Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information security manual

Cybersecurity terminology

Last updated: September 2025

Glossary of abbreviations

Abbreviation	Meaning
AACA	ASD-Approved Cryptographic Algorithm
AACP	ASD-Approved Cryptographic Protocol
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AH	Authentication Header
AISEP	Australian Information Security Evaluation Program
API	application programming interface
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ATA	Advanced Technology Attachment
AUSTEO	Australian Eyes Only
BGP	Border Gateway Protocol

CA	Certification Authority
CCRA	Common Criteria Recognition Arrangement
CDN	content delivery network
CDS	Cross Domain Solution
CISO	chief information security officer
CRQC	cryptographically relevant quantum computer
DAST	dynamic application security testing
DH	Diffie-Hellman
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EEPROM	electrically erasable programmable read-only memory
EPROM	erasable programmable read-only memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FT	Fast Basic Service Set Transition
HACE	High Assurance Cryptographic Equipment

HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	infrared
IRAP	Infosec Registered Assessors Program
ISM	*Information security manual*
ISO	International Organization for Standardization
IT	information technology
LAN	Local Area Network
MAC	Media Access Control
MFD	multifunction device
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
MTA-STS	Mail Transfer Agent Strict Transport Security
NAA	National Archives of Australia
NIDS	Network-based Intrusion Detection System

NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OT	operational technology
OWASP	Open Worldwide Application Security Project
PDF	Portable Document Format
PFS	Perfect Forward Secrecy
PMK	Pairwise Master Key
PP	Protection Profile
PRF	pseudorandom function
RADIUS	Remote Access Dial-In User Service
REL	Releasable To
RF	radio frequency
ROA	Route Origin Authorization
ROV	Route Origin Verification
RPKI	Resource Public Key Infrastructure
RSA	Rivest-Sharmir-Adleman
SAST	static application security testing
SCA	software composition analysis
SCEC	Security Construction and Equipment Committee
SHA-2	Secure Hashing Algorithm 2
SHA-3	Secure Hashing Algorithm 3
SIEM	Security Information and Event Management
S/MIME	Secure/Multipurpose Internet Mail Extension
SMB	Server Message Block

SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation and Response
SOE	Standard Operating Environment
SP	Special Publication
SPF	Sender Policy Framework
SPN	Service Principal Name
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	web application firewall
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
XOF	extendable-output function

Glossary of cybersecurity terms

Term	Meaning
access control	The process of granting or denying requests for access to systems. 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.

accountable material	Accountable material requires the strictest control over its access and movement. Accountable material includes TOP SECRET data, some types of caveated data and any data designated as accountable material by its originator.
application control	An approach in which only an explicitly defined set of trusted applications are allowed to execute on systems.
assets	In the context of technology, an overarching term used to refer to operating systems, applications, IT equipment, OT equipment, services and data. Such assets may also be referred to as technology assets.
asymmetric cryptographic algorithms	Cryptographic algorithms where two different keys are used, commonly a private and a public key. Asymmetric cryptographic algorithms are also known as public key cryptographic algorithms.
attack surface	The operating systems, applications, IT equipment, OT equipment and services used by a system. The greater the attack surface the greater the chances of malicious actors finding an exploitable vulnerability.
Australian Eyes Only data	Data not to be passed to, or accessed by, foreign nationals.
Australian Government Access Only data	Data not to be passed to, or accessed by, foreign nationals, with the exception of seconded foreign nationals.
Australian 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 Certification Authority within the Australian Signals Directorate (ASD).
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 are accessible and useable by authorised entities when required.
biometrics	Measurable physical characteristics used to identify or verify an individual.

caveat	A marking that indicates that the data 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.
change and configuration management plan	A document that describes the management of changes to the configuration of systems.
chief information security officer	A senior executive who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and associated security risk management processes.
classification	The categorisation of systems according to the expected impact if it was to be compromised.
classified data	Data that would cause limited through to exceptionally grave damage to Australia’s national interests, the Australian Government generally or to an individual Commonwealth entity if compromised (i.e. data assessed as OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET).
commercial cryptographic equipment	A subset of IT 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 controls applied to protect telecommunications from unauthorised interception and exploitation, as well as ensure the authenticity of such telecommunications.
computer accounts	Accounts used to identify computers that belong to a domain, also known as machine accounts. Computer accounts provide a means for authenticating and auditing computer access to networks and domain resources.
conduit	A tube, duct or pipe used to protect cables.
confidentiality	The assurance that data 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.

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 controls for a system.
control plane	The administrative interface that allows for the management and orchestration of a system’s infrastructure and applications.
critical server	A server that provides critical network or security services. For example, Microsoft Active Directory Domain Services domain controllers, Microsoft Active Directory Certificate Services Certification Authority servers, Microsoft Active Directory Federation Services servers and Microsoft Entra Connect servers.
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 application	An application designed to perform cryptographic functions.
cryptographic equipment	A generic term for commercial 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 module	The set of hardware and software that implements approved cryptographic functions (including key generation) that are contained within the cryptographic boundary of the module.
cryptographic protocol	An agreed standard for secure communication between two or more entities to provide confidentiality, integrity, authentication and non-repudiation of data.
cryptographic system	A related set of hardware, software and supporting infrastructure used for cryptographic communication, processing or storage and the administrative framework in which it operates. Cryptographic systems may be based upon traditional cryptography, post-quantum cryptography or a combination of both.

cryptographically relevant quantum computer	A quantum computer that is capable of successfully executing attacks against traditional cryptographic systems.
customer	A person that an organisation has dealings with, typically via the consumption of goods or services. A customer does not necessarily need to purchase goods or services from the organisation.
cyber resilience	The ability to adapt to disruptions caused by cybersecurity incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cybersecurity incidents.
cybersecurity	Measures used to protect the confidentiality, integrity and availability of information technology (IT) and operational technology (OT) systems.
cybersecurity documentation	An organisation's cybersecurity strategy; system-specific cybersecurity documentation; and any supporting diagrams, plans, policies, processes, procedures and registers.
cybersecurity 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.
cybersecurity incident	An unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.
cybersecurity incident response plan	A document that describes the plan for responding to cybersecurity incidents.
cyberthreat	Any circumstance or event with the potential to harm systems.
data at rest	Data that resides on media or a system.
data in transit	Data that is being communicated across a communication medium.
data repository	A location in which data is stored, managed and made available to users.
data security	Measures used to protect the confidentiality, integrity and availability of data.
data spill	The accidental or deliberate exposure of data into an uncontrolled or unauthorised environment, or to people without a need-to-know.
declassification	A process whereby requirements for the protection of data are removed and an administrative decision is made to formally authorise its release into the public domain.

decommission	The process of removing something from operational service.
degausser	An electrical device or permanent magnet assembly which generates a 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 magnetic force, rendering any previously stored data 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 data to less trusted networks, such as the internet.
denial-of-service attack	An attempt by malicious actors 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 application	An application that can be used to prevent removable media and mobile devices from being connected to workstations and servers via external communication interfaces.
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	IT equipment that implements Internet Protocol version 4 and Internet Protocol version 6 protocol stacks.
elliptic curve cryptography	A group of asymmetric cryptographic algorithms underpinned by the mathematics of elliptic curves.
emanation security	The countermeasures employed to reduce sensitive or 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.
event	In the context of system logs, an event constitutes an evident change to the normal behaviour of a network, system or user.

extendable-output function	A function that uses a hash function to output a digest of a user-chosen length. This is different to a hash function which outputs a digest of a fixed length.
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 IT equipment or OT equipment.
fly lead	A lead that connects IT 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.
gateway	Gateways securely manage data flows between connected networks from different security domains.
hardware	A generic term for IT equipment and OT equipment.
hardware security module	A physical computing device that safeguards cryptographic keys and provides cryptographic processing. A hardware security module is or contains a cryptographic module. Hardware security modules are commonly deployed in Public Key Infrastructure, digital identity solutions and payment systems.
Hash-based Message Authentication Code	A cryptographic function 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 authorised by ASD for the protection of SECRET and TOP SECRET data.
High Assurance Evaluation Program	The rigorous investigation, analysis, verification and validation of products by ASD to protect SECRET and TOP SECRET data.
high assurance IT equipment	IT equipment that has been designed and authorised for the protection of SECRET and TOP SECRET data.
high-value server	A server that provides important network services or contains data repositories. For example, Domain Name System servers, database servers, email servers, file servers and web servers.

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.
information technology	Hardware, software and supporting infrastructure used for the processing, storage or communication of data.
Infosec Registered Assessors Program	An initiative of ASD 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.
insider	Any person that has, or had, authorised logical or physical access to a system and its resources.
insider threat	An insider that performs, or attempts to perform, damaging activities (either intentionally or unintentionally) to a system or its resources. Some organisations may choose to exclude unintentional damage to systems and their resources (often referred to as negligent or accidental damage) from their definition of insider threat in order to focus on insiders with malicious intent (often referred to as malicious insiders).
integrity	The assurance that data 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 malicious or unwanted activities. An Intrusion Detection System can be host-based or network-based.
Intrusion Prevention System	An automated system used to identify malicious or unwanted activities and react in real-time to block or prevent such activities. An Intrusion Prevention System can be host-based or network-based.
IRAP assessment	A security assessment conducted by an IRAP assessor against the requirements of the *Information security manual*.

IT equipment	Any device that can process, store or communicate data within IT environments, such as computers, multifunction devices, network devices, smartphones, electronic storage media and smart devices.
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.
key encapsulation mechanism	A form of asymmetric cryptography that carries out two functions. Specifically, generating an encryption session key and then securely transporting it to the receiver.
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.
keying material	Cryptographic keys generated or used by cryptographic equipment, applications or libraries.
logging facility	A facility that collects and stores event logs.
malicious actors	Individuals, groups or organisations that conduct malicious activities, such as cyber espionage, cyberattacks or cyber-enabled crime.
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.
media	A generic term for hardware, often portable in nature, which is used to store data.
media destruction	The process of physically damaging media with the intent of making data stored on it inaccessible. To destroy media effectively, only the actual material in which data 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 data stored on media so that it cannot be retrieved or reconstructed.
medical device	Devices approved by the Therapeutic Goods Administration under the *Therapeutic Goods (Medical Devices) Regulations 2002* for diagnostic or therapeutic purposes.

memory-safe programming languages	Programming languages that prevent the introduction of vulnerabilities related to memory use. Examples of memory-safe programming languages include C#, Go, Java, Ruby, Rust and Swift. Examples of non-memory-safe programming languages include Assembly and C/C++.
metadata	Descriptive data about the content and context used to identify data.
mobile device	A portable computing or communications device. For example, smartphones, tablets and laptop computers.
multi-factor authentication	Authentication using two or more different authentication factors. This may include something users know, something users have or something users are.
multifunction device	IT 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 data 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	IT equipment designed to facilitate the communication of data. For example, routers, switches and wireless access points.
network infrastructure	The infrastructure used to carry data between workstations and servers or other network devices.
network management traffic	Network traffic generated by system administrators over a network in order to control workstations and servers. This includes standard management protocols and other network traffic that contains data relating to the management of the network.
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-volatile flash memory media	A specific type of electrically erasable programmable read-only memory.
non-volatile media	A type of media which retains its data when power is removed.

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 directly accessible over the internet, including those located behind a perimeter firewall. Such services may also be referred to as internet-facing services.
OpenPGP Message Format	An open-source implementation of Pretty Good Privacy, a widely available cryptographic toolkit.
operating system	Software that provides the interface through which users access a system. Operating systems also facilitate access to user applications, server applications, mobile applications and web applications.
operational technology	Systems that detect or cause a direct change to the physical environment through the monitoring or control of devices, processes and events. Operational technology is predominantly used to describe industrial control systems which include supervisory control and data acquisition systems and distributed control systems.
OT equipment	Any device that can process, store or communicate data or signals within OT environments, such as programmable logic controllers and remote terminal units.
passphrase	A sequence of words used for authentication.
password	A sequence of characters used for authentication.
password complexity	The use of different character sets, such as lower-case alphabetical characters (a-z), upper-case alphabetical characters (A-Z), numeric characters (0-9) and special characters.
passwordless authentication	Authentication that does not involve the use of something users know. Passwordless authentication may be single-factor or multi-factor, with the later often referred to as passwordless multi-factor authentication.
passwordless multi-factor authentication	Multi-factor authentication using something users have that is unlocked by something users know or are. Note, while a memorised secret may be used as part of passwordless multi-factor authentication (e.g. to unlock access to a cryptographic private key stored on a device) it is not the primary authentication factor, hence the use of the passwordless terminology.

patch	A piece of software designed to remedy vulnerabilities or improve the usability or performance of operating systems, applications, IT equipment or OT 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 scenarios in an attempt to achieve a specific goal, such as compromising critical systems.
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 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 cases, additional screening may be required. Positions of trust can include, but are not limited to, chief information security officers and their delegates, system administrators and privileged users.
post-quantum cryptography	Asymmetric cryptography designed to remain secure in the presence of a cryptographically relevant quantum computer.
post-quantum traditional hybrid scheme	An asymmetric cryptographic scheme that incorporates at least two different components based on different mathematically hard problems. Generally, post-quantum traditional hybrid schemes are used to combine post-quantum cryptography and traditional cryptography such that defeating the scheme requires defeating each component.
privileged operating environments	Privileged operating environments are those used for activities that require a degree of privileged access, such as system administration activities.
privileged user accounts	User accounts that have the capability to modify system configurations, account privileges, event logs or security configurations. This also applies to user accounts that may only have limited privileges but still have the ability to bypass some system controls. A privileged user account may belong to a person or a service.

product	A generic term used to describe software or hardware.
PROTECTED area	An area that has been authorised to process, store or communicate PROTECTED data. 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 a Common Criteria evaluation to meet a range of defined threats. Protection Profiles also define the activities to be taken to assess the security function of an evaluated product.
protective marking	An administrative label assigned to data that not only shows the value of the data but also defines the level of protection to be provided.
public data	Data that has been formally authorised for release into the public domain.
public network infrastructure	Network infrastructure that an organisation has no control over, such as the internet.
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 controls used to protect data based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the controls for media containing sensitive or classified data often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the controls protecting the data.
Releasable To data	Data not to be passed to, or accessed by, foreign nationals beyond those belonging to specific nations which the data 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, such as Universal Serial Bus flash drives and 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 data. Such areas are not necessarily tied to a specific level of security zone.
Secure Admin Workstation	A hardened workstation, or virtualised privileged operating environment, used specifically in the performance of administrative activities.
Secure by Default	A software development principle whereby products and services are configured for maximum security by default.
Secure by Demand	When a customer requests that their suppliers provide evidence of their commitment to security and transparency for their products and services.
Secure by Design	A software development principle whereby security is designed into every stage of a product or service's development.
secure channel	A path for transferring data between two entities that ensures confidentiality and integrity, as well as mutual authentication, between the two entities.
Secure Shell	A network protocol that can be used to securely log into, execute commands on, and transfer files between remote workstations and servers.
Secure/Multipurpose Internet Mail Extension	A protocol which allows the encryption and signing of email messages.
secured space	An area certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Department of Home Affairs' *Protective Security Policy Framework*.
security assessment	An activity undertaken to assess 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 the 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 used for IPsec connections.
security association lifetime	The duration a security association 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 domain	A system or collection of systems operating under a consistent security policy that defines the classification, releasability and special handling caveats for data 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 data 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 their security risk tolerance. These criteria help an organisation identify security risks, 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.
sensitive data	Data that would cause damage to an organisation or an individual if compromised.
server	A computer that provides services to users or other systems. For example, a file server, email server or database server.
service accounts	User accounts that are used to perform automated tasks without manual intervention, such as machine to machine communications. Service accounts will typically be configured to disallow interactive logins.
shared facility	A facility shared by multiple tenants. For example, a single floor, or part of a floor, within a multi-tenanted building.
shared responsibility model	A framework that describes the management and operational responsibilities between different parties for a system. Where responsibilities relating to specific controls are shared between multiple parties, enough detail is documented to provide clear demarcation between the parties.
software	An element of a system including, but not limited to, an operating system or application.

solid-state drive	Non-volatile media that uses non-volatile flash memory media to retain its data when power is removed and, unlike non-volatile magnetic media, contains no moving parts.
split tunnelling	Functionality that allows personnel to access public network infrastructure and a Virtual Private Network 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 applications that can be used for servers, workstations and mobile devices.
supplier	Organisations, such as software developers, IT equipment manufacturers, OT equipment manufacturers, service providers and data brokers, that provide products and services. Suppliers can also include other organisations involved in distribution channels.
symmetric cryptographic algorithms	Cryptographic algorithms that use the same key for encryption and decryption. Block ciphers and stream ciphers are common types of symmetric cryptographic algorithms.
system	The cyber supply chain, infrastructure, operating systems and applications supporting the processing, storage or communication of data, including the governance framework in which they operate.
system administrator	A system administration role performed by a privileged user that holds a position of trust.
system classification	The classification of a system is the highest classification of data which the system is authorised to store, process or communicate.
system owner	The executive responsible for a system.
system security plan	A document that describes a system and its associated controls.
system-specific cybersecurity documentation	A system’s system security plan, cybersecurity incident response plan, change and configuration management 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.

TOP SECRET area	An area that has been authorised to process, store or communicate TOP SECRET data. Such areas are not necessarily tied to a specific level of security zone.
traditional cryptography	Common well studied and understood cryptographic algorithms that existed before the threat of a cryptographically relevant quantum computer existed.
Transfer Cross Domain Solution	A system that facilitates the transfer of data, 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.
trustworthy source	A person or system formally identified as being capable of reliably producing data meeting certain defined parameters, such as a maximum data classification and reliably reviewing data produced by others to confirm compliance with certain defined parameters.
trustworthy supplier	A supplier that has been verified as trustworthy as part of a cyber supply chain risk management assessment and subsequently recorded on an organisation’s approved supplier list.
tunnel mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unprivileged user accounts	User accounts that do not have the capability to modify system configurations, account privileges, event logs or security configurations. An unprivileged user account may belong to a person or a service.
unprivileged operating environments	Unprivileged operating environments are those used for activities that do not require privileged access, such as reading emails and browsing the web.
unsecured space	An area not certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Department of Home Affairs’ *Protective Security Policy Framework*.
untrusted device	Any IT equipment that an organisation does not trust. For example, unknown IT equipment (which might belong to malicious actors), or an uncontrolled personal mobile device of an employee.
user	An individual that works for an organisation and is authorised to access a system.
user accounts	User accounts include privileged user accounts and unprivileged user accounts.

validation	Confirmation that stakeholder requirements for the intended use of operating systems, applications, IT equipment or OT equipment have been met.
verification	Confirmation that design or compliance requirements for operating systems, applications, IT equipment or OT equipment have been met.
Virtual Local Area Network	Network devices and networked IT equipment grouped logically based on resources, security or business requirements instead of their physical location.
virtual patching	A security measure designed to prevent known exploitation attempts against known vulnerabilities in web applications, typically via the use of a network-based intrusion prevention system or a web application firewall.
Virtual Private Network	A network that maintains privacy through a tunnelling protocol and security procedures. Virtual Private Networks may use encryption to protect network traffic.
virtualisation	Simulation of hardware or software resources.
volatile media	A type of media, such as random-access memory, which gradually loses its data when power is removed.
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.
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 tools. In each case, the goal is to identify as many vulnerabilities as possible.
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	A protocol designed for communicating data over wireless networks.
Wi-Fi Protected Access 2	A protocol designed to replace the Wi-Fi Protected Access protocol for communicating data over wireless networks.
Wi-Fi Protected Access 3	A protocol designed to replace the WPA2 protocol for communicating data 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.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre