Information Security Manual

Published: 22 June 2023

Cyber Security Terminology

Glossary of abbreviations

Abbreviation	Meaning
AACA	ASD-Approved Cryptographic Algorithm
AACP	ASD-Approved Cryptographic Protocol
ACSC	Australian Cyber Security Centre
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
AGAO	Australian Government Access Only
AGD	Attorney-General's Department
AH	Authentication Header
AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
API	application programming interface
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
CISO	Chief Information Security Officer
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
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
HSTS	Hypertext Transfer Protocol Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
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
LAN	Local Area Network
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MFD	multifunction device
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
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PFS	Perfect Forward Secrecy
PMK	Pairwise Master Key
PP	Protection Profile
PRF	pseudorandom function
PSPF	Protective Security Policy Framework
PSTN	Public Switched Telephone Network
RADIUS	Remote Access Dial-In User Service
REL	Releasable To
RF	Radio Frequency
ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure
RSA	Rivest-Sharmir-Adleman
SCEC	Security Construction and Equipment Committee
SHA-2	Secure Hashing Algorithm 2
S/MIME	Secure/Multipurpose Internet Mail Extension
SNMP	Simple Network Management Protocol
SOE	Standard Operating Environment
SQL	Structured Query Language
SP	Special Publication

SPF	Sender Policy Framework
SPN	Service Principal Name
SSH	Secure Shell
SSID	Service Set Identifier
TLS	Transport Layer Security
USB	Universal Serial Bus
UEFI	Unified Extensible Firmware Interface
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

Glossary of cyber security terms

Term	Meaning
access control	The process of granting or denying requests for access to systems, applications and data. 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.
aggregation (of data)	A term used to describe compilations of data 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 data.
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.
ASD Enterprise Mobility Evaluation Program	The investigation, analysis, verification and validation of enterprise mobility solutions by the Australian Signals Directorate (ASD) to protect up to PROTECTED data.
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 Cyber Security Centre.
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.
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 data 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 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.
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 and data according to the expected impact if it was to be compromised.
classified data	Data that would cause damage, serious damage or exceptionally grave damage to the national interest, an organisation or an individual if compromised (i.e. data assessed as PROTECTED, SECRET or TOP SECRET).
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 controls applied to protect telecommunications from unauthorised interception and exploitation, as well as ensure the authenticity of such telecommunications.
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, a Microsoft Active Directory Domain Services domain controller or an authentication server.
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 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 data.
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 data.
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 has either compromised business operations or has a significant probability of compromising business operations.
cyber threat	Any circumstance or event with the potential to harm systems or data.
data at rest	Data that resides on media or a system.
data in transit	Data that is being communicated across a communication medium.
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.
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 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 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 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.
escort	A person who ensures that when maintenance or repairs are undertaken to ICT equipment that uncleared

	personnel are not exposed to data 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.
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 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 ICT equipment	ICT equipment that has been designed and authorised for the protection of SECRET and TOP SECRET data.
high-value server	A server that provide important network services or contains important data repositories. For example, a Domain Name System server, database server, email server, file server or web server.
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 data, such as computers, multifunction devices, network devices, smartphones, digital cameras, electronic storage media, smart devices and other radio devices.
incident response plan	A document that describes the plan for responding to cyber security incidents.
Infosec Registered Assessors Program	An initiative of the Australian Cyber Security Centre 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 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 an infringement of security policy. IDS can be host-based or network-based.
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.
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.
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.

memory-safe programming languages	Programming languages that prevent the introduction of security 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 laptops.
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.
multi-factor authentication	Authentication using two or more different authentication factors. This may include something users know, something users have or something users are.
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	ICT 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 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.
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 doesn't 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 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 scenarios in an attempt to achieve a specific goal, such as compromising critical systems or data.
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 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.
privileged accounts	Privileged accounts include privileged user accounts and privileged service accounts.
privileged operating environments	Privileged operating environments are those used exclusively for administrative activities.
privileged user	A user who can alter or circumvent a system's controls. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass controls. A privileged user can have the capability to modify system configurations, account privileges, event logs and security configurations for 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 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 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.
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 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-by-default	A software development principle whereby products and services are configured for maximum security by default.
secure-by-design	A software development principle whereby security is designed into every stage of a product or service's development.
secured space	An area certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Attorney-General's Department's *Protective Security Policy Framework*, *Entity facilities* policy, to allow for the processing or storage of sensitive or classified data.
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 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 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 documentation	An organisation's cyber security strategy; system-specific security documentation; and any supporting diagrams, plans, 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 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.
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 data	Data that would cause limited damage to the national interest, 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	Where an organisation's facility resides within a larger facility that is shared with one or more different organisations.
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.
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 data 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 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.

supplier	Organisations, such as application developers, ICT equipment manufacturers and service providers, that provide products and services. Suppliers can also include other organisations involved in distribution channels.
system	A related set of hardware and software used for the processing, storage or communication of data 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 data which the system is authorised to store, process or communicate.
system security plan	A document that describes a system and its associated 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.
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.
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.
trusted 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.
tunnel mode	An IPsec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet.
unprivileged accounts	Unprivileged accounts include unprivileged user accounts and unprivileged service accounts.
unprivileged operating environments	Unprivileged operating environments are those used for non-administrative activities, such as reading emails and browsing the web.
unsecured space	An area not been certified to the physical security requirements for a Security Zone Two to Security Zone Five area, as defined in the Attorney-General's Department's *Protective Security Policy Framework*, *Entity facilities* policy, to allow for the processing or storage of sensitive or classified data.
user	An individual that is authorised to access a system.
user accounts	User accounts include privileged user accounts and unprivileged user accounts.
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 other 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. Virtual Private Networks may use encryption to protect network 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 data 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.
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.