-au/previous-versions/ms995349(v=msdn.10).

Further information on secure coding practices is available at https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21274.

Further information on implementing a vulnerability disclosure program can be found in:

- Google's ***Starting a Vulnerability Disclosure Program*** at https://developers.google.com/android/play-protect/starting-a-vdp
- European Union Agency for Cybersecurity's ***Good Practice Guide on Vulnerability Disclosure*** at https://www.enisa.europa.eu/publications/vulnerability-disclosure

- Netherland's National Cyber Security Centre's ***Coordinated Vulnerability Disclosure: The Guideline*** at https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
- Carnegie Mellon University's ***The CERT Guide to Coordinated Vulnerability Disclosure*** at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 29147:2018, ***Information technology – Security techniques – Vulnerability disclosure***, at https://www.iso.org/standard/72311.html
- ISO/IEC 30111:2019, ***Information technology – Security techniques – Vulnerability handling processes***, at https://www.iso.org/standard/69725.html.

Web application development

Protecting web applications

Even when a web application only contains public information, there remains a need to protect the integrity and availability of the information processed by the web application and the system it is hosted on.

Web application frameworks

Web application frameworks can be leveraged by software developers to enhance the security of a web application while decreasing development time. These resources can assist software developers to securely implement complex components such as session management, input handling and cryptographic operations.

Security Control: 1239; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Robust web application frameworks are used to aid in the development of secure web applications.

Web application interactions

Hypertext Transfer Protocol Secure (HTTPS) is Hypertext Transfer Protocol (HTTP) using Transport Layer Security (TLS) encryption. The use of HTTPS for web applications ensures that not only are individuals' interactions with web applications kept confidential, but the integrity of their interactions are also maintained.

Security Control: 1552; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
All web application content is offered exclusively using HTTPS.

Web application input handling

Most web application security vulnerabilities are caused by the lack of secure input handling. It is essential that web applications do not trust any input such as the website address and its parameters, Hypertext Markup Language (HTML) form data, cookie values and request headers without validating or sanitising it. Examples of validation and sanitisation include:

- ensuring a telephone form field contains only numerals
- ensuring data used in a Structured Query Language query is sanitised properly
- ensuring Unicode input is handled appropriately.

Security Control: 1240; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Validation and/or sanitisation is performed on all input handled by a web application.

Web application output encoding

The likelihood of cross-site scripting and other content injection attacks can be reduced through the use of 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.

Security Control: 1241; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Output encoding is performed on all output produced by a web application.

Web browser-based security controls

Web browser-based security controls such as Content-Security-Policy, HTTP Strict Transport Security (HSTS) and X-Frame-Options can be leveraged by web applications to help protect themselves and their users. This is achieved via the use of security policy in response headers which users' web browsers apply according to the defined security policy. Since the security controls are applied via response headers, it makes it possible to apply the security controls to legacy or proprietary web applications where changes to the source code are impractical.

Security Control: 1424; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
Web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers.

Open Web Application Security Project

The Open Web Application Security Project (OWASP) provides a comprehensive resource to consult when developing web applications.

Security Control: 0971; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS
The OWASP Application Security Verification Standard is followed when developing web applications.

Further information

Further information on auditing of web applications can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Further information on implementing TLS can be found in the Transport Layer Security section of the ***Guidelines for Cryptography***.

Further information on web application security can be found in the following ACSC publications:

- ***Implementing Certificates, TLS and HTTPS*** at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-and-https
- ***Protecting Web Applications and Users*** at https://www.cyber.gov.au/acsc/view-all-content/publications/protecting-web-applications-and-users
- ***Securing Content Management Systems (CMS)*** at https://www.cyber.gov.au/acsc/view-all-content/publications/securing-content-management-systems.

Further information on web application security is available in the OWASP ***Application Security Verification Standard*** at https://wiki.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project.

Further information on common web application frameworks for different programming languages, including a comparison of their functionality, is available at https://en.wikipedia.org/wiki/Comparison_of_web_frameworks.

Guidelines for Database Systems

Database servers

Protecting database server contents

Database server contents can be protected from unauthorised access (e.g. by the physical theft of a database server or failure to sanitise database server hardware before disposal) through the use of encryption.

Security Control: 1425; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Hard disks of database servers are encrypted using full disk encryption.

Functional separation between database servers and web servers

Placing databases used by web applications on the same physical server as a web server can expose them to an increased possibility of compromise by an adversary.

Security Control: 1269; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database servers and web servers are functionally separated, physically or virtually.

Communications between database servers and web servers

Information communicated between database servers and web applications, especially over the internet, is susceptible to capture by an adversary.

Security Control: 1277; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Information communicated between database servers and web applications is encrypted.

Network environment

Placing database servers on the same network segment as an organisation's workstations and allowing them to communicate with other network resources exposes them to an increased possibility of compromise by an adversary. Alternatively, in cases where databases will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary security risk.

Security Control: 1270; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database servers that require network connectivity are placed on a different network segment to an organisation's workstations.

Security Control: 1271; Revision: 2; Updated: Jan-20; Applicability: O, P, S, TS
Network access controls are implemented to restrict database server communications to strictly defined network resources such as web servers, application servers and storage area networks.

Security Control: 1272; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
If only local access to a database is required, networking functionality of database management system (DBMS) software is disabled or directed to listen solely to the localhost interface.

Separation of production, test and development database servers

Using production database servers for test and development activities could result in accidental damage to their integrity or contents.

Security Control: 1273; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Test and development environments do not use the same database servers as production environments.

Further information

Further information on developing Standard Operating Environments for database servers can be found in the operating system hardening section of the ***Guidelines for System Hardening***.

Further information on patching operating systems of database servers can be found in the system patching section of the ***Guidelines for System Management***.

Further information on using cryptography can be found in the ***Guidelines for Cryptography***.

Database management system software

Temporary installation files and logs

DBMS software will often leave behind 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 passphrases in the clear, could provide valuable information to an adversary.

Security Control: 1245; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All temporary installation files and logs are removed after DBMS software has been installed.

Hardening and configuration

Poorly configured DBMS software could provide an opportunity for an adversary to gain unauthorised access to database content. To assist organisations in deploying DBMS software, vendors often provide guidance on how to securely configure their DBMS software. Furthermore, DBMS software is often installed with most features enabled by default.

Security Control: 1246; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DBMS software is configured according to vendor guidance.

Security Control: 1247; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DBMS software features, stored procedures, accounts and databases that are not required are disabled or removed.

Restricting privileges

If DBMS software operating as a local administrator or root account is compromised by an adversary, it can present a significant security risk to the underlying operating system.

DBMS software is also often capable of accessing files that it has read access to on the database server. For example, an adversary 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.

Security Control: 1249; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DBMS software is configured to run as a separate account with the minimum privileges needed to perform its functions.

Security Control: 1250; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The account under which DBMS software runs has limited access to non-essential areas of the database server's file system.

Security Control: 1251; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The ability of DBMS software to read local files from a server is disabled.

Database administrator accounts

DBMS software often comes pre-configured with default database administrator accounts and passphrases that are listed in vendor documentation. These default database administrator accounts should be disabled, renamed or have their passphrases changed.

When sharing database administrator accounts for the performance of administrative tasks, any actions undertaken will not be attributable to an individual database administrator. This can hinder investigations relating to an attempted, or successful, targeted cyber intrusion. Furthermore, database administrator accounts shared across different databases can exacerbate any compromise of a database administrator account by an adversary.

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.

Security Control: 1260; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Default database administrator accounts are disabled, renamed or have their passphrases changed.

Security Control: 1262; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Database administrators have unique and identifiable accounts.

Security Control: 1261; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database administrator accounts are not shared across different databases.

Security Control: 1263; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Database administrator accounts are used exclusively for administrative tasks, with standard database accounts used for general purpose interactions with databases.

Security Control: 1264; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Database administrator access is restricted to defined roles rather than accounts with default administrative permissions, or all permissions.

Further information

Further information on authenticating users can be found in the authentication hardening section of the ***Guidelines for System Hardening***.

Further information on patching DBMS software can be found in the system patching section of the ***Guidelines for System Management***.

Databases

Database register

Without knowledge of all the databases in an organisation, and the information they contain, an organisation will be unable to appropriately protect their assets.

Security Control: 1243; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
A database register is maintained and regularly audited.

Protecting database contents

Database contents can be protected from unauthorised copying and subsequent offline analysis by applying file-based access controls to database files.

Security Control: 1256; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
File-based access controls are applied to database files.

Protecting authentication credentials in databases

Storing authentication credentials such as usernames and passphrases as plaintext in databases poses a significant security risk. An adversary that manages to gain access to a database's contents could extract these authentication credentials to gain access to users' accounts. In addition, it is possible that a user could have reused a username and passphrase for their workstation posing an additional security risk.

Security Control: 1252; Revision: 3; Updated: Jun-19; Applicability: O, P, S, TS
Passphrases stored in databases are hashed with a uniquely salted Australian Signals Directorate Approved Cryptographic Algorithm.

Protecting database contents

Database administrators and database users should know the sensitivity or classification associated with a database and its contents to ensure that sufficient security controls are applied. In cases where all of a database's contents are the same sensitivity or classification an organisation may choose to classify the entire database at this level. Alternatively, in cases where a database's contents are of varying sensitivity or classification levels, and database users have differing levels of access to such information, an organisation may choose to apply classifications at a more granular level within the database.

Limiting database user's ability to access, insert, modify or remove content from databases based on their work duties ensures the need-to-know principle is applied and the likelihood of unauthorised modifications is reduced.

Security Control: 0393; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS
Databases and their contents are classified based on the sensitivity or classification of information that they contain.

Security Control: 1255; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Database users' ability to access, insert, modify and remove content in databases is restricted based on their work duties.

Security Control: 1268; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles.

Aggregation of database contents

Where concerns exist that the sum, or aggregation, of separate pieces of information from within databases could lead to an adversary determining more 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 adversary cannot access the sum of information components leading to the aggregated information.

Security Control: 1258; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Where concerns exist that the sum, or aggregation, of separate pieces of information from within databases could lead to a database user determining more sensitive or classified information, database views in combination with database user access roles are implemented.

Separation of production, test and development databases

Using information from production databases in test or development databases could result in inadequate protection being applied to the information.

Security Control: 1274; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Information in production databases is not used in testing or development databases unless the testing or development environments are secured to the same level as the production environment.

Web application interaction with databases

SQL injection is a significant threat to the confidentiality, integrity and availability of database contents. SQL injections can allow an adversary to steal information from databases, modify database contents, delete an entire database or even in some circumstances gain control of the underlying database server. Furthermore, when database queries from web applications fail they may display detailed error information about the database schema to users of the web application. This can be used by an adversary to tailor SQL injection attempts.

Security Control: 1275; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All queries to databases from web applications are filtered for legitimate content and correct syntax.

Security Control: 1276; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Parameterised queries or stored procedures are used for database interaction instead of dynamically generated queries.

Security Control: 1278; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Web applications are designed to provide as little error information as possible to users about database schemas.

Further information

Further information on logging and auditing of database events can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Guidelines for Email

Email usage

Email usage policy

There are many security risks associated with the use of email that are often overlooked by users. Documenting these security risks, and associated mitigations, in an email usage policy will inform users of precautions to take when using email.

Security Control: 0264; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
An email usage policy is developed and implemented.

Webmail services

When users access non-approved webmail services they are effectively bypassing email content filtering controls as well as other security controls that may have been implemented for an organisation's email gateways and servers. While web content filtering controls may mitigate some security risks (e.g. some forms of malicious attachments), they are unlikely to address specific security risks relating to emails (e.g. spoofed email contents).

Security Control: 0267; Revision: 7; Updated: Mar-19; Applicability: O, P, S, TS
Access to non-approved webmail services is blocked.

Protective markings for emails

Implementing protective markings for emails ensures that appropriate security controls are applied to information, and also helps to prevent unauthorised information being released into the public domain. In doing so, it is important that protective markings accurately reflect the information in the subject, body and attachments of emails.

Security Control: 0270; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
Protective markings are applied to emails and reflect the information in their subject, body and attachments.

Protective marking tools

Requiring user involvement in the marking of emails ensures a conscious decision by users, thereby lessening the chance of incorrectly marked emails. In addition, allowing users to select only protective markings for which a system is authorised to process, store or communicate lessens the chance of users inadvertently over-classifying an email. This also serves to remind users of the maximum sensitivity or classification of information permitted on a system.

Email content filters may only check the most recent protective marking applied to an email. Therefore, when users are responding to or forwarding an email, requiring a protective marking which is at least as high as that of the email they received will help email content filters prevent emails being sent to systems that are not authorised to handle the original sensitivity or classification of the email.

Security Control: 0271; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Protective marking tools do not automatically insert protective markings into emails.

Security Control: 0272; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS
Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.

Security Control: 1089; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS
Protective marking tools do not allow users replying to or forwarding an email to select a protective marking that is lower than previously used for the email.

Handling emails with inappropriate, invalid or missing protective markings

It is important that email servers are configured to block emails with inappropriate protective markings. For example, blocking inbound and outbound emails with a protective marking higher than the sensitivity or classification of the receiving system will prevent a data spill from occurring. In doing so, it is important to inform recipients of blocked inbound emails, and the sender of blocked outbound emails, that this has occurred.

If an email is received with an invalid or missing protective marking it may still be passed to its intended recipients; however, the recipients will have an obligation to determine the appropriate protective marking for the email if it is to be responded to, forwarded or printed. If unsure, the sender of the original email should be contacted to seek clarification of handling requirements.

Security Control: 0565; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS
Email servers are configured to block, log and report emails with inappropriate protective markings.

Security Control: 1023; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
The intended recipients of any blocked inbound emails, and the sender of any blocked outbound emails, are notified.

Email distribution lists

Often the membership and nationality of members of email distribution lists is unknown. Therefore, users sending emails with Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or Releasable To (REL) information to distribution lists could accidentally cause a data spill.

Security Control: 0269; Revision: 3; Updated: Sep-20; Applicability: S, TS
Emails containing AUSTEO, AGAO or REL 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.

Further information

Further information on the Australian Government's email protective marking standard can be found in the Attorney-General's Department's ***Protective Security Policy Framework***, ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.

Email gateways and servers

Centralised email gateways

Without a centralised email gateway it is difficult to deploy Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and protective marking checks.

Security Control: 0569; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Email is routed through a centralised email gateway.

Security Control: 0571; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
When users send email from outside their network, an authenticated and encrypted channel is configured to allow email to be routed via a centralised email gateway.

Email gateway maintenance activities

An adversary will often avoid using an organisation's primary email gateway when sending malicious emails. This is because backup and alternative email gateways are often poorly maintained in terms of patches and email content filtering controls. As such, it is important that extra effort is made to ensure that backup and alternative email gateways are maintained to the same standard as the primary email gateway.

Security Control: 0570; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Where backup or alternative email gateways are in place, they are maintained at the same standard as the primary email gateway.

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 that email server. Such configurations are highly undesirable as spammers and worms can exploit them.

Security Control: 0567; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS
Email servers only relay emails destined for or originating from their domains.

Email server transport encryption

Emails can be intercepted anywhere between originating email servers and destination email servers. Enabling Transport Layer Security (TLS) on email servers will mitigate the compromise of email traffic, with the exception of cryptanalysis of email traffic.

Implementing Internet Engineering Task Force (IETF) Request for Comments (RFC) 3207 can protect email traffic while ensuring email servers remain compatible with other email servers due to the use of opportunistic TLS encryption.

Opportunistic TLS for email is susceptible to downgrade attacks. Mail Transfer Agent Strict Transport Security (MTA-STS) allows domain owners to indicate to other email servers that emails should only be sent if satisfactory TLS encryption is negotiated prior to transfer.

Implementing IETF RFC 8461 reduces the opportunity for downgrade attacks during email transfer and provides email server operators with visibility when downgrade attacks are attempted. IETF RFC 8460 supports the implementation of IETF RFC 8461 by providing a mechanism for a domain owner to publish a location where other email server operators can submit reports about their success or failure trying to initiate encrypted sessions when sending email to the specified domain.

Security Control: 0572; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Opportunistic TLS encryption, as defined in IETF RFC 3207, is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.

Security Control: 1589; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
MTA-STS, as defined in IETF RFC 8461, is enabled to prevent the transfer of unencrypted emails between complying servers.

Sender Policy Framework

SPF aids in the detection of spoofed emails by specifying a list of domains that are allowed to send emails. If an email server is not in the SPF record for a domain, SPF verification will fail.

Security Control: 0574; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
SPF is used to specify authorised email services (or lack thereof) for all domains.

Security Control: 1183; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
A hard fail SPF record is used when specifying email servers.

Security Control: 1151; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
SPF is used to verify the authenticity of incoming emails.

Security Control: 1152; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Incoming emails that fail SPF checks are blocked or marked in a manner that is visible to the recipients.

DomainKeys Identified Mail

DKIM enables the detection of spoofed email contents. This is achieved by DKIM records specifying the public key used to sign an email's contents. Specifically, if the signed digest in the email header does not match the signed contents of the email, verification will fail.

Security Control: 0861; Revision: 2; Updated: Mar-19; Applicability: O, P, S, TS
DKIM signing is enabled on emails originating from an organisation's domains.

Security Control: 1026; Revision: 5; Updated: Jan-20; Applicability: O, P, S, TS
DKIM signatures on received emails are verified.

Security Control: 1027; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Email distribution list software used by external senders is configured such that it does not break the validity of the sender's DKIM signature.

Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (DMARC) enables a domain owner to specify what action receiving email servers should take if they receive an email that fails SPF or DKIM checks. This includes 'reject' (the email is rejected), 'quarantine' (the email is marked as spam) or 'none' (no action is taken).

DMARC also provides a reporting feature which enables a domain owner to receive reports on the actions taken by receiving email servers. While this feature does not mitigate malicious emails sent to the domain owner's organisation, it can give the domain owner some visibility of attempts by adversaries to spoof their organisation's domains.

Security Control: 1540; Revision: 1; Updated: Oct-19; Applicability: O, P, S, TS
DMARC records are configured for all domains such that emails are rejected if they fail SPF or DKIM checks.

Email content filtering

Content filtering performed on email bodies and attachments provides a defence-in-depth approach to preventing malicious content being introduced into a network. Specific guidance on implementing email content filtering can be found in the Australian Cyber Security Centre (ACSC)'s ***Malicious Email Mitigation Strategies*** publication.

Security Control: 1234; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Email content filtering controls are implemented for email bodies and attachments.

Blocking suspicious emails

Blocking specific types of emails reduces the likelihood of phishing emails entering an organisation's network.

Security Control: 1502; Revision: 1; Updated: Mar-19; Applicability: O, P, S, TS
Emails arriving via an external connection where the source address uses an internal domain name are blocked at the email gateway.

Undeliverable messages

Undeliverable or bounce emails are commonly sent by receiving email servers when an 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 SPF, or other trusted means, avoids contributing to this problem and allows trusted parties to receive legitimate bounce messages.

Security Control: 1024; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS

Notification of undeliverable, bounced or blocked emails are only sent to senders that can be verified via SPF or other trusted means.

Further information

Further information on content filtering can be found in the content filtering section of the ***Guidelines for Gateways***.

Further information on email content filtering can be found in the ACSC's ***Malicious Email Mitigation Strategies*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/malicious-email-mitigation-strategies.

Further information on implementing SPF, DKIM and DMARC can be found in the ACSC's ***How to Combat Fake Emails*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/how-to-combat-fake-emails.

Further information on implementing opportunistic TLS encryption for email servers can be found in the ACSC's ***Implementing Certificates, TLS, HTTPS and Opportunistic TLS*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-https-and-opportunistic-tls.

Further information on engaging the services of email service providers for marketing or filtering purposes can be found in the ACSC's ***Marketing and Filtering Email Service Providers*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/marketing-and-filtering-email-service-providers.

Further information on opportunistic TLS encryption can be found in IETF RFC 3207 and its related update:

- IETF RFC 3207, ***SMTP Service Extension for Secure SMTP over Transport Layer Security***, at https://tools.ietf.org/html/rfc3207
- IETF RFC 7817, ***Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols***, at https://tools.ietf.org/html/rfc7817.

Further information on MTA-STS and associated reporting can be found in IETF RFC 8461 and IETF RFC 8460:

- IETF RFC 8461, ***SMTP MTA Strict Transport Security (MTA-STS)***, at https://tools.ietf.org/html/rfc8461
- IETF RFC 8460, ***SMTP TLS Reporting***, at https://tools.ietf.org/html/rfc8460.

Further information on SPF can be found in IETF RFC 7208 and its related updates:

- IETF RFC 7208, ***Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1***, at https://tools.ietf.org/html/rfc7208
- IETF RFC 7372, ***Email Authentication Status Codes***, at https://tools.ietf.org/html/rfc7372
- IETF RFC 8553, ***DNS AttrLead Changes: Fixing Specifications That Use Underscored Node Names***, at https://tools.ietf.org/html/rfc8553
- IETF RFC 8616, ***Email Authentication for Internationalized Mail***, at https://tools.ietf.org/html/rfc8616.

Further information on DKIM can be found in IETF RFC 6376 and its related updates:

- IETF RFC 6376, ***DomainKeys Identified Mail (DKIM) Signatures***, at https://tools.ietf.org/html/rfc6376
- IETF RFC 8301, ***Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)***, at https://tools.ietf.org/html/rfc8301
- IETF RFC 8463, ***A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)***, at https://tools.ietf.org/html/rfc8463
- IETF RFC 8553, ***DNS AttrLead Changes: Fixing Specifications That Use Underscored Node Names***, at https://tools.ietf.org/html/rfc8553
- IETF RFC 8616, ***Email Authentication for Internationalized Mail***, at https://tools.ietf.org/html/rfc8616.

Further information on DMARC can be found in IETF RFC 7489 and its related updates:

- IETF RFC 7489, ***Domain-based Message Authentication, Reporting, and Conformance (DMARC)***, at https://tools.ietf.org/html/rfc7489
- IETF RFC 8553, ***DNS AttrLead Changes: Fixing Specifications That Use Underscored Node Names***, at https://tools.ietf.org/html/rfc8553
- IETF RFC 8616, ***Email Authentication for Internationalized Mail***, at https://tools.ietf.org/html/rfc8616.

Further information on email security is available from the National Institute of Standards and Technology (NIST):

- NIST Special Publication (SP) 800-45 Rev. 2, ***Guidelines on Electronic Mail Security***, at https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final
- NIST SP 800-177 Rev. 1, ***Trustworthy Email***, at https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/final
- NIST SP 1800-6, ***Domain Name System-Based Electronic Mail Security***, at https://www.nccoe.nist.gov/publication/1800-6/.

Guidelines for Networking

Network design and configuration

Network documentation

It is important that network documentation accurately depicts the current state of a network. This typically includes network devices such as firewalls, data diodes, intrusion detection and prevention systems, routers, switches, and critical servers and services. Furthermore, as this documentation could be used by an adversary to assist in compromising a network, it is important that it is appropriately protected.

Security Control: 0516; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Network documentation includes a high-level network diagram showing all connections into the network; a logical network diagram showing all network devices, critical servers and services; and the configuration of all network devices.

Security Control: 0518; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Network documentation is updated as network configuration changes are made and includes a 'current as at [date]' or equivalent statement.

Security Control: 1178; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Network documentation provided to a third party, or published in public tender documentation, only contains details necessary for other parties to undertake contractual services.

Network segmentation and segregation

Network segmentation and segregation is one of the most effective security controls to prevent an adversary from propagating through a network and accessing target information after they have gained initial access. Technologies to enforce network segmentation and segregation also contain logging functionality that can be valuable in detecting an intrusion and, in the event of a compromise, isolating compromised devices from the rest of a network.

Network segmentation and segregation involves separating a network into multiple functional network zones with a view to protecting important information and critical services. For example, one network zone may contain user workstations while another network zone contains authentication servers. Network segmentation and segregation also assists in the creation and maintenance of network access control lists.

Security Control: 1181; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Networks are divided into multiple functional network zones according to the sensitivity or criticality of information or services.

Security Control: 1577; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
Organisation networks are segregated from service provider networks.

Using Virtual Local Area Networks

Virtual Local Area Networks (VLANs) can be used to implement network segmentation and segregation as long as the networks are all official networks or all the same classification. In such cases, if a data spill occurs between the networks the impact will be lesser than if a data spill occurred between two networks of different classifications or between an official or classified network and public network infrastructure.

For the purposes of this section, Multiprotocol Label Switching is considered to be equivalent to VLANs and is subject to the same controls.

Security Control: 1532; Revision: 1; Updated: Aug-19; Applicability: O, P, S, TS
VLANs are not used to separate network traffic between official or classified networks and public network infrastructure.

Security Control: 0529; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
VLANs are not used to separate network traffic between official and classified networks, or networks of different classifications.

Security Control: 1364; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
VLANs belonging to different security domains are terminated on separate physical network interfaces.

Security Control: 0535; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
VLANs belonging to official and classified networks, or networks of different classifications, do not share VLAN trunks.

Security Control: 0530; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Network devices implementing VLANs are managed from the most trusted network.

Using Internet Protocol version 6

Internet Protocol version 6 (IPv6) functionality can introduce additional security risks to a network. As such, disabling IPv6 functionality until it is intended to be used will minimise the attack surface of the network and ensure that any IPv6 functionality that is not intended to be used cannot be exploited.

To aid in the transition from Internet Protocol version 4 (IPv4) to IPv6, numerous tunnelling protocols have been developed that are designed to allow interoperability between the protocols. Disabling IPv6 tunnelling protocols on network devices and ICT equipment that do not explicitly require such functionality will prevent an adversary bypassing traditional network defences by encapsulating IPv6 data inside IPv4 packets.

Stateless Address Autoconfiguration (SLAAC) is a method of stateless Internet Protocol (IP) address configuration in IPv6 networks. SLAAC reduces the ability of an organisation to maintain effective logs of IP address assignment on a network. For this reason, stateless IP addressing should be avoided.

Security Control: 0521; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
IPv6 functionality is disabled in dual-stack network devices and ICT equipment unless it is being used.

Security Control: 1186; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
IPv6 capable network security devices are used on IPv6 and dual-stack networks.

Security Control: 1428; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Unless explicitly required, IPv6 tunnelling is disabled on all network devices and ICT equipment.

Security Control: 1429; Revision: 2; Updated: Jan-20; Applicability: O, P, S, TS
IPv6 tunnelling is blocked by network security devices at externally-connected network boundaries.

Security Control: 1430; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Dynamically assigned IPv6 addresses are configured with Dynamic Host Configuration Protocol version 6 in a stateful manner with lease information stored in a centralised logging facility.

Network access controls

If an adversary has limited opportunities to connect to a network, they have limited opportunities to compromise that network. Network access controls 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 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 standard user workstations.

Security Control: 0520; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Network access controls are implemented on networks to prevent the connection of unauthorised network devices.

Security Control: 1182; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Network access controls are implemented to limit traffic within and between network segments to only those that are required for business purposes.

Network device register

Maintaining and regularly auditing a register of authorised network devices can assist in determining whether devices such as switches, routers, wireless access points and internet dongles on a network or connected directly to workstations are rogue or not. The use of automated discovery and mapping tools can assist in this process.

Security Control: 1301; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
A network device register is maintained and regularly audited.

Default accounts for network devices

Network devices can come pre-configured with default credentials. For example, wireless access points with an administrator account named 'admin' and a passphrase of 'admin' or 'password'. Ensuring default accounts are disabled, renamed or have their passphrase changed can assist in reducing the likelihood of their exploitation by an adversary.

Security Control: 1304; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Default accounts for network devices are disabled, renamed or have their passphrase changed.

Disabling unused physical ports on network devices

Disabling unused physical ports on network devices such as switches, routers and wireless access points reduces the opportunity for an adversary to connect to a network if they can gain physical access to network devices.

Security Control: 0534; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Unused physical ports on network devices are disabled.

Functional separation between servers

Implementing functional separation between servers can reduce the security risk that a server compromised by an adversary will pose an increased security risk to other servers.

Security Control: 0385; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Servers maintain effective functional separation with other servers allowing them to operate independently.

Security Control: 1479; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Servers minimise communications with other servers at both the network and file system level.

Management traffic

Implementing security measures specifically for management traffic provides another layer of defence on a network should an adversary find an opportunity to connect to that network. This also makes it more difficult for an adversary to enumerate a network.

Security Control: 1006; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Security measures are implemented to prevent unauthorised access to network management traffic.

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. Furthermore, changing all default SNMP community strings on network devices and limiting access to read-only access is strongly encouraged.

Security Control: 1311; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
SNMP version 1 and 2 are not used on networks.

Security Control: 1312; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All default SNMP community strings on network devices are changed and have write access disabled.

Using Network-based Intrusion Detection and Prevention Systems

A Network-based Intrusion Detection System (NIDS) or Network-based Intrusion Prevention System (NIPS), when configured correctly and supported by suitable processes and resources, can be an effective way of identifying and responding to known intrusion profiles.

In addition, generating alerts for information flows that contravene any rule in a firewall rule set can help security personnel respond to suspicious or malicious traffic entering a network due to a failure or configuration change to firewalls.

Security Control: 1028; Revision: 7; Updated: Aug-20; Applicability: O, P, S, TS
NIDS or NIPS are deployed in all gateways between an organisation's networks and other networks they do not manage.

Security Control: 1030; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
NIDS or NIPS in gateways are located immediately inside the outermost firewall and configured to generate a log entry, and an alert, for any information flows that contravene any rule in firewall rule sets.

Security Control: 1185; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When deploying NIDS or NIPS in non-internet gateways, they are configured to monitor unusual patterns of behaviour or traffic flows rather than internet-based communication protocol signatures.

Blocking anonymity network traffic

Inbound network connections from anonymity networks (such as Tor, Tor2web and I2P) to an organisation's internet-facing services can be used by adversaries for reconnaissance and malware delivery purposes with minimal risk of detection and attribution. As such, this traffic should be blocked provided it will not meaningfully impact accessibility for legitimate users. For example, some organisations might choose to support anonymous connections to their websites to cater for individuals who want to remain anonymous for privacy reasons. In such cases, it is suggested that traffic from anonymity networks be logged and monitored instead. Additionally, outbound network connections to anonymity networks can be used by malware for command and control or data exfiltration and should be blocked given they rarely have legitimate business uses.

Security Control: 1627; Revision: 0; Updated: Nov-20; Applicability: O, P, S, TS
Inbound network connections from anonymity networks to internet-facing services are blocked.

Security Control: 1628; Revision: 0; Updated: Nov-20; Applicability: O, P, S, TS
Outbound network connections to anonymity networks are blocked.

Further information

Further information on wireless networks can be found in the wireless networks section of these guidelines.

Further information on functional separation of servers using virtualisation can be found in the virtualisation hardening section of the ***Guidelines for System Hardening***.

Further information on implementing network segmentation and segregation for administration purposes can be found in the system administration section of the ***Guidelines for System Management***.

Further information on event logging and auditing can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Further information on gateways can be found in the ***Guidelines for Gateways***.

Further information on network segmentation and segregation can be found in the Australian Cyber Security Centre (ACSC)'s ***Implementing Network Segmentation and Segregation*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation.

Further information on network plans can be found in the United States' National Security Agency's ***Manageable Network Plan Guide (version 4.0)*** publication at https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/networks/manageable-network-plan.cfm.

Further information on blocking anonymity network traffic can be found in the ACSC's ***Defending Against the Malicious Use of the Tor Network*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/defending-against-malicious-use-tor-network.

Further information on Domain Name Systems can be found in the ACSC's ***Domain Name System Security for Domain Owners*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/domain-name-system-security-domain-owners and the ***Domain Name System Security for Domain Resolvers*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/domain-name-system-security-domain-resolvers.

Wireless networks

Choosing wireless access points

Wireless access points that have been certified against a Wi-Fi Alliance certification program provide an organisation with the assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points will prevent any problems on a wireless network.

Security Control: 1314; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All wireless access points are Wi-Fi Alliance certified.

Wireless networks for public access

When an organisation provides a wireless network for the general public, connecting such a wireless network to, or sharing infrastructure with, any other network creates an additional entry point for an adversary to target connected networks to steal information or disrupt services.

Security Control: 0536; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Wireless networks provided for the general public to access are segregated from all other networks.

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. Disabling the administrative interface for wireless network connections on wireless access points will assist in preventing unauthorised connections.

Security Control: 1315; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The administrative interface on wireless access points is disabled for wireless network connections.

Default Service Set Identifiers

Some wireless access points come with a default Service Set Identifier (SSID) which is used to identify a wireless network. As the default SSIDs of wireless access points are often documented in internet forums, along with default accounts and passphrases, it is important to change the default SSID of wireless access points.

When changing the default SSID, it is important that the new SSID does not bring undue attention to an organisation's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an organisation, the location of their premises or the functionality of the wireless network.

A method commonly recommended to lower the profile of a wireless network is disabling SSID broadcasting. While this ensures that the existence of the wireless networks is not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re-association requests. As such, it is easy to determine the SSID of the wireless network by capturing these requests and responses. By disabling SSID broadcasting, organisations will make it more difficult for users to connect to a wireless network. Furthermore, an adversary could configure a malicious wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network, thereby fooling users or devices into automatically connecting to the adversary's malicious wireless access point instead. In doing so, the adversary could steal authentication credentials in order to gain access to the legitimate wireless network. For these reasons, it is recommended organisations enable SSID broadcasting.

Security Control: 1316; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The default SSID of wireless access points is changed.

Security Control: 1317; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The SSID of a non-public wireless network is not readily associated with an organisation, the location of their premises or the functionality of the wireless network.

Security Control: 1318; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
SSID broadcasting is enabled on wireless networks.

Static addressing

Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a wireless network from being assigned a routable IP address. However, some adversaries 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.

Security Control: 1319; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Static addressing is not used for assigning IP addresses on wireless networks.

Media Access Control address filtering

Devices that connect to wireless networks generally have a unique Media Access Control (MAC) address. As such, it is possible to use MAC address filtering on wireless access points to restrict which devices can connect to a wireless network. While this approach will introduce a management overhead, it can prevent rogue devices from connecting to a wireless network. However, some adversaries will be able to determine valid MAC addresses of legitimate users already on a wireless network. Adversaries can then use this information to spoof valid MAC addresses and gain access to the wireless network. MAC address filtering introduces a management overhead without any tangible security benefit.

Security Control: 1320; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
MAC address filtering is not used to restrict which devices can connect to wireless networks.

802.1X authentication

When an organisation chooses to deploy a wireless network, a number of Extensible Authentication Protocol (EAP) methods that are supported by the Wi-Fi Protected Access 2 (WPA2) protocol can be chosen. These EAP methods include WPA2-Enterprise with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), WPA2-Enterprise with Extensible Authentication Protocol-Tunnelled Transport Layer Security or WPA2-Enterprise with Protected Extensible Authentication Protocol.

WPA2-Enterprise with EAP-TLS is considered one of the most secure EAP methods. Furthermore, due to its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and operating systems. 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 organisation to have established a PKI. This involves 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, the security advantages are significant.

Security Control: 1321; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
WPA2-Enterprise with EAP-TLS is used to perform mutual authentication for wireless networks.

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 RADIUS server that is used for authentication, authorisation and accounting purposes. To provide assurance that these elements have been implemented correctly, supplicants, authenticators and the authentication server should have completed an evaluation.

Security Control: 1322; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
Evaluated supplicants, authenticators and authentication servers are used in wireless networks.

Generating and issuing certificates for authentication

When issuing a certificate to a device in order to access a wireless network, organisations should be aware that it could be stolen by malicious code. Once compromised, the certificate could be used on other devices to gain unauthorised access to the wireless network it was issued for. Organisations should also be aware that in only issuing a certificate to a device, any actions taken by a user will only be attributable to a device and not a specific user.

When issuing a certificate to a user in order to access a wireless network, it can 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. Specifically, a user is more likely to notice a missing smart card and alert their security team, who are then able to revoke the credentials on the RADIUS server, which can minimise the time an adversary has access to the wireless network. In addition, to reduce the likelihood of a stolen smart card from being used to gain unauthorised access to a wireless network, multi-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.

Security Control: 1324; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
Certificates are generated using an evaluated certificate authority solution or hardware security module.

Security Control: 1323; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Both device and user certificates are required for accessing wireless networks.

Security Control: 1325; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS

Both device and user certificates for accessing wireless networks are not stored on the same device.

Security Control: 1326; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
User certificates for accessing wireless networks are issued on smart cards with access PINs.

Security Control: 1327; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
User or device certificates stored on devices accessing wireless networks are protected by encryption.

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, organisations can choose 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).

Security Control: 1330; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The PMK caching period is not 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 a RADIUS server. To protect credentials communicated between wireless access points and a RADIUS server, communications should be encapsulated with an additional layer of encryption.

Security Control: 1454; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Communications between wireless access points and a RADIUS server are encapsulated with an additional layer of encryption.

Encryption of wireless network traffic

As wireless networks are often capable of being accessed from outside the perimeter of secured spaces, all wireless network traffic should be encrypted. Depending on the sensitivity or classification of information being communicated, this may involve using an Australian Signals Directorate (ASD) Approved Cryptographic Protocol, an evaluated product or High Assurance Cryptographic Equipment.

Security Control: 1332; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS
ASD approved cryptography is used to protect the confidentiality and integrity of all wireless network traffic.

Interference between wireless networks

Where multiple wireless networks are deployed in close proximity, there is the potential for interference to impact the availability of a wireless network, especially when operating on commonly used 802.11b/g (2.4 GHz) default channels of 1 and 11. Sufficiently separating wireless networks through the use of frequency separation can help reduce this security risk. This can be achieved by using wireless networks that are configured to operate on channels that minimise overlapping frequencies or by using both 802.11b/g (2.4 GHz) channels and 802.11n (5 GHz) channels. It is important to note though, if implementing a mix of 2.4 GHz and 5 GHz channels, not all devices may be compatible with 802.11n and able to connect to 5 GHz channels.

Security Control: 1334; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Wireless networks implement sufficient frequency separation from other wireless networks.

Protecting management frames on wireless networks

An effective denial of service can be performed by exploiting unprotected management frames using inexpensive commercial hardware. The 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or denial of service activities. However, the 802.11w amendment specifically addresses the protection of management frames on wireless networks and should be enabled.

Security Control: 1335; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Wireless access points enable the use of the 802.11w amendment to protect management frames.

Wireless network footprint

Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power can be deployed to achieve the desired footprint. This has the benefit of providing service continuity should a wireless access point become unserviceable. In such a case, the output power of nearby wireless access points can be increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

In addition to minimising the output power of wireless access points to reduce the footprint of a wireless network, the use of Radio Frequency (RF) shielding can be used for an organisation's premises. While expensive, this will limit the wireless communications to areas under the control of an organisation. RF shielding on an organisation's premises has the added benefit of preventing the jamming of wireless networks from outside of the premises in which wireless networks are operating.

Security Control: 1338; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power are deployed to achieve the desired footprint.

Security Control: 1013; Revision: 5; Updated: Sep-18; Applicability: S, TS
The effective range of wireless communications outside an organisation's area of control is limited by implementing RF shielding on buildings in which wireless networks are used.

Further information

Further information on implementing segregation using VLANs can be found in the network design and configuration section of these guidelines.

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Further information on encryption for wireless networks can be found in the ***Guidelines for Cryptography***.

Information on Wi-Fi Alliance certification programs can be obtained from https://www.wi-fi.org/certification/programs.

Further information on EAP-TLS can be found in Internet Engineering Task Force Request for Comments 5216, ***The EAP-TLS Authentication Protocol***, at https://tools.ietf.org/html/rfc5216.

Service continuity for online services

Cloud-based hosting of online services

Using a cloud service provider can allow an organisation to build highly resilient online services due to the increased computing resources, bandwidth and multiple separate physical sites made available by the cloud provider. Organisations can achieve the same results using their own infrastructure; however, this may require significant upfront costs and may still result in a limited capability to scale dynamically to meet increased demand. In case of a denial-of-

service attack, cloud-based hosting can also provide segregation from self-hosted or other cloud hosted services ensuring that other systems, such as email services, are not affected.

Security Control: 1437; Revision: 3; Updated: Jun-20; Applicability: O, P
A cloud service provider is used for hosting online services.

Location policies for online services

When using cloud service providers, organisations will need to consider whether they should lock their information to specific regions or availability zones. In doing so, organisations that specify locking policies will have an expectation that their information won't be relocated to different regions or availability zones by the cloud service provider.

Security Control: 1578; Revision: 0; Updated: Jul-20; Applicability: O, P
Organisations are notified by cloud service providers of any change to configured regions or availability zones.

Availability planning and monitoring for online services

It is important that the connectivity between organisations and their cloud service providers meets organisational requirements for bandwidth, latency and reliability. To support this, organisations and cloud service providers should discuss and document any specific network requirements, performance characteristics or planned responses to availability failures, especially when requirements for high availability exist. This includes whether network connections between organisations and cloud service providers will use dedicated communication links, or connect over the internet, and whether any secondary communications links will provide sufficient capacity to maintain operational requirements should the primary communication link become unavailable.

Furthermore, capacity monitoring should be performed in order to manage workloads and monitor the health of online services. This can be achieved through continuous and real-time monitoring of metrics such as latency, jitter, packet loss, throughput and availability. In addition, feedback should be provided to cloud service providers when performance does not meet service level agreement targets. To assist with this, anomaly detection can be performed through network telemetry that is integrated into security monitoring tools.

Security Control: 1579; Revision: 0; Updated: Jul-20; Applicability: O, P
Cloud service providers' ability to dynamically scale resources due to a genuine spike in demand or a denial-of-service attack is tested as part of capacity planning processes.

Security Control: 1580; Revision: 0; Updated: Jul-20; Applicability: O, P
Where a high availability requirement exists, online services are architected to automatically transition between availability zones.

Security Control: 1441; Revision: 2; Updated: Jul-20; Applicability: O, P
Where a requirement for high availability exists, a denial of service mitigation service is used.

Security Control: 1581; Revision: 0; Updated: Jul-20; Applicability: O, P
Organisations perform continuous real-time monitoring of the availability of online services.

Using content delivery networks

Similar to cloud-based hosting, the use of content delivery networks (CDNs) and denial of service mitigation services can allow an organisation to create highly resilient online services by leveraging the large bandwidth, geographically dispersed hosting locations, traffic scrubbing and other security controls offered by CDN and denial of service mitigation service providers.

The use of CDNs is particularly effective when serving static, bandwidth intensive media such as images, sound or video files. However, the services offered by a CDN can include more than basic content hosting such as web response caching, load balancing, web application security controls or denial of service mitigations.

Care should be taken when configuring the use of a CDN or denial of service mitigation service to ensure that the IP address of the organisation's web server is not identifiable by an adversary as this could allow for protections to be bypassed. Additionally, appropriate network security controls should be applied to only allow communication between an organisation's server, the CDN or denial of service mitigation service provider and the authorised management environment.

Security Control: 1438; Revision: 1; Updated: Sep-18; Applicability: O, P
Where a high availability requirement exists for website hosting, CDNs that cache websites are used.

Security Control: 1439; Revision: 1; Updated: Sep-18; Applicability: O, P
If using a CDN, disclosing the IP address of the web server under the organisation's control (referred to as the origin server) is avoided and access to the origin server is restricted to the CDN and an authorised management network.

Denial of service strategies

Denial-of-service attacks are designed to disrupt or degrade online services such as website, email and Domain Name System services. To achieve this goal, adversaries may use a number of approaches to deny access to legitimate users of online services:

- using multiple computers to direct a large volume of unwanted network traffic at online services in an attempt to consume all available network bandwidth
- using multiple computers to direct tailored traffic at online services in an attempt to consume the processing resources of online services
- hijacking online services in an attempt to redirect legitimate users away from those services to other services that the adversary controls.

Although an organisation cannot avoid being targeted by denial-of-service attacks, there are a number of measures they can implement to prepare for and potentially reduce the impact if targeted. This includes engaging with their cloud service providers to identify the denial of service detection technologies that may be available for use. For example, real-time capacity reporting dashboards, that provide out-of-band and real-time alerts based on organisation-defined thresholds, can assist with the rapid identification of denial-of-service attacks. In addition, not all online services or functionality offered by an organisation may be business critical. Understanding what services can be offered with reduced functionality, deprioritised, disabled or lived without can help an organisation reduce or eliminate the impact on other more essential services or free up resources to respond to more critical services first.

Overall, preparing for denial-of-service attacks before they occur is by far the best strategy as it is very difficult to respond once they begin and efforts at this stage are unlikely to be effective.

Security Control: 1431; Revision: 2; Updated: Jul-20; Applicability: O, P
Denial-of-service attack prevention and mitigation strategies are discussed with cloud service providers, specifically:

- *their capacity to withstand denial-of-service attacks*
- *any costs likely to be incurred as a result of denial-of-service attacks*
- *thresholds for notification of denial-of-service attacks*
- *thresholds for turning off online services during denial-of-service attacks*
- *pre-approved actions that can be undertaken during denial-of-service attacks*
- *denial-of-service attack prevention arrangements with upstream service providers to block malicious traffic as far upstream as possible.*

Security Control: 1458; Revision: 1; Updated: Sep-18; Applicability: O, P
The functionality and quality of online services, how to maintain such functionality, and what functionality can be lived without during a denial-of-service attack, are determined and documented.

Domain name registrar locking

The use of domain name registrar locking can prevent a denial of service caused by unauthorised deletion or transferal of a domain, or other unauthorised modification of a domain's registration details.

Security Control: 1432; Revision: 1; Updated: Sep-18; Applicability: O, P
Domain names for online services are protected via registrar locking and confirming domain registration details are correct.

Monitoring with real-time alerting for online services

Organisations should perform automated monitoring of online services with real-time alerting to ensure that a denial-of-service attack is detected and responded to as soon as possible.

Security Control: 1435; Revision: 1; Updated: Sep-18; Applicability: O, P
Availability monitoring with real-time alerting is implemented to detect denial-of-service attacks and measure their impact.

Segregation of critical online services

Denial-of-service attacks are typically focused on highly visible online services, such as an organisation's core website, in order to have a publicly noticeable impact. By segregating online services (e.g. having one internet connection for email and internet access and a separate connection for web hosting services) the impact of a denial-of-service attack can be limited to just a targeted service.

Security Control: 1436; Revision: 1; Updated: Sep-18; Applicability: O, P
Critical online services are segregated from other online services that are more likely to be targeted.

Preparing for service continuity

Depending on the nature of a denial-of-service attack, replacing a full-featured website with a minimal impact static version can help provide a level of service or information which would otherwise not be possible.

An organisation's standard full-featured website may have higher processing or resource demands due to database integration or the presence of large media files such as high-resolution images or videos. These additional resource requirements may make the website more susceptible to denial-of-service attacks.

Security Control: 1518; Revision: 0; Updated: Sep-18; Applicability: O, P
A static version of a website is pre-prepared that requires minimal processing and bandwidth in order to facilitate at least a basic level of service when under a denial-of-service attack.

Further information

Further information on mitigating denial-of-service attacks can be found in the ACSC's ***Preparing for and Responding to Denial-of-Service Attacks*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/preparing-and-responding-denial-service-attacks.

Guidelines for Cryptography

Cryptographic fundamentals

Purpose of cryptography

The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of information. Confidentiality protects information by making it unreadable to all but authorised users, integrity protects information from accidental or deliberate manipulation, authentication ensures that a person or entity is who they claim to be, and non-repudiation provides proof that a user performed an action and prevents them from denying that they did so.

Using encryption

Encryption of data at rest can be used to reduce the physical storage and handling requirements for ICT equipment and media while encryption of data in transit can be used to provide protection for sensitive or classified information communicated over public network infrastructure.

When organisations use encryption for data at rest, or data in transit, they are not reducing the sensitivity or classification of information. However, as the information is encrypted, the consequences of the encrypted information being accessed by an adversary is considered to be less. Therefore, physical storage and handling requirements applied to the encrypted information can be reduced. As the sensitivity or classification of the unencrypted information does not change, additional layers of encryption cannot be used to further lower physical and handling requirements.

Additional cryptographic requirements

These guidelines describe the general use of cryptography. The Australian Signals Directorate (ASD) may specify additional requirements in consumer guides for cryptographic equipment or encryption software once they have completed an ASD Cryptographic Evaluation (ACE). Such requirements supplement these guidelines and where conflicts occur take precedence.

International standards for cryptographic modules

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2012, ***Information technology – Security techniques – Security requirements for cryptographic modules***, and ISO/IEC 24759:2017, ***Information technology – Security techniques – Test requirements for cryptographic modules***, are international standards for the design and validation of hardware and software cryptographic modules.

Federal Information Processing Standard (FIPS) 140-3, ***Security Requirements for Cryptographic Modules***, is a United States standard based upon ISO/IEC 19790:2012, ISO/IEC 24759:2017 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 180-140 series.

Where a cryptographic module's functionality has been validated under FIPS 140-2, FIPS 140-3 or ISO/IEC 19790:2012, ASD can at its discretion reduce the scope of an ACE.

High Assurance Cryptographic Equipment

High Assurance Cryptographic Equipment (HACE) is used by organisations to protect highly classified information. HACE is designed to lower the physical storage and handling requirements of highly classified information using cryptography. Due to the sensitive nature of HACE, and the limited information publicly available on it, organisations must contact the Australian Cyber Security Centre (ACSC) before using it.

Reducing physical storage and handling requirements

When encryption is applied to information it provides an additional layer of defence. Encryption does not change the sensitivity or classification of the information, but when encryption is used, the physical storage and handling requirements of ICT equipment and media may be reduced.

Security Control: 1161; Revision: 4; Updated: Sep-18; Applicability: O
Encryption software that implements an ASD Approved Cryptographic Algorithm (AACA) is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains sensitive information.

Security Control: 0457; Revision: 5; Updated: Sep-18; Applicability: P
Encryption software that has completed an ACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains classified information.

Security Control: 0460; Revision: 8; Updated: Sep-18; Applicability: S, TS
HACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains highly classified information.

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 files may be left in temporary locations used by an operating system.

Security Control: 0459; Revision: 3; Updated: Sep-18; Applicability: O, P
Encryption software used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.

Security Control: 0461; Revision: 5; Updated: Sep-18; Applicability: S, TS
HACE used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.

Encrypting particularly important information at rest

Due to the sensitivities associated with Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) information, this information needs to be encrypted when at rest.

Security Control: 1080; Revision: 2; Updated: Sep-18; Applicability: S, TS
In addition to any encryption already in place, an AACA is used to encrypt AUSTEO and AGAO information when at rest on a system.

Data recovery

The requirement for cryptographic equipment and encryption software to provide a key escrow function, where practical, was issued under a cabinet directive in July 1998.

Security Control: 0455; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Where practical, cryptographic equipment and encryption software provides 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 and media

When a user authenticates to encryption functionality for ICT equipment or media storing encrypted information, the encrypted information becomes accessible. At such a time, the ICT equipment or media should be handled according to

its original sensitivity or classification. Once the user deauthenticates from encryption functionality (e.g. shuts down a device, activates a lock screen) the ICT equipment or media can return to potentially being handled at a lower level.

Security Control: 0462; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
When a user authenticates to encryption functionality for ICT equipment or media storing encrypted information, it is treated in accordance with its original sensitivity or classification until such a time that the user deauthenticates from the encryption functionality.

Encrypting information in transit

Where insufficient physical security is provided for the protection of information communicated over network infrastructure or via wireless networks, encryption can be used to assist in protecting such information from compromise.

Security Control: 1162; Revision: 3; Updated: Sep-18; Applicability: O
Cryptographic equipment or encryption software that implements an ASD Approved Cryptographic Protocol (AACP) is used to communicate sensitive information over public network infrastructure and through unsecured spaces.

Security Control: 0465; Revision: 6; Updated: Sep-18; Applicability: P
Cryptographic equipment or encryption software that has completed an ACE is used to communicate classified information over official networks, public network infrastructure and through unsecured spaces.

Security Control: 0467; Revision: 8; Updated: Sep-18; Applicability: S, TS
HACE is used to communicate highly classified information over networks of a lower classification, official networks, public network infrastructure and through unsecured spaces.

Encrypting particularly important information in transit

Due to the sensitivities associated with AUSTEO and AGAO information, it needs to be encrypted when being communicated across network infrastructure.

Security Control: 0469; Revision: 3; Updated: Sep-18; Applicability: S, TS
In addition to any encryption already in place, an AACP is used to protect AUSTEO and AGAO information when communicated across network infrastructure.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Further information on the use of HACE can be found in Australian Communications Security Instructions (ACSIs). ACSIs include requirements for the approved use of HACE and can be provided to organisations by the ACSC upon request.

Further information on the storage and transfer of ICT equipment and media can be found in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Physical security for entity resources*** policy, at https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx.

Further information on the ACE program is available at https://www.cyber.gov.au/acsc/view-all-content/programs/asd-cryptographic-evaluation-program.

Further information on international standards for cryptographic modules and their evaluation can be found in:

- ISO/IEC 19790:2012, ***Information technology – Security techniques – Security requirements for cryptographic modules***, at https://www.iso.org/standard/52906.html
- ISO/IEC 24759:2017, ***Information technology – Security techniques – Test requirements for cryptographic modules***, at https://www.iso.org/standard/72515.html

- FIPS 140-3, ***Security Requirements for Cryptographic Modules***, at https://csrc.nist.gov/publications/detail/fips/140/3/final
- NIST SP 800-140, ***FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759***, at https://csrc.nist.gov/publications/detail/sp/800-140/final.

ASD Approved Cryptographic Algorithms

Evaluated cryptographic implementations

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

High assurance cryptographic algorithms, which are not covered in this section, can be used for the protection of highly classified information if they are suitably implemented in HACE. Further information on high assurance cryptographic algorithms can be obtained from the ACSC.

ASD Approved Cryptographic Algorithms

There is no guarantee of an algorithm's resistance against currently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. There have been some cases where theoretically impressive security 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 key exchange
- 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-2) (i.e. SHA-224, SHA-256, SHA-384 and SHA-512).

The approved symmetric encryption algorithms are Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and Triple Data Encryption Standard (3DES) using three distinct keys.

Where there is a range of key sizes for an algorithm, some of the smaller key sizes are not approved as they do not provide an adequate safety margin against possible future attacks. For example, advances in integer factorisation methods could render smaller RSA moduli vulnerable.

Using ASD Approved Cryptographic Algorithms

If cryptographic equipment or software implements unapproved algorithms, as well as AACAs, it is possible that these unapproved algorithms could be used without a user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, organisations can ensure that only the AACA can be used by disabling the unapproved algorithms (which is preferred) or advising users not to use the unapproved algorithms via usage policies.

Security Control: 0471; Revision: 6; Updated: Jun-20; Applicability: O, P
Only AACAs are used by cryptographic equipment and software.

Approved asymmetric/public key algorithms

DH and DSA are vulnerable to different attacks than ECDH and ECDSA. As a result, ECDH and ECDSA offer more effective security per bit increase. This leads to smaller data requirements which in turn means that elliptic curve variants have become de facto global standards. For reduced data cost, and to promote interoperability, ECDH and ECDSA should be used when possible.

Security Control: 0994; Revision: 5; Updated: Sep-18; Applicability: O, P
ECDH and ECDSA are used in preference to DH and DSA.

Using Diffie-Hellman

A modulus of 2048 bits for correctly implemented DH provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

When DH in a prime field is used, the prime modulus impacts the security of the algorithm. The security considerations when creating such a prime modulus can be found in NIST SP 800-56A Rev. 3, along with a collection of commonly used secure moduli.

Security Control: 0472; Revision: 5; Updated: Dec-20; Applicability: O, P
When using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used.

Security Control: 1629; Revision: 0; Updated: Dec-20; Applicability: O, P
When using DH for agreeing on encryption session keys, a modulus and associated parameters are selected according to NIST SP 800-56A Rev. 3.

Using the Digital Signature Algorithm

A modulus of 2048 bits for correctly implemented DSA provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

Security Control: 0473; Revision: 5; Updated: Dec-20; Applicability: O, P
When using DSA for digital signatures, a modulus of at least 2048 bits is used.

Security Control: 1630; Revision: 0; Updated: Dec-20; Applicability: O, P
When using DSA for digital signatures, a modulus and associated parameters are generated according to FIPS 186-4.

Using Elliptic Curve Cryptography

The curve used within an elliptic curve algorithm impacts the security of the algorithm. Only approved curves should be used.

Security Control: 1446; Revision: 1; Updated: Sep-18; Applicability: O, P
When using elliptic curve cryptography, a curve from FIPS 186-4 is used.

Using Elliptic Curve Diffie-Hellman

When using a curve from FIPS 186-4, a base point order and key size of at least 224 bits for correctly implemented ECDH provides 112 bits of effective security strength. Security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Security Control: 0474; Revision: 5; Updated: Dec-20; Applicability: O, P

When using ECDH for agreeing on encryption session keys, a base point order and key size of at least 224 bits is used.

Using the Elliptic Curve Digital Signature Algorithm

When using a curve from FIPS 186-4, a base point order and key size of 224 bits for correctly implemented ECDSA provides 112 bits of effective security strength. Security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Security Control: 0475; Revision: 5; Updated: Dec-20; Applicability: O, P
When using ECDSA for digital signatures, a base point order and key size of at least 224 bits is used.

Using Rivest-Shamir-Adleman

A modulus of 2048 bits for correctly implemented RSA provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

Security Control: 0476; Revision: 6; Updated: Dec-20; Applicability: O, P
When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 2048 bits is used.

Security Control: 0477; Revision: 6; Updated: Sep-18; Applicability: O, P
When using RSA for digital signatures, and for passing encryption session keys or similar keys, a key pair for passing encrypted session keys that is different from the key pair used for digital signatures is used.

Approved symmetric encryption algorithms

The use of Electronic Codebook Mode with block ciphers allows repeated patterns in plaintext to appear as repeated patterns in ciphertext. Most plaintext, including written language and formatted files, contains significant repeated patterns. As such, an adversary can use this to deduce possible meanings of ciphertext. The use of other modes such as Galois/Counter Mode, Cipher Block Chaining, Cipher Feedback or Output Feedback can prevent such attacks, although each has different properties which can make them inappropriate for certain use cases.

Security Control: 0479; Revision: 4; Updated: Sep-18; Applicability: O, P
Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.

Using the Triple Data Encryption Standard

Using three distinct keys for 3DES is deemed the only secure option for practical purposes. All other keying options are susceptible to attacks that reduce the security of 3DES and are therefore not deemed secure. Where practical, organisations should use an approved implementation of AES, instead of 3DES.

Security Control: 0480; Revision: 6; Updated: Sep-18; Applicability: O, P
3DES is used with three distinct keys.

Protecting highly classified information

ASD has approved the following cryptographic algorithms for the protection of highly classified information when used in an evaluated implementation.

Recommended algorithms and key sizes should be given preference in order to ensure interoperability with the Commercial National Security Algorithm (CNSA) Suite.

Purpose	Algorithm	Approved for SECRET	Approved for TOP SECRET	Recommended

Encryption	AES	AES-128 AES-192 AES-256	AES-256	AES-256
Hashing	SHA-2	SHA-256 SHA-384 SHA-512	SHA-384 SHA-512	SHA-384
Digital signatures	ECDSA	NIST P-256 NIST P-384 NIST P-521	NIST P-384 NIST P-521	NIST P-384
	RSA	3072 bit key or larger	3072 bit key or larger	3072 bit key
Key exchange	DH	3072 bit key or larger	3072 bit key or larger	3072 bit key
	ECDH	NIST P-256 NIST P-384 NIST P-521	NIST P-384 NIST P-521	NIST P-384
	RSA	3072 bit key or larger	3072 bit key or larger	3072 bit key

Security Control: 1232; Revision: 5; Updated: May-19; Applicability: S, TS
AACAs are used in an evaluated implementation.

Security Control: 1468; Revision: 5; Updated: Oct-19; Applicability: S, TS
Preference is given to using the CNSA Suite algorithms and key sizes.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

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 186-4, ***Digital Signature Standard (DSS)***, at https://csrc.nist.gov/publications/detail/fips/186/4/final.

Further information on ECDH can be found in:

- American National Standards Institute (ANSI) X9.63-2011 (R2017), ***Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-63-2011-R2017--2086_SAIG_ABA_ABA_5343/
- ANSI X9.42-2003 (R2013), ***Public Key Cryptography for the Financial Services Industry, Agreement of Symmetric Keys Using Discrete Logarithm Cryptography***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-42-2003-R2013--2071_SAIG_ABA_ABA_5311/
- NIST SP 800-56A Rev. 3, ***Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography***, at https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final.

Further information on ECDSA can be found in:

- ANSI X9.63-2011 (R2017), ***Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-63-2011-R2017--2086_SAIG_ABA_ABA_5343/
- ANSI X9.62-2005, ***Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-62-2005-2085_SAIG_ABA_ABA_5340/
- FIPS 186-4, ***Digital Signature Standard (DSS)***, at https://csrc.nist.gov/publications/detail/fips/186/4/final.

Further information on the CNSA Suite can be found in the ***CNSA Suite and Quantum Computing FAQ*** at https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm.

Further information on RSA can be found in Internet Engineering Task Force (IETF) Request for Comments (RFC) 8017, ***PKCS #1: RSA Cryptography Specifications Version 2.2***, at https://tools.ietf.org/html/rfc8017.

Further information on SHA can be found in FIPS 180-4, ***Secure Hash Standard (SHS)***, at https://csrc.nist.gov/publications/detail/fips/180/4/final.

Further information on AES can be found in FIPS 197, ***Advanced Encryption Standard (AES)***, at https://csrc.nist.gov/publications/detail/fips/197/final.

ASD Approved Cryptographic Protocols

Evaluated cryptographic implementations

Implementations of the protocols in this section need to undergo an ACE before they can be approved to protect classified information.

High assurance cryptographic protocols

High assurance cryptographic protocols, which are not covered in this section, can be used for the protection of highly classified information if they are suitably implemented in HACE. Further information on high assurance cryptographic protocols can be obtained from the ACSC.

ASD Approved Cryptographic Protocols

In general, ASD only approves the use of cryptographic equipment and software that has passed a formal evaluation. However, ASD approves the use of some cryptographic protocols even though their implementations in specific cryptographic equipment or software has not been formally evaluated by ASD. This approval is limited to cases where they are used in accordance with these guidelines.

The AACPs are:

- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)
- Wi-Fi Protected Access 2 (WPA2).

Using ASD Approved Cryptographic Protocols

If cryptographic equipment or software implements unapproved protocols, as well as AACPs, it is possible that these unapproved protocols could be used without a user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, organisations can ensure that only AACPs can be used by disabling unapproved protocols (which is preferred) or advising users not to use unapproved protocols via usage policies.

Security Control: 0481; Revision: 5; Updated: Jun-20; Applicability: O, P
Only AACPs are used by cryptographic equipment and software.

Further information

Further information on AACPs can be found in the found in the following sections of these guidelines.

Further information on the use of WPA2 in wireless networks can be found in the wireless networks section of the ***Guidelines for Networking***.

Further information on the OpenPGP Message Format can be found in IETF RFC 3156, ***MIME Security with OpenPGP***, at https://tools.ietf.org/html/rfc3156.

Transport Layer Security

Definitions

The terms Secure Sockets Layer (SSL) and TLS have traditionally been used interchangeably. However, as SSL 3.0 is no longer an AACP, instances of 'SSL' refer to SSL version 3.0 and below while 'TLS' refers to TLS 1.0 and beyond.

Using Transport Layer Security

The latest version of TLS is version 1.3, which was released in August 2018.

When using ICT equipment or software that implements TLS, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Security Control: 1139; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
Only the latest version of TLS is used.

Security Control: 1369; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
AES in Galois Counter Mode is used for symmetric encryption.

Security Control: 1370; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Only server-initiated secure renegotiation is used.

Security Control: 1372; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DH or ECDH is used for key establishment.

Security Control: 1448; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
When using DH or ECDH for key establishment, the ephemeral variant is used.

Security Control: 1373; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Anonymous DH is not used.

Security Control: 1374; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
SHA-2-based certificates are used.

Security Control: 1375; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
Cipher suites are configured to use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function.

Security Control: 1553; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
TLS compression is disabled.

Perfect Forward Secrecy

Using Perfect Forward Secrecy (PFS) reduces the impact of the compromise of a TLS session.

Security Control: 1453; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
PFS is used for TLS connections.

Further information

Further information on handling TLS traffic through gateways can be found in the web content filters section of the ***Guidelines for Gateways***.

Further information on the implementation of TLS for websites can be found in in the ACSC's ***Implementing Certificates, TLS and HTTPS*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-and-https.

Further information on TLS can be found in IETF RFC 8446 and its related updates:

- IETF RFC 8446, ***The Transport Layer Security (TLS) Protocol Version 1.3***, at https://tools.ietf.org/html/rfc8446
- IETF RFC 5705, ***Keying Material Exporters for Transport Layer Security (TLS)***, at https://tools.ietf.org/html/rfc5705
- IETF RFC 6066, ***Transport Layer Security (TLS) Extensions: Extension Definitions***, at https://tools.ietf.org/html/rfc6066.

Secure Shell

Using Secure Shell

When using ICT equipment or software that implements SSH, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Configuring Secure Shell

SSH version 1 was found to have a number of security vulnerabilities. As such, it was replaced by SSH version 2. A number of security risks also exist when SSH is configured in an insecure manner. For example, forwarding connections and access privileges, using host-based authentication, and permitting system administrator logins. The configuration settings below are based on OpenSSH. Organisations using other implementations of SSH should adapt these settings to suit their SSH implementation.

Security Control: 1506; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The use of SSH version 1 is disabled.

Security Control: 0484; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The configuration settings in the following table are implemented for the SSH daemon.

Configuration	*Description*
ListenAddress xxx.xxx.xxx.xxx	*On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces*

AllowTCPForwarding no	*Disable connection forwarding*
GatewayPorts no	*Disable gateway ports*
PermitRootLogin no	*Disable the ability to login directly as root*
HostbasedAuthentication no	*Disable host-based authentication*
IgnoreRhosts yes	*Disable rhosts-based authentication*
PermitEmptyPasswords no	*Do not allow empty passphrases*
Banner x	*Configure a suitable login banner*
LoginGraceTime xx	*Configure a login authentication timeout of no more than 60 seconds*
X11Forwarding no	*Disable X11 forwarding*

Authentication mechanisms

Public key-based authentication schemes offer stronger authentication than passphrase-based authentication schemes due to passphrases being more susceptible to guessing attacks. Therefore, if passphrases are used, counter-measures should be put in place to reduce the chance of a successful brute force attack.

Security Control: 0485; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Public key-based authentication is used for SSH connections.

Security Control: 1449; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
SSH private keys are protected with a passphrase or a key encryption key.

Automated remote access

If using logins without a passphrase for automated purposes, a number of security risks may arise, specifically:

- if access from unknown Internet Protocol (IP) addresses is not restricted, an adversary could automatically authenticate to systems without needing to know any passphrases
- 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 an adversary and a host
- if agent credential forwarding is enabled, an adversary could connect to the stored authentication credentials and use them to connect to other trusted hosts, or even intranet hosts if port forwarding has been allowed as well
- if X11 display remoting is not disabled, an adversary could gain control of displays as well as keyboard and mouse control functions
- if console access is allowed, every user who logs into the console could run programs that are normally restricted to authenticated users.

To assist in mitigating these security risks, it is essential that the 'forced command' option is used to specify what command is executed and parameter checked is enabled.

Security Control: 0487; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS

When using logins without a passphrase for automated purposes, the following are disabled:

- *access from IP addresses that do not require access*
- *port forwarding*
- *agent credential forwarding*
- *X11 display remoting*
- *console access.*

Security Control: 0488; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
If using remote access without the use of a passphrase, the 'forced command' option is used to specify what command is executed and parameter checked is enabled.

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 requests the user's passphrase 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 a long period of time. Furthermore, to limit the exposure of credentials, agent credential forwarding should only be enabled when SSH traversal is required.

Security Control: 0489; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
When SSH-agent or other similar key caching programs are used, it is only on workstations and servers with screen locks, key caches are set to expire within four hours of inactivity, and agent credential forwarding is enabled only when SSH traversal is required.

Further information

Further information on SSH can be found in IETF RFC 4252 and its updates:

- IETF RFC 4252, ***The Secure Shell (SSH) Authentication Protocol***, at https://tools.ietf.org/html/rfc4252
- IETF RFC 8308, ***Extension Negotiation in the Secure Shell (SSH) Protocol***, at https://tools.ietf.org/html/rfc8308
- IETF RFC 8332, ***Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol***, at https://tools.ietf.org/html/rfc8332.

Further information on configuring OpenSSH can be found at https://www.openssh.com/manual.html and https://man.openbsd.org/sshd_config.

Secure/Multipurpose Internet Mail Extension

Using Secure/Multipurpose Internet Mail Extension

S/MIME 2.0 required the use of weaker cryptography (40-bit keys) than is approved for use in these guidelines. Version 3.0 was the first version to become an IETF standard.

Organisations choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and attachments for inappropriate content, and for server-based antivirus software to scan for viruses and other malicious code.

When using ICT equipment or software that implements S/MIME, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Security Control: 0490; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS

Versions of S/MIME earlier than 3.0 are not used.

Further information

Further information on S/MIME can be found in IETF RFC 8551, ***Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification***, at https://tools.ietf.org/html/rfc8551.

Internet Protocol Security

Using Internet Protocol Security

When using ICT equipment or software that implements IPsec, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Internet Security Association Key Management Protocol authentication

Most IPsec implementations handle a number of methods for authentication as part of Internet Security Association Key Management Protocol (ISAKMP). These can include digital certificates, encrypted nonces or pre-shared keys. These methods are all considered suitable for use.

Mode of operation

IPsec can be operated in transport mode or tunnel mode. 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.

Security Control: 0494; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.

Protocol selection

IPsec contains two major protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). 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. However, if 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.

Security Control: 0496; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The ESP protocol is used for IPsec connections.

Key exchange

There are several methods for establishing shared keying material for an IPsec connection, including manual keying and Internet Key Exchange (IKE) version 1 and 2. IKE addresses a number of security risks associated with manual keying, and for this reason is the preferred method for key establishment.

Security Control: 1233; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
IKE is used for key exchange when establishing an IPsec connection.

Internet Security Association Key Management Protocol modes

ISAKMP main mode provides greater security than aggressive mode since all exchanges are protected.

Security Control: 0497; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
If using ISAKMP in IKE version 1, aggressive mode is disabled.

Security association lifetimes

Using a secure association lifetime of four hours, or 14400 seconds, provides a balance between security and usability.

Security Control: 0498; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
A security association lifetime of less than four hours, or 14400 seconds, is used.

Hashed Message Authentication Code algorithms

The approved Hashed Message Authentication Code (HMAC) algorithms are HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512.

Security Control: 0998; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 is used as a HMAC algorithm.

Diffie-Hellman groups

Using a larger DH group provides more security for the key exchange. The minimum modulus size needed is specified in the ASD Approved Cryptographic Algorithms section of these guidelines.

Security Control: 0999; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
The largest modulus size possible for all relevant components in the network is used when conducting a key exchange.

Perfect Forward Secrecy

Using PFS reduces the impact of the compromise of a security association.

Security Control: 1000; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
PFS is used for IPsec connections.

Internet Key Exchange Extended Authentication

XAuth using IKE version 1 has documented security vulnerabilities associated with its use.

Security Control: 1001; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The use of XAuth is disabled for IPsec connections using IKE version 1.

Further information

Further information on IPsec can be found in IETF RFC 4301 and its updates:

- IETF RFC 4301, ***Security Architecture for the Internet Protocol***, at https://tools.ietf.org/html/rfc4301
- IETF RFC 6040, ***Tunnelling of Explicit Congestion Notification***, at https://tools.ietf.org/html/rfc6040
- IETF RFC 7619, ***The NULL Authentication Method in the Internet Key Exchange Protocol Version 2 (IKEv2)***, at https://tools.ietf.org/html/rfc7619.

Cryptographic system management

Cryptographic systems

Cryptographic systems are comprised of cryptographic equipment and keying material. Where security controls for cryptographic systems are different to other systems, the variations are contained in this section.

Commercial grade cryptographic equipment

Transporting Commercial Grade Cryptographic Equipment (CGCE) in a keyed state may expose the keying material in it to potential compromise. Therefore, if CGCE is transported in a keyed state it should be done based on the sensitivity or classification of the keying material in it.

If CGCE or associated keying material is compromised or suspected of being compromised (e.g. stolen, lost, copied or communicated over the internet) then the confidentiality and integrity of previous and future communications may also be compromised.

Security Control: 0501; Revision: 4; Updated: Sep-18; Applicability: O, P
Keyed CGCE is transported based on the sensitivity or classification of the keying material in it.

Security Control: 0142; Revision: 3; Updated: Jun-19; Applicability: O, P
The compromise or suspected compromise of CGCE or associated keying material is reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs.

Security Control: 1091; Revision: 5; Updated: Jun-19; Applicability: O, P
Keying material is changed when compromised or suspected of being compromised.

High Assurance Cryptographic Equipment

HACE can be used by organisations to protect highly classified information. ACSI 53 E, ACSI 103 A, ACSI 105 B, ACSI 107 B, ACSI 173 A and equipment-specific doctrine outline the requirements that need to be complied with for the use of HACE.

Security Control: 0499; Revision: 8; Updated: Apr-19; Applicability: S, TS
ACSI 53 E, ACSI 103 A, ACSI 105 B, ACSI 107 B, ACSI 173 A and the latest equipment-specific doctrine is complied with when using HACE.

Storing cryptographic equipment

As cryptographic equipment can protect sensitive or classified information, additional physical security controls should be applied to its storage.

Security Control: 0505; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Cryptographic equipment is stored in a room that meets the requirements for a server room based on the sensitivity or classification of the information the cryptographic equipment processes.

Security Control: 0506; Revision: 3; Updated: Sep-18; Applicability: S, TS
Areas in which HACE is used are separated from other areas and designated as a cryptographic controlled area.

Further information

Further information on the use of HACE can be found in associated ACSIs. ACSIs can be provided to organisations by the ACSC upon request.

Further information on Security Zones and secure rooms can be found in AGD's PSPF, ***Entity facilities*** policy, at https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx.

Guidelines for Gateways

Gateways

Purpose of gateways

Gateways act as information flow control mechanisms at the network layer and may also control information at the higher layers of the Open System Interconnect (OSI) model.

Deploying gateways

This section describes the security controls applicable to all gateways. Additional areas of these guidelines should also be consulted depending on the type of gateway deployed:

- For connections between different security domains, where at least one system is SECRET or higher, see the Cross Domain Solutions section of these guidelines.
- For devices used to control data flow in bi-directional gateways, see the firewalls section of these guidelines.

Applying the security controls

In all cases, gateways assumes the highest sensitivity or classification of the connected security domains.

Gateway architecture and configuration

Gateways are necessary to control data flows between security domains and prevent unauthorised access from external networks. Given the criticality of gateways in controlling the flow of information between security domains, any failure, particularly at higher classifications, may have serious consequences. As such, robust mechanisms for alerting personnel to situations that may cause cyber security incidents are especially important for gateways.

Security Control: 0628; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
All systems are protected from systems in other security domains by one or more gateways.

Security Control: 1192; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All connections between security domains implement mechanisms to inspect and filter data flows for the transport and higher layers as defined in the OSI model.

Security Control: 0631; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
Gateways:

- *are the only communications paths into and out of internal networks*
- *allow only explicitly authorised connections*
- *are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)*
- *log all physical and logical access to their components*
- *are configured to save logs to a secure logging facility*
- *have all security controls tested to verify their effectiveness after any changes to their configuration.*

Security Control: 1427; Revision: 2; Updated: Jun-19; Applicability: O, P, S, TS
Gateways implement ingress traffic filtering to detect and prevent Internet Protocol (IP) source address spoofing.

Gateway operation

Implementing logging and alerting capabilities for gateways can assist in detecting cyber security incidents, attempted intrusions and unusual usage patterns. In addition, storing event logs on a secure logging facility increases the difficulty for an adversary to delete logging information in order to destroy evidence of a targeted cyber intrusion.

Security Control: 0634; Revision: 7; Updated: Jun-19; Applicability: O, P, S, TS
All gateways connecting networks in different security domains are operated such that they:

- *log network traffic permitted through the gateway*
- *log network traffic attempting to leave the gateway*
- *are configured to save event logs to a secure logging facility*
- *provide real-time alerts for any cyber security incidents, attempted intrusions and unusual usage patterns.*

Demilitarised zones

Demilitarised zones are used to prevent direct access to information and services on internal networks. Organisations 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.

Security Control: 0637; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Demilitarised zones are used to broker access to services accessed by external entities, and mechanisms are applied to mediate internal and external access to less-trusted services hosted in these demilitarised zones.

Gateway testing

Testing security controls on gateways assists with understanding its security posture by determining the effectiveness of security controls. An adversary may be aware of regular testing activities. Therefore, performing testing at irregular intervals will reduce the likelihood that an adversary could exploit regular testing activities.

Security Control: 1037; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Gateways are subject to rigorous testing, performed at irregular intervals no more than six months apart, to determine the strength of security controls.

Gateway administration

Administrator privileges should be minimised and roles should be separated (e.g. separate network administration and security policy configuration roles) to minimise security risks posed by a malicious user with privileged access to a 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 Standard Operating Procedures or reference documents bound by a formal agreement.

The system owner of the highest security domain of connected security domains is responsible for protecting the most sensitive information, and as such is best placed to manage any shared components of gateways. However, in cases where multiple security domains from different organisations are connected to a gateway, it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected organisations.

Security Control: 0611; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS
Access to gateway administration functions is limited to the minimum roles and privileges to support the gateway securely.

Security Control: 0612; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
System administrators are formally trained to manage gateways.

Security Control: 1520; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
All system administrators of gateways are cleared to access the highest level of information communicated or processed by the gateway.

Security Control: 0613; Revision: 4; Updated: Sep-18; Applicability: S, TS
All system administrators of gateways that process Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) information are Australian nationals.

Security Control: 0616; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Roles for the administration of gateways are separated.

Security Control: 0629; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
For gateways between networks in different security domains, a formal arrangement exists whereby any shared components are managed by the system managers of the highest security domain or by a mutually agreed third party.

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 should formally agree to be active information stakeholders in other security domains to which they are connected via a gateway.

Security Control: 0607; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
Once connectivity is established, system owners become information stakeholders for all connected security domains.

Gateway authentication

Ensuring users and services are authenticated by gateways can reduce the likelihood of unauthorised access and provides an auditing capability to support the investigation of cyber security incidents.

Security Control: 0619; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Users and services accessing networks through gateways are authenticated.

Security Control: 0620; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Only users and services authenticated and authorised to a gateway can use the gateway.

Security Control: 1039; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used 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, by using 802.1X.

Security Control: 0622; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment accessing networks through gateways is authenticated.

Further information

Further information on topics covered in this section can be found in the following cyber security guidelines:

- ***Guidelines for Cyber Security Incidents***
- ***Guidelines for Physical Security***
- ***Guidelines for Evaluated Products***
- ***Guidelines for ICT Equipment***
- ***Guidelines for System Hardening***

- ***Guidelines for System Management***
- ***Guidelines for System Monitoring***
- ***Guidelines for Networking***
- ***Guidelines for Data Transfers***.

Further information on preventing IP source address spoofing can be found in ***Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*** at https://tools.ietf.org/html/bcp38.

Cross Domain Solutions

Introduction to cross domain security

A Cross Domain Solution (CDS) is a system comprising security-enforcing functions tailored to mitigate the specific security risks of accessing or transferring information between security domains. A CDS may be an integrated appliance or, more commonly, be composed of discrete technologies or sub-systems, with each sub-system consisting of hardware and/or software components.

This section describes the security controls applicable to a CDS and extends upon the security controls within the prior gateways section which are also applicable. Furthermore, the ***Guidelines for Data Transfers*** is also applicable to a CDS. Finally, additional sections of these guidelines should be consulted depending on the specific type of CDS deployed.

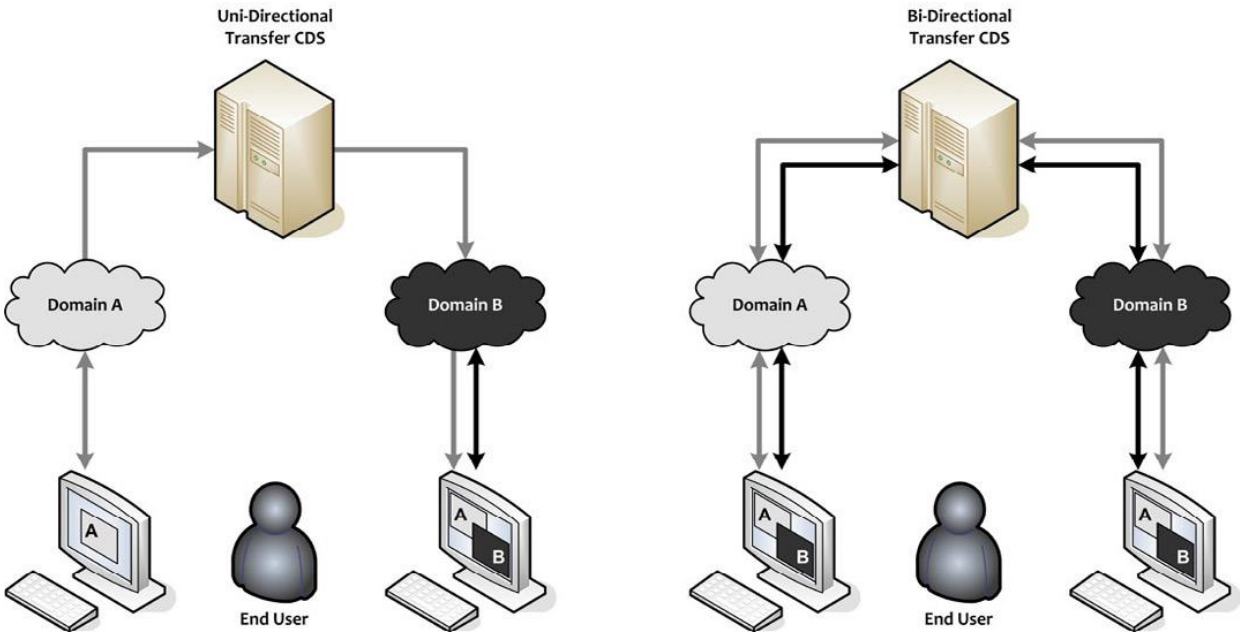
Personnel involved in the planning, analysis, design, implementation or assessment of a CDS should refer to the Australian Cyber Security Centre (ACSC)'s ***Introduction to Cross Domain Solutions*** and ***Fundamentals of Cross Domain Solutions*** publications.

Types of Cross Domain Solution

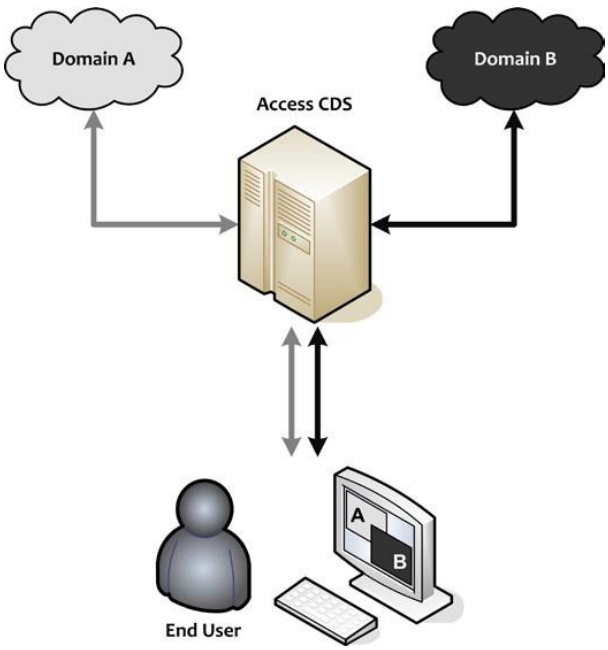
These guidelines define two logical types of CDS: a Transfer CDS and an Access CDS. These logical definitions are more closely aligned with how a CDS is described and sold by vendors and system integrators. Vendors may also offer a combined Access and Transfer solution.

Regardless of logical configuration, the underlying mechanisms in each CDS will consist of a low to high data transfer path, a high to low data transfer path, or both. Data filtering and other security controls are then applied to mitigate threats applicable to the system's operating context, including specific data paths and business cases.

A Transfer CDS facilitates the transfer of information, in one (unidirectional) or multiple (bi-directional) directions between different security domains.



An Access CDS provides the user with access to multiple security domains from a single device. Conceptually, an Access CDS allows remote interaction with one or multiple systems in a different security domain, such as a 'virtual desktop', and does not allow users to move data between security domains.



Applying the security controls

In all cases the gateway or CDS assumes the highest sensitivity or classification of the connected security domains.

When to implement a Cross Domain Solution

There are significant security risks associated with connecting highly classified systems to the internet or to a lower classified system. An adversary having control of, or access to, a gateway or CDS can invoke a serious security risk.

Security Control: 0626; Revision: 4; Updated: Sep-18; Applicability: S, TS
When connecting a highly classified network to any other network from a different security domain, a CDS is implemented.

Consultation when implementing or modifying a Cross Domain Solution

CDS environments can be complex to deploy and manage securely, as such, the likelihood of a network compromise is increased. Secure CDS implementations ensure that the security policy of each security domain involved is upheld in a robust manner across all physical and logical layers of the connection between domains.

Security Control: 0597; Revision: 6; Updated: Sep-18; Applicability: S, TS
When designing and deploying a CDS, the ACSC is notified and consulted; and directions provided by the ACSC are complied with.

Security Control: 0627; Revision: 5; Updated: Sep-18; Applicability: S, TS
When introducing additional connectivity to a CDS, such as adding a new gateway to a common network, the ACSC is consulted on the impact to the security of the CDS; and directions provided by the ACSC are complied with.

Separation of data flows

A CDS connecting highly classified systems to other potentially internet-connected systems should implement robust security enforcing functions, including content filtering and isolated paths, to ensure data flows are appropriately controlled.

Security Control: 0635; Revision: 5; Updated: Dec-19; Applicability: S, TS
A CDS between a highly classified network and any other network implements isolated upward and downward network paths.

Security Control: 1521; Revision: 1; Updated: Dec-19; Applicability: S, TS
A CDS between a highly classified network and any other network implements protocol breaks at each layer of the OSI model.

Security Control: 1522; Revision: 1; Updated: Dec-19; Applicability: S, TS
A CDS between a highly classified network and any other network implements content filtering and separate independent security-enforcing components for upward and downward data flows.

Event logging

In addition to the security controls listed in the event logging and auditing section of the ***Guidelines for System Monitoring***, a CDS should have comprehensive logging capabilities to establish accountability for all actions performed by users. Effective logging practices can increase the likelihood that unauthorised behaviour will be detected.

Due to the criticality of data import and export functions provided by a CDS, organisations should regularly assess the performance of a CDS's data transfer policies against the security policies the CDS has been deployed to enforce.

Security Control: 0670; Revision: 4; Updated: Sep-18; Applicability: S, TS
All security-relevant events generated by a CDS are logged and regularly analysed.

Security Control: 1523; Revision: 0; Updated: Sep-18; Applicability: S, TS
A representative sample of security events generated by a CDS, relating to the enforcement of data transfer policies, is taken at least every 3 months and assessed against the security policies that the CDS is responsible for enforcing between security domains.

User training

It is important that users know how to use a CDS securely. This can be achieved via training before access is granted, and reinforced by logon banners and awareness messages.

Security Control: 0610; Revision: 6; Updated: Apr-19; Applicability: O, P, S, TS
Users are trained on the secure use of a CDS before access to the CDS is granted.

Further information

Further information on topics covered in this section can be found in the following cyber security guidelines:

- ***Guidelines for Cyber Security Incidents***
- ***Guidelines for Physical Security***
- ***Guidelines for Evaluated Products***
- ***Guidelines for ICT Equipment***
- ***Guidelines for System Hardening***
- ***Guidelines for System Management***
- ***Guidelines for System Monitoring***
- ***Guidelines for Networking***
- ***Guidelines for Data Transfers***.

Further information on the basics of a CDS can be found in the ACSC's ***Introduction to Cross Domain Solutions*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/introduction-to-cross-domain-solutions.

Further information on the fundamentals of a CDS can be found in the ACSC's ***Fundamentals of Cross Domain Solutions*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/fundamentals-of-cross-domain-solutions.

Firewalls

Using firewalls

Where an organisation connects to another organisation, both organisations should implement a firewall in their gateway environment to protect themselves from intrusions that originate outside of their environment. This requirement may not be necessary in the specific cases where shared network infrastructure is used only as a transport medium and link encryption is used.

Security Control: 1528; Revision: 1; Updated: Apr-19; Applicability: O, P, S, TS
An evaluated firewall is used between official or classified networks and public network infrastructure.

Security Control: 0639; Revision: 8; Updated: Apr-19; Applicability: O, P, S, TS
An evaluated firewall is used between networks belonging to different security domains.

Security Control: 1194; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
The requirement to use a firewall as part of gateway infrastructure is met by both parties independently; shared ICT equipment does not satisfy the requirements of both parties.

Firewalls for particularly important networks

As AUSTEO and AGAO networks are particularly important, additional assurances should be put in place when connecting such networks to other networks.

Security Control: 0641; Revision: 7; Updated: Sep-18; Applicability: S, TS
In addition to the firewall between networks of different security domains, an evaluated firewall is used between an AUSTEO or AGAO network and a foreign network.

Security Control: 0642; Revision: 7; Updated: Sep-18; Applicability: S, TS
In addition to the firewall between networks of different security domains, an evaluated firewall is used between an AUSTEO or AGAO network and another Australian controlled network.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Diodes

Using 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 an adversary to use the same path to both launch a targeted cyber intrusion and exfiltrate information afterwards.

Security Control: 0643; Revision: 5; Updated: Sep-18; Applicability: O, P
An evaluated diode is used for controlling the data flow of unidirectional gateways between official or classified networks and public network infrastructure.

Security Control: 0645; Revision: 5; Updated: Sep-18; Applicability: S, TS
A high assurance diode is used for controlling the data flow of unidirectional gateways between classified networks and public network infrastructure.

Security Control: 1157; Revision: 3; Updated: Sep-18; Applicability: O, P
An evaluated diode is used for controlling the data flow of unidirectional gateways between official and classified networks.

Security Control: 1158; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
A high assurance diode is used for controlling the data flow of unidirectional gateways between official or classified networks where the highest system is SECRET or above.

Diodes for particularly important networks

While diodes between networks at the same classification are generally not needed, AUSTEO and AGAO networks require additional assurances to be put in place when connecting such networks to other networks.

Security Control: 0646; Revision: 4; Updated: Sep-18; Applicability: S, TS
An evaluated diode is used between an AUSTEO or AGAO network and a foreign network at the same classification.

Security Control: 0647; Revision: 6; Updated: Sep-18; Applicability: S, TS
An evaluated diode is used between an AUSTEO or AGAO network and another Australian 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 an organisation to potential malicious activity if the volume of data suddenly changes from the norm.

Security Control: 0648; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
A diode (or server connected to the diode) deployed to control data flow in unidirectional gateways monitors the volume of the data being transferred.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Web proxies

Web usage policy

If organisations allow users to access the web they should define the extent of access that is granted. This can be achieved through a web usage policy and education of users.

Security Control: 0258; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
A web usage policy is developed and implemented.

Using web proxies

Web proxies are a key component in enforcing web usage policies and preventing cyber security incidents.

Security Control: 0260; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
All web access, including that by internal servers, is conducted through a web proxy.

Web proxy authentication and logging

Thorough web proxy logs are a valuable asset when responding to cyber security incidents and user violation of web usage policies.

Security Control: 0261; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
A web proxy authenticates users and provides logging that includes the following details about websites accessed:

- *address (uniform resource locator)*
- *time/date*
- *user*
- *amount of data uploaded and downloaded*
- *internal and external IP addresses.*

Web content filters

Using web content filters

An effective web content filter greatly reduces the likelihood of malicious code infection or other inappropriate content from being accessed by users. Web content filters can also disrupt or prevent an adversary from communicating with their malicious code if deployed on an organisation's network.

Some forms of content filtering performed by web content filters are the same as those performed by other types of content filters, while other forms of content filtering are specific to web content filters.

Security Control: 0963; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
A web content filter is used to filter potentially harmful web-based content.

Security Control: 0961; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
Client-side active content, such as Java, is restricted to a list of allowed websites.

Security Control: 1237; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Web content filtering controls are applied to outbound web traffic where appropriate.

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, organisations can reduce this security risk by using TLS inspection.

Security Control: 0263; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
For TLS traffic communicated through internet gateways, either of the following approaches are implemented:

- *a solution that decrypts and inspects all TLS traffic as per content filtering security controls*
- *a list of websites to which encrypted connections are allowed, with all other TLS traffic decrypted and inspected as per content filtering security controls.*

Inspection of Transport Layer Security traffic

As encrypted TLS traffic may contain personal information, organisations are recommended to seek legal advice on whether inspecting such traffic could be in breach of the ***Privacy Act 1988***.

Security Control: 0996; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Legal advice is sought regarding the inspection of TLS traffic by internet gateways.

Allowing access to specific websites

Defining a list of allowed websites and blocking all other websites effectively removes one of the most common data delivery and exfiltration techniques used by an adversary. However, if users have a legitimate requirement to access numerous websites, or a rapidly changing list of websites, organisations should consider the costs of such an implementation.

Even a relatively permissive list of allowed websites offers better security than relying on a list of known malicious websites, or no restrictions at all, while still reducing implementation costs. An example of a permissive list could be the entire Australian subdomain, that is '*.au', or the top 1,000 websites from the Alexa website ranking (after filtering Dynamic Domain Name System domains and other inappropriate domains).

Security Control: 0958; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
A list of allowed websites, using either domain name or IP address, is implemented for all Hypertext Transfer Protocol (HTTP) and HTTPS traffic communicated through internet gateways.

Security Control: 1170; Revision: 3; Updated: Apr-20; Applicability: O, P, S, TS
If a list of allowed websites is not implemented, a list of allowed website categories is implemented instead.

Blocking access to specific websites

Collections of websites that have been deemed to be inappropriate due to their content or hosting of malicious content can be blocked to prevent them from being accessed.

Targeted cyber intrusions commonly use dynamic or other domains where domain names can be registered anonymously for free due to their lack of attribution.

Security Control: 0959; Revision: 6; Updated: Apr-20; Applicability: O, P, S, TS
If a list of allowed websites is not implemented, a list of blocked websites is implemented instead.

Security Control: 0960; Revision: 6; Updated: Apr-20; Applicability: O, P, S, TS
If a list of blocked websites is implemented, the list is updated on a daily basis to ensure that it remains effective.

Security Control: 1171; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS

Attempts to access a website through its IP address instead of through its domain name are blocked.

Security Control: 1236; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Dynamic domains and other domains where domain names can be registered anonymously for free are blocked.

Further information

Further information on content filtering techniques can be found in the content filtering section of these guidelines.

Examples of client-side JavaScript controls are available at https://noscript.net/.

Content filtering

Content filtering techniques

Content filters reduce the likelihood of unauthorised or malicious content transiting a security domain boundary by assessing data based on defined security policies. The following techniques can assist with assessing the suitability of 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 inappropriate or undesirable 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.
Verification against file specification	Verifies that the file conforms to the defined file specification and can be effectively processed by subsequent content filters.

Content filtering

Implementing an effective content filter which cannot be bypassed reduces the likelihood of malicious content successfully passing into a security domain. Content filtering is only effective when suitable components are selected and appropriately configured with consideration of an organisation's business processes and threat environment.

When content filters are protecting classified environments as a component of a CDS, their assurance requirements necessitate rigorous security testing.

Security Control: 0659; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
When importing data into a security domain, by any means including a CDS, the data is filtered by a content filter designed for that purpose.

Security Control: 1524; Revision: 1; Updated: Dec-19; Applicability: S, TS
Content filters deployed in a CDS are subject to rigorous security assessment to ensure they mitigate content-based threats and cannot be bypassed.

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.

Security Control: 0651; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
All suspicious, malicious and active content is blocked from entering a security domain.

Security Control: 0652; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Any data identified by a content filtering process as suspicious is blocked 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.

Security Control: 1389; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Email and web content entering a security domain is 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 an approved standard. For example, content validation can be used to identify malformed content thereby allowing potentially malicious content to be blocked.

Examples of content validation include:

- ensuring numeric fields only contain numeric numbers
- ensuring content falls within acceptable length boundaries

- ensuring Extensible Markup Language (XML) documents are compared to a strictly defined XML schema.

Security Control: 1284; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Content validation is performed on all data passing through a content filter with content which fails content validation blocked.

Content conversion and transformation

Content conversion or 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.

Examples of content conversion and transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a Portable Document Format (PDF) file
- converting a Microsoft PowerPoint presentation to a series of image files
- converting a Microsoft Excel spreadsheet to a comma-separated values 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 (e.g. archive files or encoded files embedded in XML) can increase the effectiveness of a content filter.

Security Control: 1286; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Content conversion is performed 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, will assist in mitigating the threat of content exploitation. Examples include:

- removal of document property information in Microsoft Office documents
- removal or renaming of JavaScript sections from PDF files
- removal of metadata from within image files.

Security Control: 1287; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Content sanitisation is performed on suitable file types if content conversion is not appropriate for data transiting a security domain boundary.

Antivirus scanning

Antivirus scanning is used to prevent, detect and remove malicious code that includes computer viruses, worms, Trojans, spyware and adware.

Security Control: 1288; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Antivirus scanning, using multiple different scanning engines, is performed on all content.

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 security risk due to processor, memory or disk space exhaustion. To limit the likelihood 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.

Security Control: 1289; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The contents from archive/container files are extracted and subjected to content filter checks.

Security Control: 1290; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Controlled inspection of archive/container files is performed to ensure that content filter performance or availability is not adversely affected.

Security Control: 1291; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Files that cannot be inspected are blocked and generate an alert or notification.

Allowing access to specific content types

Creating and enforcing a list of allowed content types, based on business requirements and the results of a risk assessment, is a strong content filtering method that can reduce the attack surface of a system. As a simple example, an email content filter might only allow Microsoft Office documents and PDF files.

Security Control: 0649; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
A list of allowed content types is implemented.

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 (e.g. by the addition or substitution of information). If content passing through a filter contains a form of integrity protection, such as a 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 DomainKeys Identified Mail
- a web service verifying the XML digital signature contained within a Simple Object Access Protocol request
- validating a file against a separately supplied hash
- checking that data to be exported from a security domain has been digitally signed by a release authority.

Security Control: 1292; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The integrity of content is verified where applicable and blocked if verification fails.

Security Control: 0677; Revision: 4; Updated: Sep-18; Applicability: S, TS
If data is signed, 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. Organisations should 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 security risk that malicious code's encrypted communications and data could move between security domains. In addition, encryption could mask information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill.

Where a business need to preserve the confidentiality of encrypted data exists, an organisation may consider a dedicated system to allow encrypted content through external, boundary or perimeter controls to be decrypted in an appropriately secure environment, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

Security Control: 1293; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
All encrypted content, traffic and data is decrypted and inspected to allow content filtering.

Peripheral switches

Using peripheral switches

When accessing different systems through a peripheral switch, it is important that sufficient assurance is held in the operation of the switch to ensure that information does not pass between different security domains. As such, the level of assurance needed in a peripheral switch is determined by the difference in sensitivity or classification of systems connected to the switch.

There is no requirement for an evaluated peripheral switch when all connected systems belong to the same security domain.

Security Control: 0591; Revision: 6; Updated: Sep-18; Applicability: O, P
An evaluated peripheral switch is used when sharing peripherals between official and classified systems.

Security Control: 1480; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
A high assurance peripheral switch is used when sharing peripherals between official or classified systems and highly classified systems.

Security Control: 1457; Revision: 2; Updated: Sep-18; Applicability: S, TS
An evaluated, preferably high assurance, peripheral switch is used when sharing peripherals between systems of different classifications.

Security Control: 0593; Revision: 9; Updated: Apr-19; Applicability: O, P, S, TS
An evaluated peripheral switch is used when sharing peripherals between official systems, or classified systems at the same classification, that belong to different security domains.

Peripheral switches for particularly important systems

As AUSTEO and AGAO systems are particularly important, additional assurances should be put in place when such systems share a peripheral switch with other systems.

Security Control: 0594; Revision: 4; Updated: Sep-18; Applicability: S, TS
An evaluated peripheral switch is used when accessing a system containing AUSTEO or AGAO information and a system of the same classification that is not authorised to process the same caveat.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Guidelines for Data Transfers

Data transfers

Data transfer process and procedures

Ensuring that a data transfer process, and supporting data transfer procedures, is adhered to will facilitate the consistent application of data transfer-related security controls and the generation of necessary audit records.

Security Control: 0663; Revision: 5; Updated: Aug-19; Applicability: O, P, S, TS
A data transfer process, and supporting data transfer procedures, is developed and implemented.

User responsibilities

When users transfer data to or from a system, they should understand the potential consequences of their actions. This could include spills of data onto a system not authorised to handle the data, or the unintended introduction of malicious code to a system. Accordingly, users should be held accountable for all data transfers that they make.

Security Control: 0661; Revision: 7; Updated: Apr-19; Applicability: O, P, S, TS
Users transferring data to and from a system are held accountable for the data they transfer.

Trusted sources

Trusted sources are people or systems responsible for authorising data exports based on a formal assessment. Trusted sources may include an organisation's Chief Information Security Officer (CISO) and their delegates.

Security Control: 0665; Revision: 5; Updated: Jun-20; Applicability: S, TS
Trusted sources are limited to people and systems that have been authorised as such by an organisation's CISO.

Data transfer approval

Users can prevent cyber security incidents by checking protective markings to ensure that the destination system is appropriate for the data being transferred, performing antivirus scanning on data to be transferred, and following all other procedures as part of the data transfer process.

Security Control: 0664; Revision: 5; Updated: Sep-18; Applicability: S, TS
All data transferred to a system of a lesser sensitivity or classification is reviewed and approved by a trusted source.

Security Control: 0675; Revision: 4; Updated: Jun-20; Applicability: S, TS
A trusted source signs all data authorised for export from a system.

Import of data

Scanning data being imported to a system for malicious and active content reduces the likelihood of the system being infected with malicious code.

Security Control: 0657; Revision: 4; Updated: Sep-18; Applicability: O, P
Data imported to a system is scanned for malicious and active content.

Security Control: 0658; Revision: 4; Updated: Sep-18; Applicability: S, TS
Data imported to a system is scanned for malicious and active content, undergoes data format checks and logging, and is monitored to detect overuse/unusual usage patterns.

Export of data

When data is exported from a system, protective markings should be assessed to determine if the export is permitted. Thorough inspection, the likelihood of data being transferred to a system that is not authorised to handle it, or into the public domain, can be reduced.

Security Control: 1187; Revision: 1; Updated: Sep-18; Applicability: O, P
When exporting data, protective marking checks are undertaken.

Security Control: 0669; Revision: 3; Updated: Sep-18; Applicability: S, TS
When exporting data, the following activities are undertaken:

- *protective marking checks*
- *data format checks and logging*
- *monitoring to detect overuse/unusual usage patterns*
- *limitations on data types and sizes*
- *keyword searches on all textual data.*

Preventing export of particularly important data to foreign systems

In order to reduce the likelihood of spilling Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) data onto foreign systems, it is important that a process, and supporting procedures, is developed to detect AUSTEO and AGAO data and to prevent it from crossing into foreign systems.

Security Control: 1535; Revision: 1; Updated: Aug-19; Applicability: S, TS
A process, and supporting procedures, is developed and implemented to prevent AUSTEO and AGAO data in both textual and non-textual formats from being exported to foreign systems.

Security Control: 0678; Revision: 2; Updated: Sep-18; Applicability: S, TS
When exporting data from an AUSTEO or AGAO system, keyword searches are undertaken on all textual data and any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator.

Monitoring data import and export

It is important to monitor data import and export processes to ensure the confidentiality and integrity of systems and data. This applies to all import and export mechanisms including those which are performed using a gateway, Cross Domain Solution or removable media. Data transfer logs can assist with such activities and may contain information such as who authorised the data transfer, what data was transferred, where the data was transferred from/to, when the data was transferred, why the data was transferred and how the data was transferred.

Security Control: 1586; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Data transfer logs are used to record all data imports and exports from systems.

Security Control: 1294; Revision: 3; Updated: Aug-20; Applicability: O, P
Data transfer logs are partially audited at least monthly.

Security Control: 0660; Revision: 7; Updated: Aug-20; Applicability: S, TS
Data transfer logs are fully audited at least monthly.

Further information

Further information on using removable media for data transfers can be found in the media usage section of the ***Guidelines for Media***.

Further information on data transfers involving a gateway or Cross Domain Solution can be found in the content filtering section of the ***Guidelines for Gateways***.

Cyber Security Terminology

Glossary of abbreviations

Abbreviation	Meaning
3DES	Triple Data Encryption Standard
AACA	ASD Approved Cryptographic Algorithm
AACP	ASD Approved Cryptographic Protocol
ACE	ASD Cryptographic Evaluation
ACSC	Australian Cyber Security Centre
ACSI	Australian Communications Security Instruction
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AGD	Attorney-General's Department
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
ANSI	American National Standards Institute
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ATA	Advanced Technology Attachment
AUSTEO	Australian Eyes Only
CCRA	Common Criteria Recognition Arrangement
CDN	content delivery network
CDS	Cross Domain Solution

CGCE	Commercial Grade Cryptographic Equipment
CISO	Chief Information Security Officer
CNSA	Commercial National Security Algorithm
DBMS	database management system
DH	Diffie-Hellman
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	electrically erasable programmable read-only memory
EMET	Enhanced Mitigation Experience Toolkit
EPROM	erasable programmable read-only memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HACE	High Assurance Cryptographic Equipment
HIPS	Host-based Intrusion Prevention System

HMAC	Hashed Message Authentication Code
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRAP	Information Security Registered Assessors Program
ISAKMP	Internet Security Association Key Management Protocol
ISM	Australian Government Information Security Manual
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MFD	multifunction device
mSATA	Mini-Serial Advanced Technology Attachment
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology

OSI	Open System Interconnect
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PFS	Perfect Forward Secrecy
PIN	personal identification number
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PP	Protection Profile
PSC	Protective Security Circular
PSPF	Protective Security Policy Framework
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RDP	Remote Desktop Protocol
REL	Releasable To
RF	Radio Frequency
RFC	Request for Comments
RSA	Rivest-Sharmir-Adleman
RTP	Real-time Traffic Protocol
SCEC	Security Construction and Equipment Committee
SEG	Security Equipment Guide
SHA-2	Secure Hashing Algorithm 2
SIP	Session Initiation Protocol

SLAAC	Stateless Address Autoconfiguration
S/MIME	Secure/Multipurpose Internet Mail Extension
SNMP	Simple Network Management Protocol
SOE	Standard Operating Environment
SP	Special Publication
SPF	Sender Policy Framework
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WPA2	Wi-Fi Protocol Access 2
XML	Extensible Markup Language

Glossary of cyber security terms

Term	Meaning
access control	The process of granting or denying requests for access to systems, applications and information. Can also refer to the process of granting or denying requests for access to facilities.
Access Cross Domain Solution	A system permitting access to multiple security domains from a single client device.
aggregation (of data)	A term used to describe compilations of information that may require a higher level of protection than their component parts.

application control	An approach in which only an explicitly defined set of trusted applications are allowed to execute on systems.
asset	Anything of value, such as ICT equipment, software or information.
attack surface	The amount of ICT equipment and software used in a system. The greater the attack surface the greater the chances of an adversary finding an exploitable security vulnerability.
audit log	A chronological record of system activities including records of system access and operations performed.
audit trail	A chronological record that reconstructs the sequence of activities surrounding, or leading to, a specific operation, procedure or event.
Australasian Information Security Evaluation Program	A program under which evaluations are performed by impartial bodies against the Common Criteria. The results of these evaluations are then certified by the Australian Cyber Security Centre (ACSC) which is responsible for the overall operation of the program.
Australian Eyes Only information	Information not to be passed to, or accessed by, foreign nationals.
Australian Government Access Only information	Information not to be passed to, or accessed by, foreign nationals, with the exception of seconded foreign nationals.
Australian Signals Directorate (ASD) Cryptographic Evaluation	The rigorous investigation, analysis, verification and validation of cryptographic functionality in products used to protect classified information.
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 Internet Protocol Security (IPsec) that provides data integrity and data origin authenticity but not confidentiality.
authorising officer	An executive with the authority to formally accept the security risks associated with the operation of a system and to authorise it to operate.

availability	The assurance that systems and information are accessible and useable by authorised entities when required.
biometrics	Measurable physical characteristics used to identify or verify an individual.
cascaded connections	Cascaded connections occur when one network is connected to another, which is then connected to another, and so on.
caveat	A marking that indicates that the information has special requirements in addition to those indicated by its classification. This term covers codewords, source codewords, releasability indicators and special-handling caveats.
certification report	An artefact of Common Criteria evaluations that outlines the outcomes of a product's 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 security controls and associated security risk management processes.
classification	The categorisation of systems and information according to the expected impact if it was to be compromised.
classified information	Information that would cause damage, serious damage or exceptionally grave damage to the national interest, organisations or individuals if compromised (i.e. information marked PROTECTED, SECRET or TOP SECRET).
classified system	A system that processes, stores or communications 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.
Commercial Grade Cryptographic Equipment	A subset of ICT equipment which contains cryptographic components.
Common Criteria	An international standard for product evaluations.

Common Criteria Recognition Arrangement	An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes.
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.
connection forwarding	The use of network address translation to allow a port on a node inside a 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	Specific configuration and usage guidance for products evaluated through the ASD Cryptographic Evaluation program or the High Assurance Evaluation program.
content filter	A filter that examines content to assess conformance against a security policy.
continuous monitoring plan	A document that describes the plan for the continuous monitoring and assurance in the effectiveness of security controls for a system.
control plane	The administrative interface that allows for the management and orchestration of a system's infrastructure and applications.
Cross Domain Solution	A 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 equipment	A generic term for Commercial Grade Cryptographic Equipment and High Assurance Cryptographic Equipment.

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 software	Software designed to perform cryptographic functions.
cryptographic system	A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates.
cyber resilience	The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents.
cyber security	Measures used to protect the confidentiality, integrity and availability of systems and information.
cyber security event	An occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
cyber security incident	An unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.
cyber threat	Any circumstance or event with the potential to harm systems or information.
data at rest	Information 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 information into an uncontrolled or unauthorised environment, or to people without a need-to-know.

declassification	A process whereby information is reduced to an OFFICIAL level 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.
demilitarised zone	A small network with one or more servers that is kept separate from the core network, typically on the outside of the firewall or as a separate network protected by the firewall. Demilitarised zones usually provide information to less trusted networks, such as the internet.
denial-of-service attack	An attempt by an adversary 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 server hosting the online service.
device access control software	Software that can be used on a system to restrict access to communications ports. Device access control software can block all access to a communications port or allow access based on device types, manufacturer's identification or even unique device identifiers.
digital preservation	The coordinated and ongoing set of processes and activities that ensure long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span the information is required.
digital signature	A cryptographic process that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.
diode	A device that allows data to flow in only one direction.
distributed-denial-of-service attack	A distributed form of denial-of-service attack.
dual-stack network device	ICT equipment that implements both Internet Protocol version 4 and Internet Protocol version 6 protocol stacks.

emanation security	The counter-measures employed to reduce classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of Radio Frequency energy, sound waves or optical signals.
Encapsulating Security Payload	A protocol used for encryption and authentication in IPsec.
encryption software	Software designed to ensure the confidentiality of data by encrypting it when at rest.
escort	A person who ensures that when maintenance or repairs are undertaken to ICT equipment that uncleared personnel are not exposed to information they are not authorised to access.
event	In the context of system logs, an event constitutes an evident change to the normal behaviour of a network, system or user.
facility	A physical space where business is performed. 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.
firewall	A network device that filters incoming and outgoing network data based on a series of rules.
firmware	Software embedded in ICT equipment.
fly lead	A lead that connects ICT equipment to the fixed infrastructure of a 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 managed by, or on behalf of, the Australian Government.
fuzzing	Fuzzing (or fuzz testing) is a method used to discover errors or potential security vulnerabilities in software.
gateway	Gateways securely manage data flows between connected networks from different security domains.

handling requirements	An agreed standard for the storage and dissemination of information to ensure its protection. This can include electronic information, paper-based information or media containing information.
hardware	A generic term for ICT equipment.
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 Cryptographic Equipment	Cryptographic equipment that has been designed and authorised for the protection of highly classified information.
High Assurance Evaluation	The rigorous investigation, analysis, verification and validation of products used to protect highly classified information.
high assurance ICT equipment	ICT equipment that has been designed and authorised for the protection of highly classified information.
highly classified information	Information that would cause serious damage or exceptionally grave damage to the national interest, organisations or individuals if compromised (i.e. information marked SECRET or TOP SECRET).
highly classified system	A system that processes, stores or communicates highly classified information.
Host-based Intrusion Detection System	Software, resident on a system, which monitors system activities for malicious or unwanted behaviour.
Host-based Intrusion Prevention System	Software, resident on a system, which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities.
hybrid hard drive	Non-volatile magnetic media that uses a cache to increase read/write speeds and reduce boot times. The cache is normally non-volatile flash memory media.
ICT equipment	Any device that can process, store or communicate electronic information (e.g. computers, multifunction devices, mobile phones, digital cameras, electronic storage media and other radio devices).

incident response plan	A document that describes the plan for responding to cyber security incidents.
Information Security Registered Assessors Program	An initiative of the ACSC designed to register suitably qualified individuals to carry out security assessments for systems.
infrared device	Devices such as mice, keyboards and pointing devices that have an infrared communications capability.
integrity	The assurance that information has been created, amended or deleted only by authorised individuals.
interactive authentication	Authentication that involves the interaction of a person with a system.
Internet Protocol Security	A suite of protocols for secure communications through authentication or encryption of Internet Protocol (IP) packets as well as including protocols for cryptographic key establishment.
Internet Protocol telephony	The transport of telephone calls over IP networks.
Internet Protocol version 6	A protocol used for communicating over packet switched networks. Version 6 is the successor to version 4 which is widely used on the internet.
Intrusion Detection System	An automated system used to identify an infringement of security policy. IDS can be host-based or network-based.
Internet Security Association Key Management Protocol aggressive mode	A protocol that uses half the exchanges of main mode to establish an IPsec connection.
Internet Security Association Key Management Protocol main mode	A protocol that offers optimal security using six packets to establish an IPsec connection.
jump server	A computer which is used to manage important or critical resources in a separate security domain. Also known as a jump host or jump box.
keying material	Cryptographic keys generated or used by cryptographic equipment or software.
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.
lockable commercial cabinet	A cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
logical access controls	Measures used to control access to systems and their information.
logging facility	A facility that includes software which generates events and their associated details, the transmission (if necessary) of event logs, and how they are stored.
malicious code	Any software that attempts to subvert the confidentiality, integrity or availability of a system.
malicious code infection	The occurrence of malicious code infecting a system.
management traffic	Traffic generated by system administrators over a network in order to control workstations and servers. This includes standard management protocols and traffic that contains information relating to the management of the network.
media	A generic term for hardware, often portable in nature, which is used to store information.
media destruction	The process of physically damaging media with the intent of making information stored on it inaccessible. To destroy media effectively, only the actual material in which information is stored needs to be destroyed.
media disposal	The process of relinquishing control of media when it is no longer required.
media sanitisation	The process of erasing or overwriting information stored on media so that it cannot be retrieved or reconstructed.
metadata	Descriptive information about the content and context used to identify information.
mobile device	A portable computing or communications device. For example, a laptop, mobile phone or tablet.
multifunction device	ICT equipment 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.
need-to-know	The principle of restricting an individual's access to only the information they require to fulfil the duties of their role.
network access control	Security policies used to control access to a network and actions on a network. This can include authentication checks and authorisation controls.
network device	ICT equipment designed to facilitate the communication of information.
network infrastructure	The infrastructure used to carry information between workstations and servers or other network devices.
non-interactive authentication	Authentication between systems or services that does not involve the interaction of a person.
non-repudiation	Providing proof that a user performed an action, and in doing so preventing a user from denying that they did so.
non-shared government facility	A facility where the entire facility and personnel are cleared to the highest level of information processed in the facility.
non-volatile flash memory media	A specific type of electrically erasable programmable read-only memory.
non-volatile media	A type of media which retains its information when power is removed.
official information	Information that would cause insignificant damage to the national interest, organisations or individuals if compromised (i.e. information marked as OFFICIAL).
official system	A system that processes, stores or communications official and sensitive information.
off-hook audio protection	A method of mitigating the possibility of an active handset inadvertently allowing background discussions to be heard by a remote party. This can be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent.

online services	Services using the internet such as social media, online collaboration tools, web browsing, instant messaging, IP telephony, video conferencing, file sharing websites and peer-to-peer applications.
OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
passphrase	A sequence of words used for authentication.
passphrase complexity	The use of at least three of the following character sets in passphrases: lower-case alphabetical characters (a-z), upper-case alphabetical characters (A-Z), numeric characters (0-9) or special characters.
password	A sequence of characters used for authentication.
patch	A piece of software designed to remedy security vulnerabilities, or improve the usability or performance of software and ICT equipment.
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 patch cables.
penetration test	A penetration test is designed to exercise real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical systems or information.
Perfect Forward Secrecy	Additional security for security associations ensuring 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 multiple computers. For example, a keyboard, video monitor and mouse.
plan of action and milestones	A document that describes security vulnerabilities in a system and the plans for their rectification.
position of trust	A position that involves duties that require a higher level of assurance than that provided by normal employment

	screening. In some organisations additional screening may be required. Positions of trust can include, but are not limited to, an organisation's Chief Information Security Officer and their delegates, administrators or privileged users.
privileged user	A user who can alter or circumvent a system's security measures. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security measures. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
product	A generic term used to describe software or hardware.
PROTECTED area	An area that has been authorised to process, store or communicate PROTECTED information. Such areas are not necessarily tied to a specific level of Security Zone.
Protection Profile	A document that stipulates the security functionality that must be included in 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 an evaluated product.
protective marking	An administrative label assigned to information that not only shows the value of the information but also defines the level of protection to be provided.
public information	Information that has been formally authorised for release into the public domain.
public network infrastructure	Network infrastructure that an organisation has no control over (e.g. the internet).
Public Switched Telephone Network	Public network infrastructure used for voice communications.
push-to-talk handsets	Handsets that have a button which is pressed by the user before audio can be communicated, thus providing off-hook audio protection.
quality of service	The ability to provide different priorities to different applications, users or data flows, or to guarantee a certain level of performance to a data flow.
Radio Frequency transmitter	A device designed to transmit electromagnetic radiation as part of a radio communication 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 sensitive or classified information often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security measures protecting the information.
Releasable To information	Information not to be passed to, or accessed by, foreign nationals beyond those belonging to specific nations which the information has been authorised for release to.
remote access	Access to a system that originates from outside an organisation's 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 (e.g. Universal Serial Bus flash drives or optical media).
seconded foreign national	A representative of a foreign government on exchange or long-term posting.
SECRET area	An area that has been authorised to process, store or communicate SECRET information. Such areas are not necessarily tied to a specific level of Security Zone.
secured space	An area certified to the physical security requirements for a Zone 2 to Zone 5 area, as defined in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Entity facilities*** policy, to allow for the processing or storage of sensitive or classified information.
Secure/Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of email messages.
Secure Shell	A network protocol that can be used to securely log into, execute commands on, and transfer files between remote workstations and servers.
security assessment	An activity undertaken to assess security controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.

security assessment report	A document that describes that outcomes of a security assessment and contributes to the development of a plan of action and milestones.
security association	A collection of connection-specific parameters containing information about a one-way connection in IPsec that is required for each protocol used.
security association lifetime	The duration security association information is valid for.
Security Construction and Equipment Committee	An Australian Government interdepartmental committee responsible for the evaluation and endorsement of security equipment and services. The committee is chaired by the Australian Security Intelligence Organisation.
security documentation	An organisation's cyber security strategy; system-specific security documentation; and any supporting policies, processes, procedures and registers.
security domain	A system or collection of systems operating under a consistent security policy that defines the classification, releasability and special handling caveats for information processed within the domain.
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 information or resources, or deliberate harm to people measured in terms of its likelihood and consequences.
security risk appetite	Statements that communicate the expectations of an organisation's senior management about the organisation's security risk tolerance. These criteria help an organisation identify security risk and prepare appropriate treatments and provide a benchmark against which the success of mitigations can be measured.
security risk management	The process of identifying, assessing and taking steps to reduce security risks to an acceptable level.
security target	An artefact of Common Criteria evaluations that specifies conformance claims, threats and assumptions,

	security objectives, and security requirements for an evaluated product.
security vulnerability	A weakness in a system's 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.
sensitive information	Information that would cause limited damage to the national interest, organisations or individuals if compromised (i.e. information marked OFFICIAL: Sensitive).
server	A computer that provides services to users or other systems. For example, a file server, email server or database server.
shared government facility	A facility where the facility and personnel are cleared at different levels.
shared non-government facility	A facility where the facility is shared by government organisations and non-government organisations.
shared responsibility model	A framework that describes the management and operational responsibilities between different parties for a system. Where responsibilities relating to specific security controls are shared between multiple parties, enough detail is documented to provide clear demarcation between the parties.
softphone	An application that allows a workstation to act as a phone using a built-in or externally-connected microphone and speaker.
software	An element of a system including, but not limited to, an application or operating system.
solid state drive	Non-volatile media that uses non-volatile 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 public network infrastructure and a Virtual Private Network (VPN) connection at the same time, such as an organisation's system and the internet.

Standard Operating Environment	A standardised build of an operating system and associated software that can be used for servers, workstations, laptops and mobile devices.
Standard Operating Procedure	Instructions for following a defined set of activities in a specific manner. For example, an approved data transfer process.
standard user	A user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass security measures.
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 executive responsible for a system.
system classification	The classification of a system is the highest classification of information which the system is authorised to store, process or communicate.
system security plan	A document that describes a system and its associated security controls.
system-specific security documentation	A system's system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.
telemetry	The automatic measurement and transmission of data collected from remote sources. Such data is often used within systems to measure the use, performance and health of one or more functions or devices that make up the system.
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 communications.
TEMPEST	A short name referring to investigations and studies of compromising emanations.
TOP SECRET area	An area that has been authorised to process, store or communicate TOP SECRET information. Such areas are not necessarily tied to a specific level of Security Zone.

traffic flow filter	A device that has been configured to automatically filter and control the flow of data.
Transfer Cross Domain Solution	A 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 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 IPsec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unsecured space	An area not been certified to the physical security requirements for a Zone 2 to Zone 5 area, as defined in AGD's PSPF, ***Entity facilities*** policy, to allow for the processing or storage of sensitive or classified information.
user	An individual that is authorised to access a 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	Network devices and ICT equipment grouped logically based on resources, security or business requirements instead of their physical location.
Virtual Private Network	A network that maintains privacy through a tunnelling protocol and security procedures. VPNs may use encryption to protect traffic.
virtualisation	Simulation of a hardware platform, operating system, application, storage device or network resource.

volatile media	A type of media, such as random-access memory, which gradually loses its information when power is removed.
vulnerability assessment	A vulnerability assessment can consist of a documentation-based review of a system's design, an in-depth hands-on assessment or automated scanning with software tools. In each case, the goal is to identify as many security vulnerabilities as possible.
vulnerability management	Vulnerability management assists in identifying, prioritising and responding to security vulnerabilities.
wear levelling	A technique used in non-volatile flash memory media to prolong the life of the media. As data can be written to and erased from memory blocks a finite number of times, wear-levelling helps to distribute writes evenly across each memory block, thereby decreasing wear and increasing its lifetime.
Wi-Fi Protected Access 2	A protocol designed to replace the Wi-Fi Protected Access protocol for communicating information over wireless networks.
wireless access point	A device which enables communications between wireless clients. It is typically also the device which connects wired and wireless networks.
wireless communications	The transmission of data over a communications path using electromagnetic waves rather than a wired medium.
wireless network	A network based on the 802.11 standards.
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 device to be shown on another device.