Australian Government Information Security Manual

Supporting information

Glossary of cyber security terminology

Term	Meaning
access control	The process of granting or denying requests for access to information and systems. Can also refer to the process of granting or denying requests to enter facilities.
Access Cross Domain Solution	A system permitting access to multiple security domains from a single client device.
accreditation	The process by which an authorising officer formally accepts security risks associated with the operation of a system and authorises it to operate.
aggregation (of data)	A term used to describe compilations of information that may require a higher level of protection than their component parts.
application whitelisting	An approach in which only an explicitly defined set of applications are permitted to execute on system.
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	A caveat indicating that information is not to be passed to, or accessed by, foreign nationals.
Australian Government Access Only	A caveat used by the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), the Australian Signals Directorate (ASD), the Department of Defence and the Office of National Assessments (ONA) indicating information is 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 an appropriate level of understanding and authority to formally recognise and accept security risks associated the operation of a system and 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.
blacklist	A list of things that are considered to be unacceptable and should not be trusted. A blacklist is the opposite of a whitelist.
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	The process by which the security posture and security risks associated with the operation of a system is determined through a security assessment.
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 information or systems according to the business impact level associated with that information or system.
classified information	Information that requires increased security to protect its confidentiality (i.e. information marked 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 software and ICT equipment 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 (SSH) server to forward a Transmission Control Protocol connection to an arbitrary port on the local host.
consumer guide	Specific guidance for evaluated products and services.
content filter	A filter that examines content to assess conformance against a policy.
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 (CGCE) and high assurance cryptographic equipment (HACE).
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 security	Measures used to protect systems and information processed, stored or communicated on such systems from compromise of confidentiality, integrity and availability.

cyber security event	An identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of safeguards.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.
Cyber Security Incident Reporting Scheme	A scheme established by the ACSC to collect information on cyber security incidents.
cyber threat	Any circumstance or event with the potential to harm a system 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 using a whitelisting approach 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 (IPv4) and Internet Protocol version 6 (IPv6) 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 (RF) 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.
flash memory media	A specific type of electrically erasable programmable read-only memory (EEPROM).
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 solely owned and managed by 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	A subset of high assurance ICT equipment which contains cryptographic components.
high assurance evaluation	The rigorous investigation, analysis, verification and validation of ICT equipment against a stringent security standard.
high assurance ICT equipment	ICT equipment that has been approved by the ACSC for the protection of information classified SECRET or above.

highly classified information	Information that requires the highest level of security to protect its confidentiality (i.e. information marked SECRET or TOP SECRET).
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 flash memory media or battery backed random-access memory (RAM).
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 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.
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 (ISAKMP) aggressive mode	A protocol that uses half the exchanges of ISAKMP main mode to establish an IPsec connection.
ISAKMP 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 with information storage capability that can be used from a non-fixed location. Mobile devices include mobile phones, smartphones, tablets, laptops, portable electronic devices and other portable internet-connected devices.
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.
nationality releasable information	A caveat indicating that information is not to be passed to, or accessed by, foreign nationals beyond those belonging to specific countries which the information has been authorised for release to.
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	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-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 media	A type of media which retains its information when power is removed.
official information	Non-classified information identified as requiring basic protection (i.e. information marked as OFFICIAL or OFFICIAL: Sensitive).
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 characters or words used for authentication. Also known as a password.
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 business information or services.
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.
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 (CISO) 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.
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.
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 (USB) 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 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 ASIO.
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.
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.
softphone	An application that allows a workstation to act as a phone using a built-in, or externally connected, microphone and speaker.
software component	An element of a system including, but not limited to, a database, operating system, network or web application.
solid state drive	Non-volatile media that uses flash memory media to retain its information when power is removed and, unlike non-volatile magnetic media, contains no moving parts.
split tunnelling	Functionality that allows personnel to access both public network infrastructure and a Virtual Private Network (VPN) connection at the same time, such as an organisation's system and the Internet.
SSH-agent	An automated or script-based SSH session.
Standard Operating Environment	A standardised build of an operating system and associated software that is deployed on multiple devices. A Standard Operating Environment (SOE) 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 plan documenting the security controls and procedures for a 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.
TEMPEST-rated ICT equipment	ICT equipment that has been specifically designed to minimise TEMPEST 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 private data 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 RAM, 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 flash memory to prolong the life of the media. As data can be written to and erased from an address on flash memory a finite number of times, wear-levelling helps to distribute writes evenly across each memory block, thereby decreasing the wear on the media and increasing its lifetime.
whitelist	A list of things that are considered to be acceptable and should be trusted. A whitelist is the opposite of a blacklist.
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.