16 Entity facilities

A. Purpose

1. This policy provides the consistent and structured approach to be applied to building construction, security zoning and physical security control measures of entity facilities. This ensures the protection of Australian Government people, information and physical assets secured by those facilities.

B. Requirements

B.1 Core requirement

Each entity must:

a. ensure it fully integrates protective security in the process of planning, selecting, designing and modifying its facilities for the protection of people, information and physical assets

b. in areas where sensitive or security classified information and assets are used, transmitted, stored or discussed, certify its facility's physical security zones in accordance with the applicable ASIO Technical Notes, and

c. accredit its security zones.

B.2 Supporting requirements

2. The supporting requirements help entities consider physical security controls for entity facilities and apply relevant PSPF requirements.

Supporting requirements for entity facilities

#	Supporting requirements	
Requirement 1. Design and modify facilities	When designing or modifying facilities, entities **must**: a. secure and control access to facilities to meet the highest risk level to entity resources, and b. define restricted access areas as detailed below.	
	Zone name	**Zone definition**
	Zone One	Public access.
	Zone Two	Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control.
	Zone Three	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control.
	Zone Four	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Single factor authentication for access control.
	Zone Five	No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual factor authentication for access control.

#	Supporting requirements
Requirement 2. Building construction	Entities **must** ensure: a. facilities for Zones Two to Five that store sensitive or security classified information and assets are constructed in accordance with applicable sections of: i. ASIO Technical Note 1/15 – Physical Security Zones, and ii. ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas b. security zones are constructed to protect against the highest risk level in accordance with the entity security risk assessment in areas: i. accessed by the public and authorised personnel, and ii. where physical assets, other than sensitive and security classified assets, are stored.
Requirement 3. Hardware	Entities must, in areas that store sensitive and security classified information, ensure perimeter doors and hardware are: a. constructed in accordance with ASIO Technical Notes in Zones Two to Five, and b. secured with SCEC-approved products rated to Security Level 3 in Zones Three to Five.
Requirement 4. Security alarm systems	Entities **must**: a. for Zone Three, use either: i. a Type 1 security alarm system [Note i], or ii. a Class 5 commercial security alarm system, or iii. guard patrols performed at random intervals and within every four hours. b. for Zone Four and Zone Five, use: i. SCEC-approved Type 1A or Type 1 security alarm system in accordance with the Type 1A security alarm system transition policy [Note i] with SCEC-approved detection devices and ii. a SCEC-endorsed Security Zone Consultant to design and commission the SCEC-approved Type 1A alarm system. c. in Zones Three [Note ii] to Five: i. use sectionalised security alarm systems ii. security alarm systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. monitored and responded to in a timely manner, and iii. privileged alarm systems operators and users are appropriately trained and security cleared.
Requirement 5. Access control	a. Entities **must** control access to Zones Two to Five within the entity's facilities by only allowing access for authorised personnel, visitors, vehicles and equipment and apply the following controls: i. for Zones Two to Five, use: A. electronic access control systems where there are no other suitable identity verification and access control measures in place. ii. for Zones Three to Five, use: A. identity cards with personal identity verification B. sectionalised access control system with full audit C. regular review of audit logs for any unusual or prohibited activity iii. for Zone Four and Zone Five, ensure access control systems are: A. directly managed and controlled by the entity B. maintained by appropriately cleared contractors C. privileged operators and users are appropriately trained and security cleared to the level of the security zone, and iv. for Zone Five, use dual authentication access control. b. When granting ongoing (or regular) access to entity facilities for people who are not directly engaged by the entity or covered by the terms of a contract or agreement, the entity's accountable authority or CSO **must** ensure the person has: i. the required level of security clearance for the facility's security zones, and ii. a business need supported by a business case and risk assessment, which is reassessed on a regular basis at least every two years.
Requirement 6. Technical surveillance counter-measures	Entities **must** ensure a technical surveillance countermeasures inspection is completed for facilities where: a. TOP SECRET discussions are regularly held, or b. the compromise of discussions may have a catastrophic business impact level.

#	Supporting requirements
Requirement 7. Security zone certification	CSOs or delegated security advisers **must**, before using a facility operationally: a. certify the facility's Zones One to Four in accordance with the PSPF and ASIO Technical Notes b. for Zone Five facilities, obtain: i. ASIO-T4 physical security certification for security areas used to handle TOP SECRET sensitive and security classified information, sensitive compartmented information (SCI) or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level.
Requirement 8. Security zone accreditation	CSOs or delegated security advisers **must**, before using a facility operationally: a. accredit Zones One to Five when the security controls are certified and the entity determines and accepts the residual risks, and b. for Zone Five facilities, obtain: i. Australian Signals Directorate security accreditation for areas used to secure and access TOP SECRET sensitive compartmented information.
Requirement 9. ICT facilities	Entities **must**: a. certify and accredit the security zone for ICT sensitive and security classified information with an extreme business impact level b. ensure that all TOP SECRET information ICT facilities are in compartments within an accredited Zone Five area and comply with Annex A – ASIO Technical Note 5/12 – Compartments within Zone Five areas, and c. before using outsourced ICT facilities operationally obtain ASIO-T4 physical security certification for the outsourced ICT facility to hold information that, if compromised, would have a catastrophic business impact level.

Supporting requirements notes:

[i] The Type 1A security alarm system transition policy details the progressive timeframe for replacement, by 1 August 2021, of the Type 1 Security Alarm System with the Type 1A Security Alarm System in certified and accredited Security Zones Four and Five. Replacement of the Type 1 Security Alarm System with the Type 1A Security Alarm System aims to ensure technology keeps pace with the changing threat environment.

[ii] Unless guard patrols are used instead of a security alarm system in accordance with **Requirement 4aiii**.

C. Guidance

C.1 Planning

3. The PSPF policy: Security planning and risk management requires entities use a security risk assessment to develop a security plan to mitigate identified and emerging security risks, aligning with the entity's priorities and objectives. This strategic level overarching security plan is supported by more detailed plans where required.

4. The Attorney-General's Department recommends that entities develop a site security plan for new facilities, including facilities under construction or major refurbishments of existing facilities, that considers security matters associated with:

   a. location and nature of the site

   b. ownership or tenancy of the site (sole or shared, including multiple entities sharing the same space)

   c. collateral exposure, such as the presence nearby of other 'attractive targets'

   d. access to the site for authorised personnel and the public (if necessary) and preventing access as required

   e. security classification of information and assets, including ICT assets and related equipment, to be stored, handled or processed in each part of the site, this includes considering the need to hold security classified and other sensitive discussions and meetings

   f. other resources that will be on the site

   g. protective security measures required for:

      i. the site as a whole

ii. particular areas within the site (eg a floor or part of a floor that will hold information of a higher classification than the rest of the site)

iii. storage, handling and processing of security classified information

iv. security classified and other sensitive discussions and meetings.

5. Security risks during business hours may be significantly different to those experienced out-of-hours. For example, during work hours there may be increased risks from public and client contact, as well as from insider threats. During out-of-hours, external threats, such as break and enters, may be more prevalent.

C.2 Site selection

6. The Attorney-General's Department recommends that the Chief Security Officer (CSO) and security advisors are involved in assessing:
   a. the suitability of the physical security environment of a proposed site for entity facilities
   b. whether a facility can be constructed or modified to incorporate security measures that provide appropriate risk mitigation strategies.
7. While security measures prevent or reduce the likelihood of events, the site and design also needs to accommodate normal business.
8. **Table 1** outlines key security factors the Attorney-General's Department encourages entities to consider when selecting a site.

Table 1 Site selection factors

Factor	Description
Neighbourhood	Consider the local threat environment from neighbourhood-related issues such as local criminal activity, risks from neighbouring entities and businesses, suitability of neighbours, oversight of entity operations.
Standoff perimeter	Consider standoff distances where there is an identified threat from pedestrians and vehicle-based improvised explosive devices (IED). However, it may not be possible in urban areas to achieve an effective standoff distance for some threats. Entities are encouraged to seek additional advice for example blast engineering advice.
Site access and parking	Consider the need and ability to control access to pedestrians and vehicles to the site including the facility, parking and standoff perimeter.
Building access point	Consider ability to secure all building access points including entries and exits, emergency exits, air intakes and outlets and service ducts.
Security zones	Establish security zones based on: a. entity risk assessment b. business impact levels, and c. security-in-depth [Note i] at the site.
Environmental risks	Seek specialist advice about the risk of natural disasters and suitable mitigation strategies and security products.

Table 1 notes:

i Security-in-depth is a multi-layered system in which security measures combine to make it difficult for an intruder or authorised personnel to gain unauthorised access.

C.3 Designing and modifying facilities

9. The **core requirement** mandates entities fully integrate protective security early in the process of planning, selecting, designing and modifying facilities.
10. **Requirement 1a** mandates entities design and modify facilities to secure and control access that meets the highest risk levels to entity resources.
11. Protection of people, information and assets is achieved through a combination of physical and procedural security measures that prevent or mitigate threats and attacks. The Attorney-General's Department recommends entities design facilities using successive layers of physical security when planning for new entity facilities or modifying existing facilities:

a. **Deter** — measures that cause significant difficulty or require specialist knowledge and tools for adversaries to defeat.

b. **Detect** — measures that identify unauthorised action are being taken or have already occurred.

c. **Delay** — measures to impede an adversary during attempted entry or attack, or slow the progress of a detrimental event to allow a response.

d. **Respond** — measures that resist or mitigate the attack or event when it is detected.

e. **Recover** — measures to restore operations to normal levels following an event.

12. In accordance with the **core requirement**, entities must consider:

    a. for new constructions or for significant modifications to facilities:

        i. protective security measures as early as possible, preferably during the concept and design stages, see ASIO Technical Note 1/15 Physical Security of Zones

        ii. the siting within a facility of entity functions that need security measures so that these locations can be constructed or modified to provide appropriate protection

    b. for new leases on facilities, the suitability of construction methods and materials to give the protections needed, see ASIO Technical Note 1/15 Physical Security of Zones.

13. ASIO Technical Notes provide protective security mitigations to maintain the confidentiality and integrity of sensitive and security classified information and assets. These protective security mitigations are especially related to overt and covert attacks from foreign intelligence services and malicious insiders. Based on the entity security risk assessment additional security mitigations for the protection of personnel and assets, other than sensitive and security classified assets, may be required and are detailed in PSPF policy: Physical security for entity resources.

C.3.1 Mailrooms and delivery areas

14. Mailrooms and parcel delivery areas can be exposed to threats such as improvised explosive devices, chemical, radiological and biological attacks. The Attorney-General's Department recommends that entities assess the likelihood of such attacks and apply appropriate physical mitigations (eg mail-screening devices, a stand-alone delivery area or using a commercial mail receiving area and sorting service). In accordance with the **core requirement**, it may be necessary to consider these options early in the process of planning, selecting, designing and modifying facilities.

C.4 Security zones

15. Security zones provide a methodology for scalable physical security risk mitigation that entities apply based on their security risk assessment.[1]

16. **Requirement 1b** mandates entities design and modify their facilities in order to define restricted access areas according to the five security zones, with increasing restrictions and access controls as the zones progress from Zone One to Zone Five.

17. The physical security measures detailed in the applicable ASIO Technical Notes are designed to protect security classified information and assets from covert and surreptitious attack.

18. **Requirement 2b** mandates security zones are constructed to protect against the highest risk level in accordance with the entity security risk assessment in areas:

    a. accessed by the public and authorised personnel access

    b. where physical assets, other than sensitive and security classified assets, are stored.

19. Further physical security mitigations to protect against blast, ballistic and forced entry may be required in addition to the ASIO Technical Note requirements. See C.5.2 Construction of buildings.

20. The number of zones required by an entity depends on the different levels of assurance and segregation required to respond to identified threats and risks. The Attorney-General's Department recommends that

[1] For information on risk assessments, see the PSPF policy: Security planning and risk management.

entities consider the business impact level of the compromise, loss or damage of sensitive and security classified information and assets to be maintained within facilities to determine the entity's minimum and maximum zone requirements. Refer to the PSPF policy: Sensitive and classified information for details on business impact levels for the compromise of sensitive and security classified information.

21. **Table 2** provides broad descriptions of each zone for the protection of sensitive and security classified information and assets, including examples of where the zones might be used and the personnel security clearance requirements for each zone. The PSPF policy: Sensitive and classified information provides guidance on the application of security zones to meet the minimum use and storage protections for sensitive and security classified information.

Table 2 Security zone descriptions and personnel security clearance requirements for the protection of sensitive and security classified information and assets

Security zone	Security zone description, including permitted use [Note i] and storage [Note ii] of sensitive and security classified resources	Personnel security clearance requirement for access to the resources stored in the zone	Examples
Zone One	Public access areas. (The inner perimeter of Zone One may move to the building or premise perimeter out-of-hours if exterior doors are secured. a. Sensitive and security classified information and assets with a business impact level of low to medium that are needed to do business may be used and stored. b. Sensitive and security classified information and assets with business impact level of high may be used. Storage is not recommended but is permitted if unavoidable. c. Sensitive and security classified information and assets with a business impact level greater than high may only be used under exceptional circumstances and requires the approval of the originating or owning entity. No storage is permitted.	Employment screening sufficient, security clearance not required.	a. Building perimeters and public foyers. b. Interview and front-desk areas where there is no segregation of authorised personnel from clients and the public. c. Out-of-office temporary work areas where the entity has no control over access. d. Fieldwork, including most vehicle-based work. e. Exhibition areas with no security controls.
Zone Two	Entity office areas. Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control. a. Sensitive and security classified information and assets with a business impact level up to high may be used and stored. b. Sensitive and security classified information and assets with a business impact level of extreme may be used, but not normally stored in the zone. No storage of these assets is permitted without originator's approval. c. Sensitive and security classified information and assets with business impact level of catastrophic may only be used under exceptional circumstances to meet operational imperatives and requires the originator's approval. No storage is permitted.	Minimum requirements for ongoing access to the security zone are determined by an entity risk assessment. If security classified information and assets are stored in the zone, a security clearance is required for ongoing access at the level required for the highest classified resources the individual will access in the zone. Ongoing access to the zone can be given to individuals without a security clearance or holding different levels of security clearances.	a. Entity office environments. b. Out-of-office or home-based worksites where the entity has control of access to the part of the site used for entity business. c. Airside work areas. d. Interview and front-desk areas where there is segregation of authorised personnel from clients and the public. e. Court houses. f. Vehicle-based work where the vehicle is fitted with a security container, alarm and immobiliser.
Zone Three	Entity restricted office areas. No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control. a. Sensitive and security classified information and assets with a business impact level up to extreme may be used and stored. b. Sensitive and security classified information with a business impact level of catastrophic may be used, but not normally stored, in the zone. Use and storage of catastrophic information requires the originators approval. Temporary storage may be permitted up to five consecutive days.	Minimum requirements for ongoing access to the security zone are determined by an entity risk assessment. If security classified information and assets are stored in the zone, a security clearance is required for ongoing access at the level required for the highest classified resources the individual will access in the zone. Ongoing access to the zone can be given to individuals without a security clearance or holding different levels of security clearances.	a. Security areas within entity premises with additional access controls on authorised personnel. b. Work area where the majority of work performed is up to PROTECTED and there is a limited requirement for personnel to have a clearance at the Negative Vetting Level 1. For example non-National Security entities.
Zone Four	Entity restricted office area. No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. a. Single factor authentication for access control. Sensitive and security classified information with business impact levels up to extreme may be used and stored. b. Sensitive and security classified information with a business impact level of catastrophic may be used, but not normally stored in the zone.	If security classified information and assets are stored in the zone, a security clearance is required for ongoing access at the level required for the highest classified resources stored in the zone. Ongoing access is given to individuals who hold the same level of security clearance for the information and assets stored in the zone.	a. Security areas within entity premises with additional access controls on authorised personnel. b. Work areas where all personnel are required to be cleared at the Negative Vetting Level 1 due to the classification of work performed in the zone.
Zone Five	Entity highly restricted office area. No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual authentication for access control. a. Information classified TOP SECRET or other information with a business impact level of catastrophic may be used and stored. [Note iii]	Security clearance required for ongoing access at the level required for the highest security classified information and assets stored in the zone. Ongoing access is given to individuals who hold the same level of security clearance for the information and assets stored in the zone.	a. Highest security areas in entity premises. b. Australian Intelligence Community facilities.

Table 2 notes:

[i] Use of information includes handling, processing (for example reading). It does not include discussions or audible dissemination (briefings, presentations, conversations) of sensitive or classified information. See PSPF policy: Sensitive and classified information and ASIO Tech note 1/15 for further information.

[ii] For advice on containers applicable for storage of information with the identified business impact level in each zone see the PSPF policy: Sensitive and classified information.

[iii] Mandated in **Requirement 8b** for Zone Five areas used to access sensitive compartmented information, the space must achieve ASIO-T4 Zone Five physical security certification and ASD Sensitive Compartmented Information Facility Accreditation.

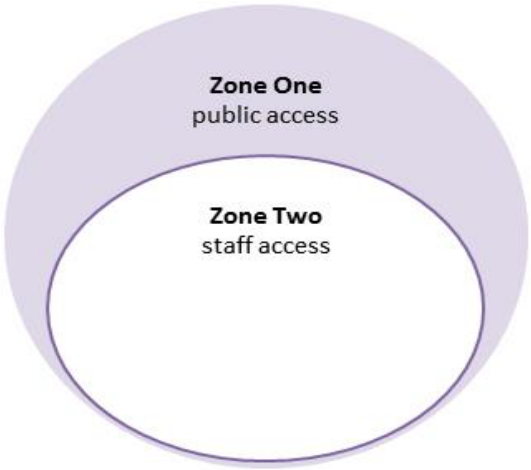
C.4.1 Layering zones

22. The Attorney-General's Department recommends entities layer zones, working in from Zone One public access areas, and increasing the level of protection with each new zone. Multiple layers are the 'delay' design feature to provide more time to detect unauthorised entry and respond before resources are compromised. **Figure 1** demonstrates indicative layering of zones implemented for different purposes. In some instances it may not be possible for higher zones to be fully located within lower zones and entities may need to strengthen higher zone areas.

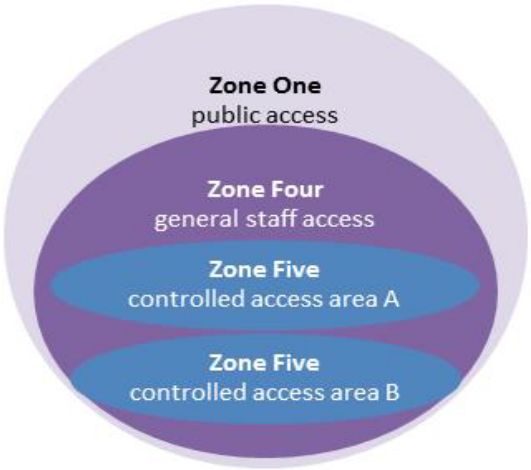
Figure 1 Indicative layering of zones

Entity with all business impact levels

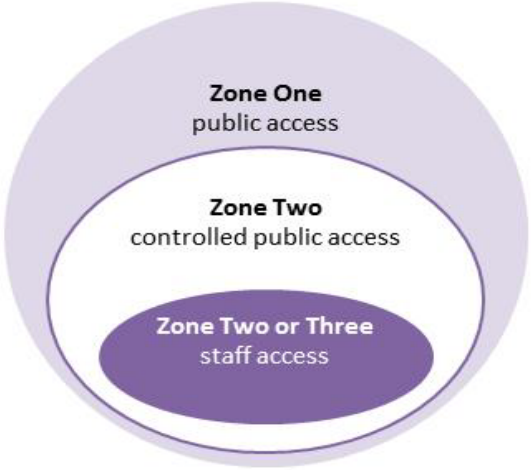
Entity with low-to-medium business impact levels and high public interaction



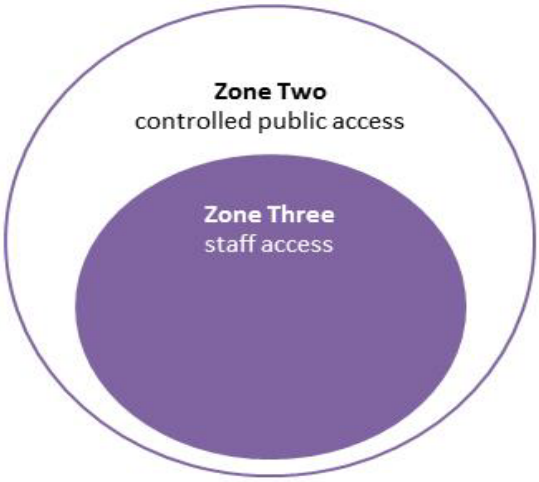
Entity with high business impact levels



Entity with mostly extreme to catastrophic business impact levels



Entity with potentially difficult clients or valuable assets



Facility where all public access is controlled at the outer perimeter

C.5 Individual control elements

23. **Table 3** details the individual control elements used in each zone to achieve the required level of protection. These zone controls provide a level of assurance against:

    a. the compromise, loss of integrity or unavailability of sensitive and security classified information

    b. the compromise, loss or damage of sensitive and security classified assets.

24. The control elements are based on the ASIO Technical Notes for the minimum requirements to protect security classified information and assets. Entity specific assets may require additional security mitigation treatments based on their risk assessment. See the PSPF policy: Security planning and risk management for guidance on risk assessments.

Table 3 Physical protections for security zones—level of assurance required for sharing of sensitive and security classified information and assets

Control element	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Building construction	In accordance with entity risk assessment.	In accordance with applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones. When only used during business hours Normal construction to the Building Code of Australia. When also used out of business hours Normal construction and: a. slab-to-slab construction, or b. tamper-evident ceilings, or c. applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones.	In accordance with applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones. For protection of valuable physical assets, recommend aligning building construction with level 4 (or above) of the Australian Standard 3555.1. In such cases, construction will be considered to meet minimum security zone protections mandated by this policy.	As for Zone Three.	Construction complies with: a. ASIO Technical Note 1/15 – Physical Security of Zones b. ASIO Technical Note 5/12 – Physical Security of Zone 5 (TOP SECRET) areas.
Perimeter doors and hardware		.			
a. Doors	In accordance with entity risk assessment.	Constructed in accordance with ASIO Technical Note 1/15 – Physical Security Zones.	As for Zone Two.	As for Zone Two.	Constructed in accordance with ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas.
b. Locks	In accordance with entity risk assessment. May use commercial locking systems.	As for Zone One.	Minimum SCEC-approved SL3 locks and hardware.	As for Zone Three.	As for Zone Three.
c. Keying systems	Recommend SCEC-approved SL1 or SL2 keying system.	As for Zone One.	SCEC-approved minimum SL3 keying system.	As for Zone Three.	As for Zone Three.
Out-of-hours security alarm system (SAS)	In accordance with entity risk assessment.	In accordance with entity risk assessment. In an office environment, recommend Class 3-4 SAS [Note i] hard wired in the zone.	Type 1 SAS, or Class 5 SAS [Note i] hard wired in the zone. If no SAS, guard patrols performed at random intervals within every four hours required.	Use in accordance with the Type 1A SAS transition policy: a. for new or significantly expanded sites, SCEC-approved Type 1A SAS with SCEC-approved detection devices (designed and commissioned by SCEC-endorsed Security Zone Consultants) b. for existing sites, SCEC Type 1 SAS with SCEC-approved detection devices.	As for Zone Four.
a. Detection devices	In accordance with entity risk assessment.	Hard wired within the zone. Recommend SCEC-approved SL2 or SL3 detection devices.	As for Zone Two.	SCEC-approved SL3 or SL4 detection devices.	As for Zone Four.
b. SAS contractor clearance requirements	In accordance with entity risk assessment.	Contractors who maintain these systems provided with short term access to security classified resources [Note ii] at the appropriate level for the information stored within the zone.	As for Zone Two.	Contractors who maintain these systems cleared at the appropriate level for the information stored within the zone.	As for Zone Four.

Control element	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
c. Management of security alarm systems	In accordance with entity risk assessment.	As for Zone One.	Control of alarm systems directly managed by the entity. Privileged alarm systems operators and users appropriately trained and security cleared to the level of the security zone. All alarm system arming and disarming personal identification numbers are secure.	As for Zone Three.	As for Zone Three.
d. Monitoring and response	All alarm systems to be monitored and responded to in a timely manner. Response capability appropriate to the threat and risk.	As for Zone One.	As for Zone One.	As for Zone One.	As for Zone One.
Interoperability of alarm system and other building management system	In accordance with entity risk assessment.	In accordance with entity risk assessment. If a separate SAS and EACS are used, ensure the alarm cannot be disabled by the access control system.	Ensure the alarm cannot be disabled by the access control system.	Ensure limited one way interoperability in accordance with the Type 1 SAS for Australian Government—Product Integration specification.	Ensure limited one way interoperability in accordance with the Type 1 SAS for Australian Government—Product: Integration specification. The alarm system may disable access control system when activated.
Access control systems	In accordance with entity risk assessment.	In accordance with entity risk assessment. Recommend using identity access card in office environments.	Use identity card and sectionalised access control systems. Use Electronic Assess Control Systems (EACS) where there are no other suitable verification and access control measures in place. Verify the identity of all personnel, including contractors, issued with EACS access cards at the time of issue (using the National Identity Proofing Guidelines to a minimum level 3). Regularly audit EACS.	As for Zone Three, with full audit trail of access control systems. Directly managed and controlled by the entity. Maintained by appropriately cleared contractors Privileged operators and users are appropriately trained and security cleared to the level of the security zone. Regularly audit EACS.	As for Zone Four, with full audit trail of access control systems and dual authentication.
Technical surveillance counter-measures (TSCM)	No requirement.	No requirement.	As determined by a risk assessment.	As for Zone Three.	TSCM and audio security inspection: a. for areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact level b. before conferences and meetings where TOP SECRET discussions are to be held c. seek advice from ASIO-T4 and refer ASIO Technical Note 5/12 Physical Security of Zone Five (TOP SECRET) areas.
Visitor control	In accordance with entity risk assessment.	In accordance with entity risk assessment. Recommended to record visitors, issue passes and escort in sensitive areas.	Visitor and contractor access only for visitors with a need to know and with close escort. Recommend providing receptionists and guards with: a. detailed auditable visitor control and access instructions b. secure method of calling for immediate assistance if threatened.	As for Zone Three and visitor and contractor access with a need to know and with close escort with constant line of sight.	As for Zone Four.

Table 3 notes:

[i] Australian Standard AS/NZS 2201.1 provides guidance on alarm systems.
[ii] Refer to PSPF policy: Access to information for guidance on short term access to security classified resources.

C.5.1 Use of Security Construction Equipment Committee approved products

25. The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment for use by the Australian Government. The SCEC determines which products will be evaluated and the priority of evaluation.

26. Evaluated products are assigned a security level (SL) rating numbered 1 to 4. SL4 products offer high level security, while SL1 products offer the lowest acceptable level of security for government use. Approved items are listed in the SCEC Security Equipment Evaluated Product List, which is only available to Australian Government security personnel and can be obtained from the Protective Security Policy community on GovTEAMS.

27. Entities may use SCEC-approved security equipment even where it is not mandated. Alternatively, entities can use suitable commercial equipment that complies with identified security related Australian and International Standards for the protection of people, information and assets. ASIO-T4 has developed the Security Equipment Guides to assist entities to select security equipment not tested by SCEC. See **Annex A**.

28. SCEC only considers the security aspects of products when evaluating their suitability for use in government. Other aspects of a product, including its safety features, are not considered by SCEC and it is necessary for entities to ensure safety requirements are considered prior to product selection.

C.5.2 Construction of buildings

29. All building work in Australia (including new buildings and new building work in existing buildings) must comply with the requirements of the Building Code of Australia (BCA).[2] Some older buildings may not comply with the current codes. The BCA classifies buildings according to the purpose for which they are designed, constructed or adapted to be used. The BCA requirements for commercial buildings, including facilities used by entities, provide an increased level of perimeter protection as well as protection for assets and information where the compromise, loss of integrity or unavailability would have a business impact level of medium or below.

30. Entities may include additional building elements to address specific risks identified in their risk assessment where building hardening[3] may provide some level of mitigation. For example:

    a. blast mitigation measures

    b. forcible attack resistance

    c. ballistic resistance

    d. siting of road and public access paths

    e. lighting (in addition to security lighting).

31. **Requirement 2** mandates entities for Zones Two to Five, that store sensitive or security classified information and assets, construct facilities in accordance with the relevant sections of ASIO Technical Note 1/15—Physical Security of Zones. It further requires that entities constructing Zone Five areas that will store TOP SECRET information or aggregated information, the compromise, loss of integrity or loss of availability of which may cause catastrophic damage, must also use ASIO Technical Note 5/12—Physical Security of Zone Five (TOP SECRET) areas.

32. ASIO Technical Notes detail the protective security mitigations to maintain the confidentiality and integrity of sensitive and security classified information and assets and are available to Australian Government security personnel only from the Protective Security Policy community on GovTEAMS.

C.5.3 Security alarm systems

33. Security alarm systems provide detection of unauthorised access to entity facilities. However, an alarm system is only effective if it is used in conjunction with other measures designed to delay and respond to

[2] Various state and territory Acts and Regulations set out the legal framework for design and construction of buildings in accordance with the BCA.

[3] Building hardening is the process where a building is made a more difficult or less attractive target.

unauthorised access. The Attorney-General's Department recommends that where possible security alarm systems are configured to monitor devices in high risk areas, for example irregularly accessed areas, roof spaces, inspection hatches and underfloor cavities.

34. Security alarm systems require periodic testing and maintenance from an authorised service provider. The Attorney-General's Department recommends that this occur at a minimum every two years to ensure the alarm system is continually operational.

35. Alarm systems can be broadly divided into two types:

    a. perimeter (or external) intrusion detection systems (PIDS) or alarms

    b. internal security alarm systems.

C.5.3.1 Perimeter alarms

36. Perimeter intruder detection systems may be of value to entities that have facilities enclosed in a perimeter fence or facilities located on a large land holding. Perimeter intruder detection systems provide detection of unauthorised breaches of the perimeter. Entities are encouraged to seek specialist advice when designing and installing these detection systems. The Security Equipment Evaluated Product List contains suitable and approved external alarm components.

C.5.3.2 Internal alarms

37. To protect entity facilities, a combination of SCEC-approved security alarm systems and commercial alarm systems can be used after consideration of the zone requirements and entity risk assessment.

38. Security alarm systems may be single sector or sectionalised to give coverage to specific areas of risk. Sectionalised alarm systems allow greater flexibility as highly sensitive areas can remain secured when not in use and other parts of the facility are open.

39. **Requirement 4** mandates entities use sectionalised security alarm systems where there is a Zone Three, Four or Five to meet the highest security zone requirements in the entity's facility.

40. Alternatively, entities may use separate security alarm systems for different security zones to meet the highest business impact level of the information stored and accessed in the zone.

C.5.3.3 SCEC-approved Type 1A and Type 1 security alarm systems

41. SCEC-approved Type 1A and Type 1 security alarm systems provide malicious insider threat protection not provided by commercial systems.

42. **Requirement 4** mandates entities in Zones Four and Five use:

    a. a SCEC-approved Type 1A or Type 1 security alarm system in accordance with the Type 1A security alarm system transition policy (available for Australian Government security personnel only from the Protective Security Policy community on GovTEAMS) with SCEC-approved detection devices

    b. SCEC-endorsed Security Zone Consultant to design and commission the SCEC-approved Type 1A alarm system.

43. SCEC-approved Type 1A and Type 1 security alarm systems protect SECRET, TOP SECRET and certain codeword information where the compromise, loss of integrity or unavailability of the aggregate of information would cause extreme or catastrophic damage to Australia's national security.

44. ASIO-T4 provides advice on SCEC Type 1A security alarm systems and may approve, other site-specific arrangements for Zones Four and Five.

45. ASD may approve site-specific arrangements for the security of sensitive compartmented information facilities (SCIF).

46. SCEC-endorsed Security Zone Consultants are endorsed to provide physical security advice at the request of Australian Government entities regarding:

    a. design, acceptance testing and commissioning of Type 1A Security Alarm Systems

    b. design and construction of security zones as defined in the Australian Government Protective Security Policy Framework and ASIO–T4 Technical Notes.

47. The Attorney-General's Department recommends entity CSOs or security advisors conduct due diligence checks in respect to a SCEC-endorsed Security Zone Consultant's ability to provide other security services.

48. The SCEC Security Zone Consultant Register on the Security Construction Equipment committee website lists SCEC-endorsed Security Zone Consultants by state and territory.

C.5.3.4 Commercial alarm systems

49. Commercial security alarm systems are graded on the level of protection they provide. The AS/NZS 2201.1 levels of security alarm systems include:

    a. Class 1 or 2 are only suitable for domestic use

    b. Class 3 or 4 are suitable for the protection of normal business operations in most entities

    c. Class 5 is suitable for protection of information and physical assets up to an extreme business impact level.

50. In Zone Three, the Attorney-General's Department recommends, based on the security risk assessment, that entities determine:

    a. whether a commercial security alarm system is appropriate at their facilities, including temporary sites

    b. the security alarm system specifications required.

51. The Attorney-General's Department recommends entities have procedures for the use, management, monitoring and response arrangements of commercial-grade alarm systems. Where possible, entities adopt the administration and management principles set out in the Type 1 security alarm system Implementation and Operation Guide.

52. There are a number of alarm options that may be suitable, including:

    a. duress alarms (or request-for-assistance devices) allow personnel to call for assistance in response to a threatening incident

    b. individual item alarms (or alarm circuits) provide additional protection to valuable physical assets in premises and on display

    c. vehicle alarms to remotely monitor vehicle security where the business impact level of the loss of information or physical assets in the vehicle, or the vehicle itself, is high or above. Remote vehicle alarms may also be linked to remote vehicle tracking and immobiliser systems.

C.5.4 Security guards

53. Security guards provide deterrence against loss of information and physical assets and can provide a rapid response to security incidents. Stationary guards and guard patrols may be used separately or in conjunction with other security measures. The Attorney-General's Department recommends response time for off-site guards be less than the delay given by the total of other controls.

54. The Attorney-General's Department recommends that:

    d. entities base the requirement for guards (their duties and the need for and frequency of patrols) on the level of threat and risk

    e. guarding response time to alarms to be within the delay period given by the physical security controls, although, the highest level of assurance is provided by on-site guards who can respond immediately, 24 hours, seven days a week

    f. entities assess the security clearance requirement for guards based on the security zone requirements and frequency of access. For information, see the PSPF policy: Access to information and the PSPF policy: Eligibility and suitability of personnel

    g. entities only employ, either through the entity or through a commercial guarding company, guards who are licensed in the jurisdiction where they are employed.

C.5.4.1 Out-of-hours guarding

55. Entities may use guard services out-of-hours in response to alarms for all zones. As noted in **Table 4**, entities may use out-of-hours guard patrols instead of a security alarm system in Zones Two and Three.

However, **Requirement 4c** mandates for Zone Three, where out-of-hours guard patrols are used instead of security alarm systems, patrols must be performed at random intervals within every four hours.

C.5.5 Interoperability of alarm systems and other building management systems

56. The more interoperability between security alarm systems and external integrated systems (eg building management systems, closed circuit television and electronic access controls systems) the greater the security alarm system vulnerabilities to unauthorised access and tampering.

57. Where SCEC-approved Type 1 security alarm systems are used, the Attorney-General's Department recommends that any integration with building management systems is in accordance with the *Type 1 security alarm system for Australian Government—Integration specification*. See **Table 3** for zone-specific requirements relating to the interoperability of security alarm systems.

C.5.6 Access control systems

58. An access control system is a measure or group of measures that allows authorised personnel, vehicles and equipment to pass through protective barriers while preventing unauthorised access. Access control can be achieved in a number of ways, for example:

    a. security guards located at entry and exit points

    b. security guards located at central points who monitor and control entry and exit points using intercoms, videophones and closed circuit television cameras

    c. mechanical-locking devices operated by keys or codes

    d. electronic access control systems

    e. psychological or symbolic barriers, can be used for deterrence, but are not considered an effective access control measure, for example signage or crime prevention through environmental design.

59. Each measure has advantages and disadvantages. The measure or mix of measures selected and used will depend on the particular circumstances in which access control will be applied.

C.5.6.1 Authorised personnel access

60. Access to a facility's security Zones Two to Five is restricted to authorised personnel. This includes:

    a. personnel (including contracted and seconded staff) who require access to entity facilities, information or assets (see the PSPF policy: Eligibility and suitability of personnel)

    b. personnel engaged by service providers contracted by an entity where access to entity facilities, information or assets is covered by the terms of the contract (see the PSPF policy: Security governance for contracted goods and service providers)

    c. personnel who, because of business need (although not directly engaged by the entity or by a contracted service provider), require ongoing or regular access that is authorised by the accountable authority (eg senior executives or personnel from portfolio entities who require regular, unescorted access to attend meetings or participate in projects without formal secondment arrangements being put in place).

61. **Requirement 5b** mandates the requirements for an entity's accountable authority (or CSO) to authorise ongoing (or regular) access for people who are not directly engaged by the entity or covered by the terms of a contract or agreement. Before authorising any access the accountable authority (or CSO) ensures:

    a. the person has the required level of security clearance for the respective facility zones (**Requirement 5bi**)

    b. there is appropriate evidence of the business need (a documented business case and risk assessment) that is reassessed on a regular basis and at least every two years (**Requirement 5bii**).

C.5.6.2 Electronic access control systems

62. **Requirement 5** mandates entities use electronic access control systems for Zones Two to Five where there are no other suitable identity verification and access control measures in place. Electronic access control may be used in conjunction with other personnel and vehicle access control measures.

63. The Attorney-General's Department recommends entities:
    a. seek specialist advice when selecting and designing electronic access control systems
    b. use an installer recommended by the manufacturer to install and commission the systems.
64. **Requirement 5** mandates entities for Zones Three to Five:
    a. have sectionalised access control systems and full audit
    b. regularly review audits for any unusual or prohibited activity.
65. The Attorney-General's Department recommends entities regularly audit access control systems for all security zones in accordance with their risk assessment. Audits are used to confirm whether personnel with access have a continued need for access and that any access has been disabled or removed for personnel who have separated from the entity (see the PSPF policy: Separating personnel).

C.5.6.3 Identity cards

66. Identity cards allow the recognition of personnel in entity facilities. **Requirement 5** mandates entities use identity cards with personal identity verification in Zones Three to Five. The Attorney-General's Department recommends entities use identity cards in all facilities, regardless of the level of the zone.
67. The PSPF policy: Eligibility and suitability of personnel requires that entities verify the identity of all personnel using the Document Verification Service. It is recommended that identities be verified to at least Level of Assurance 3 of the National Identity Proofing Guidelines. The Attorney-General's Department recommends entities use the National Identity Proofing Guidelines to at least Level 3 for personnel accessing Zones Three to Five for authorised personnel not covered by the PSPF policy: Eligibility and suitability of personnel. This is considered better practice for access to Zones One and Two.
68. The Attorney-General's Department recommends:
    a. identity cards are:
        i. uniquely identifiable
        ii. worn by all authorised personnel and clearly displayed at all times while on entity premises
        iii. audited regularly in accordance with the entity's risk assessment
    b. identity card-making equipment and spare, blank or returned cards are secured within a Zone Two or higher zone based on the security risk assessment.

C.5.6.4 Authentication factor and dual authentication

69. There are three categories of authentication factors that can be used to validate identity:
    a. What you have (for example keys, identity cards, passes).
    b. What you know (for example personal identification numbers).
    c. Who you are (for example visual recognition, biometrics).
70. Dual authentication requires the use of factors from two different categories, for example an identity card and a personal identification number. **Requirement 5** mandates entities use dual authentication for access to Zone Five. Entities may use dual authentication in other circumstances where their risk assessment identifies a need to mitigate the risk of unauthorised access.

C.5.6.5 Visitor control

71. A visitor is anyone who is not authorised to have ongoing access to all or part of an entity's facilities. Visitor control is normally an administrative process; however, this can be supported by use of electronic access control systems.
72. For management of foreign delegations associated with international agreements and arrangements to which Australia is a party, see the PSPF policy: Security governance for international sharing.
73. **Requirement 5** mandates entities control access to Zones Three to Five. Controlling access can include recording visitor details and issuing visitor passes. Visitor registers are used for this purpose and record the visitor name, entity or organisation, purpose of visit, date and time of arrival and departure. The Attorney-

General's Department recommends entities also issue visitor passes for access to Zone Two when other controls to limit access are not in place.

74. The Attorney-General's Department recommends visitor passes are:
    a. visible at all times
    b. collected and disabled at the end of the visit
    c. audited at the end of the day.
75. Where entities manage the control of access to specific areas, the Attorney-General's Department recommends those areas have their own visitor register at the entry.
76. **Requirement 1** mandates entity personnel escort all visitors in Zones Three to Five. The Attorney-General's Department recommends entities escort visitors in Zone Two unless unescorted access is approved. Entities dealing with members of the public are encouraged to use procedures for dealing with unacceptable behaviour on entity premises or unauthorised access to restricted areas.
77. Visitors can be issued with electronic access control system cards specifically enabled for the areas they may access. In more advanced electronic access control systems, it is possible to require validation at all electronic access control system access points from the escorting officer.
78. Regardless of the entry control method used, the Attorney-General's Department recommends entities only allow visitors to have unescorted access if they:
    a. have a legitimate need for unescorted entry to the area
    b. have the appropriate security clearance
    c. are able to show a suitable form of identification.

C.5.6.6 Perimeter access control

79. Entities that face significant threats and those with larger, multi-building facilities may require perimeter access controls to restrict access to their facilities with the aim to increase the level of deterrence, detection and delay. Types of perimeter control include, but are not limited to:
    a. fences and walls used to define and secure the perimeter
    b. pedestrian barriers used to restrict pedestrian access through fences or walls by installing entry and exit points
    c. vehicle security barriers.
80. The level of protection a fence provides depends on its height, construction, materials, access control and any additional features that increase its performance or effectiveness, for example lighting, signage or connection to an external alarm.
81. The Attorney-General's Department recommends that entities ensure that access points are at least as strong as any fence or wall used.
82. The Security Equipment Evaluated Product List contains details on perimeter intrusion detection devices. Refer to the ASIO-T4 Security Equipment Guide SEG-003 Perimeter Security Fences and SEG-024 Access Control Portals and Turnstiles, available for Australian Government security personnel only from the Protective Security Policy community on GovTEAMS. Related Australian Standards:
    a. AS 1725—Chain-link fabric security fencing and gates
    b. AS/NZS 3016—Electrical installations—Electric security fences.

C.5.7 Locks and door hardware

83. Locks can deter or delay unauthorised access to information and physical assets. The Attorney-General's Department recommends entities:
    a. secure all access points to their premises, including doors and windows, using commercial-grade or SCEC-approved locks and hardware—these locks may be electronic, combination or keyed

b. assign combinations, keys and electronic tokens the same level of protection as the highest classified information or most valuable physical asset contained in the area that is secured by the lock.

84. **Requirement 3** mandates entities use SCEC-approved locks and hardware rated to Security Level 3 in Zones Three to Five (see the Security Equipment Evaluated Product List). Entities may use suitable commercial locking systems in other areas. The Attorney-General's Department recommends entities assess the level of protection needed from doors and frames when selecting locks, as locks are only as strong as their fittings and hardware.

85. The Attorney-General's Department recommends:

a. using SCEC-endorsed locksmiths when using SCEC-approved locks (the SCEC-endorsed locksmith listing can be requested from ASIO-T4 and SCEC)

b. using doors that provide a similar level of protection to the locks and hardware fitted; refer to Australian Standard AS 3555.1—Building elements—Testing and rating for intruder resistance—Intruder-resistant panels.

C.5.7.1 Keying systems

86. Restricted keying systems provide a level of assurance to entities that unauthorised duplicate keys have not been made. To mitigate common keying system compromises, controls include:

a. legal controls, for example registered designs and patents

b. levels of difficulty in obtaining or manufacturing key blanks and the machinery used to cut duplicate keys

c. levels of protection against compromise techniques, such as picking, impressioning and decoding.

87. When selecting a keying system, the Attorney-General's Department recommends entities evaluate:

a. the level of protection provided against common forms of compromise

b. the extent of legal protection offered by the manufacturer

c. supplier protection of entity keying data within their facilities

d. the transferability of the system and any associated costs

e. commissioning and ongoing maintenance costs.

88. The Attorney-General's Department recommends entities strictly control and limit the number of master keys. The loss of a master key may require re-keying of all locks under that master. Key control measures include regular auditing of key registers to confirm the location of all keys in accordance with the entity's risk assessment.

89. The Attorney-General's Department recommends entities locate key cabinets within a facility's secure perimeter and, where possible, within the perimeter of the zone where the locks are located.

C.5.8 Technical surveillance countermeasures

90. TSCMs are implemented to protect security classified discussions from technical compromise. This can be achieved through real-time audio interception using electronic transmitting and receiving equipment or by a TSCM inspection that searches for surveillance devices. These countermeasures are also applicable to covert video recordings.

91. A TSCM inspection identifies technical security weaknesses and vulnerabilities and provides a high level of assurance that an area is not technically compromised, however it is not a guarantee. Developers of covert technology constantly update and develop new equipment and technologies to avoid detection.

92. A TSCM inspection is a security mitigation that deters, detects and defeats covert electronic devices that may be audio, video and imaging technologies. The Attorney-General's Department recommends entities seek advice from ASIO-T4 on the TSCMs required.

93. **Requirement 6** mandates entities carry out TSCM inspections:

a. for areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact level

b. before conferences and meetings where TOP SECRET discussions are to be held.

94. The Attorney-General's Department recommends that TSCM inspections are carried out for areas where security classified discussions will be and are held, including:

a. at the conclusion of initial construction, room renovations or alterations to fittings, for example lighting and furnishings

b. as part of programed technical security inspections undertaken at random intervals

c. before an event

d. following a security breach, for example the unauthorised disclosure of a sensitive discussion.

95. For TSCM advice, contact ASIO-T4. Requests for TSCM inspections can be made in accordance with the Protective Security Circular No 165 Facilitating TSCM inspections in Australia, available for Australian Government security personnel only from the Protective Security Policy community on GovTEAMS. Where entities hold security classified or sensitive telephone conversations, see the ISM for the logical controls that provide protection.

C.5.9 Closed circuit television

96. Entities may use closed circuit television as a visual deterrent to unauthorised access, theft or violence and it can assist in post-incident investigations and alarm activation investigations. A closed circuit television system is not a substitute for physical barriers.

97. To provide appropriate coverage it is important that entities install a sufficient number of cameras to monitor at a minimum:

a. the entire perimeter of the tenanted area or building, particularly publicly accessible areas such as the reception lobby or entry points

b. all facility access points, including car park entrances

c. public access hallways, stairwell and lift lobbies

d. inside loading docks

e. public area boundaries; that is, where there is delineation between a public and security zone.

98. Where closed circuit television images have been used in an incident investigation, the Attorney-General's Department recommends these images are stored in a secure storage container, selected to maintain evidentiary integrity, for a minimum of 31 days post-incident investigation. See the PSPF policy: Physical security for entity resources, C.3. Measures to protect entity information and assets.

99. The Attorney-General's Department recommends entities seek specialist advice in the design of closed circuit television management systems.

100. The Attorney-General's Department recommends entities seek specialist advice for the design of closed circuit television management systems.

C.5.10 Security lighting

101. Internal and external lighting is an important contributor to physical security. It can be used as a deterrent, to detect intruders, to illuminate areas to meet requirements for closed circuit television coverage, assist response teams when responding to incidents at night and to provide personnel with safety lighting in car parks and building entrances. Entities may use motion-detection devices to detect movement and activate lighting as an additional deterrent.

C.6 Security zone certification and accreditation

102. To encourage information sharing among entities, a level of confidence is required that when information is shared, other entities can and will adequately protect it. To achieve this confidence, **Requirement 7** mandates entities certify a facility's zones, before they are used operationally, in accordance with the PSPF and ASIO Technical Notes. **Requirement 8** mandates entities accredit a facility's zones, before they are

used operationally, when the security controls are certified and the entity determines and accepts the residual risks.

C.6.1 Certification

103. Certification of security zones establishes the zone's compliance with the minimum physical security requirements to the satisfaction of the relevant certification authority. For Zones One to Four, the CSO (or security advisor) may certify that the control elements have been implemented and are operating effectively.[4]

104. **Requirement 7** mandates ASIO-T4 is the relevant certification authority for Zone Five security areas that are used to handle TOP SECRET security classified information, sensitive compartmented information or aggregated information where the aggregation of information increases its business impact level to catastrophic

Table 4 Summary of control measures and certification authority

Control measure	Certification authority and applicable requirement				
	Zone One	**Zone Two**	**Zone Three**	**Zone Four**	**Zone Five**
Entity specific threat assessments, for example police threat assessment	CSO (or security advisor) if the need is identified in the risk assessment	CSO (or security advisor) if the need is identified in the risk assessment	CSO (or security advisor) if the need is identified in the risk assessment	CSO (or security advisor) if the need is identified in the risk assessment	CSO (or security advisor) if the need is identified in the risk assessment
Entity security risk assessment	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)
Site security plan	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)
SCEC-approved Type 1A	Not applicable	Not applicable	Not applicable	SCEC-endorsed security zone consultant Note iii (regular servicing by authorised provider required)	SCEC-endorsed security zone consultant Note iii (regular servicing by authorised provider required)
SCEC-approved Type 1 security alarm systems	SCEC-endorsed security zone consultant Note i, ii, iii (regular servicing by authorised provider required)	SCEC-endorsed security zone consultant Note i, ii, iii (regular servicing by authorised provider required)	SCEC-endorsed security zone consultant Note ii, iii (regular servicing by authorised provider required)	SCEC-endorsed security zone consultant Note iii (regular servicing by authorised provider required)	SCEC-endorsed security zone consultant Note iii (regular servicing by authorised provider required)
Commercial alarm system	Suitably qualified system installer or designer Note i (regular servicing by authorised provider required)	Suitably qualified system installer or designer Note i, ii (regular servicing by authorised provider required)	Suitably qualified system installer or designer Note ii (regular servicing by authorised provider required)	Not applicable	Not applicable

[4] For certification and accreditation of ICT systems, see the PSPF policy: Robust ICT systems.

Control measure	Certification authority and applicable requirement				
	Zone One	**Zone Two**	**Zone Three**	**Zone Four**	**Zone Five**
Electronic access control system Note i	Suitably qualified system installer or designer, (current software patches and no obsolete components required)	Suitably qualified system installer or designer, (current software patches and no obsolete components required)	Suitably qualified system installer or designer, (current software patches and no obsolete components required)	Suitably qualified system installer or designer, (current software patches and no obsolete components required)	Suitably qualified system installer or designer, (current software patches and no obsolete components required)
Other zone requirements	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)
Certification (including site inspection)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	CSO (or security advisor)	ASIO-T4

Table 4 notes:

[i] Inclusion of an alarm system or EACS in Zones One and Two are at the entity's discretion.
[ii] If out-of-hours guard patrols or commercial alarm systems are not used instead.
[iii] SCEC-endorsed security zone consultants design and commission SCEC Type 1A SAS and SCEC Type 1 SAS in accordance with the requirements of the *Type 1 SAS Implementation and Operation Guide.*

C.6.2 Accreditation

105. Security zone accreditation involves compiling and reviewing all applicable certifications and other deliverables for the zone to determine and accept the residual security risks. Approval is granted for the security zone to operate at the desired level for a specified time. For Zones One to Five, the CSO (or security advisor) is the accrediting authority when the controls are certified as meeting the requirements of **Table 4**.

106. **Requirement 8** mandates the Australian Signals Directorate (ASD) must accredit Zone Five facilities used to secure and access sensitive compartmented information. As well as Sensitive Compartmented Information Facility (SCIF) accreditation ASD is responsible for management of all SCIFs in Australia.

C.6.3 Recertification and reaccreditation

107. Security zone certification is time-limited. The assessment of compliance is specific to the role of the facility and the assets contained within the facility at the time of certification. This means that facilities may require recertification from time to time

108. Security zone recertification and reaccreditation may be triggered by circumstances including:

a. expiry of the certification due to the passage of time
    i. for Zone Two, which is 10 years
    ii. for Zones Three to Five, which is five years
b. changes in the assessed business impact level associated with the sensitive or security classified information or assets handled or stored within the zone
c. significant changes to the architecture of the facility or the physical security controls used
d. any other conditions stipulated by the accreditation authority, such as changes to the threat level or other environmental factors of concern.

109. For recertification of Zone Fives and SCIFs, the Attorney-General's Department recommends the CSO or delegated security advisor seek advice from ASIO-T4.

C.7 ICT facilities

110. An ICT facility is a designated space or floor of an entity's building used to house an entity's ICT systems, components of their ICT systems or ICT equipment. These facilities include:

    a. server and gateway rooms

    b. datacentres

    c. backup repositories

    d. storage areas for ICT equipment that hold official information

    e. communication and patch rooms.

111. **Requirement 9** mandates entities:

    a. certify and accredit the security zone for ICT sensitive and security classified information

    b. obtain ASIO-T4 physical security certification for outsourced ICT facilities to hold information that, if compromised, would have a catastrophic business impact level

    c. ensure that all TOP SECRET information ICT facilities are in compartments within an accredited Zone Five area and comply with Annex A – ASIO Technical Note 5/12 – Compartments within Zone Five areas.

112. The TOP SECRET compartments within a Zone Five may be certified by the CSO or delegated security advisor. Note certification of ICT systems is also required, see the PSPF policy: Robust ICT systems.

113. The Attorney-General's Department recommends entities situate ICT facilities in security zones that are specific to the facility and are separate to other entity functions.

C.7.1 Access control to ICT facilities and equipment within ICT facilities

114. Where the business impact level is lower than catastrophic, entities may limit access to ICT facilities by implementing:

    a. a dedicated section of the security alarm system, or electronic access control system where used

    b. a guard at the entrance provided with a list of people with a need-to-know or need-to-go into the ICT facility.

115. Entities may seal access to ICT equipment within ICT facilities by using SCEC-approved tamper-evident wafer seals suitable for application to hard surfaces. These seals give a visual indication of unauthorised access to equipment if the seals are removed or broken. Refer to the ASIO-T4 Security Equipment Evaluated Products List, available for Australian Government security personnel only from the Protective Security Policy community on GovTEAMS, when selecting wafer seals.

C.7.2 Outsourced ICT facilities

116. **Requirement 9** mandates entities, before using outsourced ICT facilities operationally, obtain ASIO-T4 physical security certification for the outsourced ICT facility to hold information that, if compromised, would have a catastrophic business impact level.

117. ASIO Protective Security Circular PSV 149 Physical Security Certification of Outsourced ICT facilities provides information to assist entities in the ongoing management of certified outsourced ICT facilities. It is available to Australian Government security personnel only from the Protective Security Policy community on GovTEAMS.

D. Find out more

118. Australian standards:

    a. AS/NZS 2201—Set: Intruder alarm systems set

    b. AS/NZS 2201.1—Intruder alarm systems—Client's premises—Design, installation, commissioning and maintenance

c. AS 2201.2—Intruder alarm systems—Monitoring centres

d. AS 2201.3 —Intruder alarm systems—Detection devices for internal use

e. AS/NZS 2201.5—Intruder alarm systems—Alarm transmission systems

f. AS 1725—Chain-link fabric security fencing and gates (chain-link fences provide minimal security unless used in conjunction with other security measures such as perimeter intrusion detection systems)

g. AS/NZS 3016—Electrical installations—Electric security fences

h. AS 4145.2—Locksets and hardware for doors and windows—Mechanical locksets for doors and windows in buildings

i. AS 4145.5—Building hardware—Controlled door closing devices—Part 5: Requirements and test methods

j. AS 3555.1—Building elements—Testing and rating for intruder resistance—Intruder-resistant panels. (This standard provides a testing and rating system for intruder resistance of any building element.)

k. AS/NZS 2343—Bullet-resistant panels and elements

l. AS/NZS 4421—Guard and patrol security services.

119. Other relevant documents:

a. Building Code of Australia

b. Centre for the Protection of National Infrastructure, Security Lighting: Guidance for Security Managers (2015)

c. Centre For the Protection of National Infrastructure, Catalogue of Impact Tested Vehicle Security Barriers (Available to entities by request through ASIO-T4)

d. Office of the Australian Information Commissioner Guide: Chapter 11: APP 11 – Security of personal information

120. The following guidelines are available to Australian Government security personnel only from the Protective Security Policy community on GovTEAMS. Requests for access can be made by email to pspf@ag.gov.au.

a. ASIO Technical Note 1/15 – Physical Security of Zones

b. ASIO Technical Note 5/12—Physical Security of Zone Five (TS) Areas

c. Annex A – ASIO Technical Note 5-12 Compartments within Zone Five Areas

d. Security Equipment Evaluated Products List (SEEPL)

e. PSV 149 Physical Security Certification of Outsourced ICT facilities

f. Security Equipment Guides:

i. ASIO-T4 Security Equipment Guide SEG-003 Perimeter Security Fences

ii. SEG-024 Access Control Portals and Turnstiles.

121. The following PSPF policies and guidance are available on the Protective Security Policy website:

a. PSPF policy: Sensitive and classified information

b. PSPF policy: Security planning and risk management

D.1 Change log

Table 5 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy
V2018.2	May 2019	C.4	Table 2 note i Use of information – removed discussions from the definition consistent with content of PSPF policy: Physical security for

Version	Date	Section	Amendment
			entity resources

Annex A. Summary of SCEC-tested equipment and guidelines in selecting commercial equipment

1. **Annex A Table 1** provides a summary of the equipment that is tested by SCEC and appears in the SEEPL and Security Equipment Guides.
2. This list is periodically reviewed to meet the Australian Government's physical security needs.
3. Evaluated products are assigned a security level (SL) rating. The numbers in these levels indicate the relative 'security strength' of the item. SL4 products offer a high level of security, while SL1 products offer the lowest acceptable level of security of government use.

Annex A Table 1 SCEC-tested equipment and assigned SL rating

	SL1	SL2	SL3	SL4
Type 1A security alarm system	Not applicable	Not applicable	Not applicable	SCEC
Biometrics devices for access control	SEG 014	SEG 014	SCEC	SCEC
Indoor motion detectors	SEG 002	SEG 002	SCEC	SCEC
Magnetic security switches	SEG 011	SEG 011	SCEC	SCEC
Electronic access control system input devices excluding complete systems	SEG 015	SEG 015	SCEC	SCEC
Key switches – electrical	SEG 008	SEG 008	SEG 008	SEG 008
Electronic key cabinets	SEG 013	SEG 013	SCEC	SCEC
Safes – protection of assets	SEG 022	SEG 022	SEG 022	SEG 022
Stand-alone access control devices	SEG 007	SEG 007	SCEC	SCEC
Mortice locks and strikes	SEG 020	SEG 020	SCEC	SCEC
Magnetic locks	SEG 019	SEG 019	SCEC	SCEC
Electric strikes	SEG 012	SEG 012	SCEC	SCEC
Electric mortice locks	SEG 021	SEG 021	SCEC	SCEC
Keying systems	SCEC SEG 029	SCEC	SCEC	SCEC
Padbolts	SEG 017	SEG 017	SCEC	SCEC
Padlocks chains and hasps	SEG 028 for padlocks Commercial quality	SEG 028 for padlocks Commercial quality	SCEC	SCEC
Hinge bolts	Commercial quality	Commercial quality	SCEC	SCEC
Strike shields and blocker plates	Commercial quality	Commercial quality	Commercial quality	Commercial quality
Cable transfer hinges	Commercial quality	Commercial quality	Commercial quality	Commercial quality
Door closers	SEG 006	SEG 006	SEG 006	SEG 006
Access control portals and turnstiles	SEG 024	SEG 024	SCEC	SCEC

	SL1	SL2	SL3	SL4
Door operators	SEG 006	SEG 006	SCEC	SCEC
Doors	ASIO Technical Note 1/15 – Physical Security of Zones	ASIO Technical Note 1/15 – Physical Security of Zones	ASIO Technical Note 1/15 – Physical Security of Zones	ASIO Technical Note 1/15 – Physical Security of Zones
Pits	SCEC	SCEC	SCEC	SCEC
Vehicle security barriers	SEG 004 and PSC 166	SEG 004 and PSC 166	SEG 004 and PSC 166	SEG 004 and PSC 166
Perimeter security fences	SEG 003	SEG 003	SEG 003	SEG 003
Window locks	SEG 026	SEG 026	SEG 026	SEG 026
Ballistic treatments	SEG 031	SEG 031	SEG 031	SEG 031
Fragment retention film	SEG 027	SEG 027	SEG 027	SEG 027
Barrier mounted perimeter intrusion detection systems	SCEC	SCEC	SCEC	SCEC
Ground based perimeter intrusion detection systems	SCEC	SCEC	SCEC	SCEC
Volumetric perimeter intrusion detection systems	SCEC	SCEC	SCEC	SCEC
Wafer seals	SCEC	SCEC	SCEC	SCEC and SEG 030
Single use pouches	N/A	SCEC	Not applicable	Not applicable
Shredders	SEG 001	SEG 001	SEG 001	SEG 001
Destructors	SEG 018	SEG 018	SEG 018	SEG 018
Briefcases	SEG 005	SEG 005	SEG 005	SEG 005

Annex A Table 2 SCEC-tested equipment and assigned class rating

	Class A	Class B	Class C
Security container locks	SCEC	SCEC	SCEC
Secure room doors	SCEC	SCEC	SCEC
Modular secure rooms	SCEC	SCEC	SCEC
Security containers	SCEC	SCEC	SCEC
Security container locks	SCEC	SCEC	SCEC