
Australian Government

# Physical security management guidelines

## Security zones and risk mitigation control measures

Approved

21 June 2011

Version 1.0



**Contact us**

Inquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General's Department
3-5 National Cct
BARTON ACT 2600

Telephone: (02) 6141 6666

copyright@ag.gov.au

| Document details | |
|---|---|
| Security classification | Unclassified |
| Dissemination limiting marking | Publicly available |
| Date of security classification review | July 2013 |
| Authority | Protective Security Policy Committee |
| Author | Protective Security Policy Section<br>Attorney-General's Department |
| Document status | Approved 21 June 2011 |

**Contents**


**1. Introduction ..... 1**

1.1 Purpose ..... 1

1.2 Audience ..... 1

1.3 Scope ..... 1

1.3.1 Use of specific terms in these guidelines ..... 1

**2. Background ..... 3**

2.1 Why the guidelines were developed ..... 3

2.2 Relationship to other documents ..... 3

2.3 Structure of these guidelines ..... 3

**3. Risk mitigation and assurance measures ..... 4**

3.1 The risk management process ..... 4

3.1.1 Additional requirements to meet specific threats ..... 5

3.2 Assurance required for information and physical asset sharing ..... 6

3.2.1 Assurance for security classified physical assets ..... 7

3.3 Site security plans ..... 7

3.3.1 Critical path ..... 8

3.3.2 Crime prevention through environmental design (CPTED) ..... 9

**4. Security Zones ..... 10**

4.1.1 Layering of Zones ..... 13

4.1.2 Zone requirements ..... 15

4.1.3 Accreditation of Zones ..... 19

**5. Individual control elements ..... 21**

5.1 Use of SCEC-approved products ..... 21

5.2 Building construction ..... 21

5.2.1 Construction of buildings ..... 21

5.3 Alarm systems ..... 23

5.3.1 External alarms ..... 24

5.3.2 SCEC Type 1 SAS ..... 24

5.3.3 Commercial alarm systems ..... 24

5.4 Individual alarm options ..... 25

5.4.1 Duress alarms ..... 25

5.4.2 Individual item alarm/alarm circuit ..... 26

5.4.3 Vehicle alarm ..... 27

5.5 Access control systems ..... 27
5.5.1 Dual authentication ..... 27
5.5.2 Electronic access control systems ..... 28
5.5.3 Identity cards ..... 29
5.6 Interoperability of alarm system and other building management systems ..... 29
5.7 Visitor control ..... 30
5.7.1 Visitor registers ..... 30
5.7.2 Removal of persons from agency premises ..... 31
5.7.3 Access by the media ..... 31
5.8 Receptionists and guards ..... 32
5.8.1 Out-of-hours guarding ..... 32
5.9 Locks and door hardware ..... 33
5.9.1 Locks ..... 33
5.9.2 Keying systems ..... 33
5.9.3 Key control ..... 34
5.9.4 Combination settings ..... 35
5.9.5 Doors ..... 36
5.10 CCTV coverage ..... 36
5.11 Security lighting ..... 38
5.12 Perimeter access control ..... 38
5.12.1 Fences and walls ..... 38
5.12.2 Pedestrian barriers ..... 39
5.12.3 Vehicle barriers ..... 39
5.13 Security containers and cabinets ..... 39
5.13.1 SCEC-approved security containers ..... 40
5.13.2 Commercial safes and vaults ..... 40
5.13.3 Vehicle safes ..... 41
5.14 Security rooms, strongrooms and vaults ..... 41
5.15 Other controls ..... 46
5.15.1 Vehicle immobilisation ..... 47
5.15.2 Front counters and interview or meeting rooms ..... 47
5.15.3 Mailrooms and delivery areas ..... 47
5.15.4 Technical surveillance counter measures and audio security ..... 47
5.15.5 Conference security ..... 48

**6. Physical security elements in administrative security ..... 49**
6.1 Transporting information and physical assets ..... 49
6.1.1 Valuable physical assets ..... 49
6.1.2 Classified information ..... 49
6.2 Destruction equipment ..... 50
6.2.1 Shredders ..... 50
**Annex A: Physical security measures checklist ..... 52**
**Annex B: Physical security terms for inclusion in the Australian Government lexicon of security terms ..... 59**
**Annex C: Summary of equipment tested by the Security Construction and Equipment Committee and guidelines to assist agencies in selecting commercial equipment ..... 62**
**Annex D: Summary of jurisdictional guard licencing legislation ..... 65**
**Annex E: Legislation covering CCTV installation and usage ..... 66**
**Annex F: Safe and vault types ..... 68**

## Amendments

| No. | Location | Amendment |
|---|---|---|
| | | |
| | | |
| | | |

# 1. Introduction

## 1.1 Purpose

The *Australian Government physical security management guidelines—Security zones and risk mitigation control measures* provide guidance on achieving a consistent approach to determining physical security controls in agency facilities.

They aid agencies to protect their people, information and physical assets.

## 1.2 Audience

This document is intended for:

- Australian Government security management staff
- contractors to the Australian Government providing physical security advice and services, and
- any other body or person responsible for the security of Australian Government people, information or physical assets.

## 1.3 Scope

These guidelines relate to physical security measures:

- within Australian Government facilities
- facilities handling Australian Government information and physical assets, or
- where Australian Government employees are located.

**Note**: Where legislative requirements are higher than controls identified in these guidelines—legislative controls take precedence and are to be applied.

Agencies are to protect any information or physical assets provided by another government in accordance with international agreements, see PSPF Governance arrangements—4.10 International security agreements.

These guidelines include advice on the Australian Government's expectations for the protection of Australian information and physical assets by foreign governments.

### *1.3.1 Use of specific terms in these guidelines*

In these guidelines the terms:

- 'need to'—refers to a legislative requirement that agencies must meet
- 'are required to' or 'is required to'—refer to a control:
  - to which agencies cannot give a policy exception, or
  - used in other protective security documents that set controls

- ‘are to’ or ‘is to’—are directions required to support compliance with the mandatory requirements of the physical security core policy, and
- ‘should’—refers to better practice; agencies are expected to apply better practice unless there is a reason based on their risk assessment to apply alternative controls.

For details on policy exceptions see the *Australian Government physical security management protocol,* section 1.4.

# 2. Background

## 2.1 Why the guidelines were developed

The *Australian Government physical security management guidelines—Security zones and risk mitigation control measures* provide a consistent and structured approach to determining:

- the business impact of information, people and physical assets
- the level of control required to:
  - meet the threat environment
  - give suitable protection to information, people and physical assets
  - provide assurance to other agencies for information sharing, and
- the types of controls that are suitable.

The guidelines will:

- aid in establishing consistent terminology for physical security across the Australian Government, and
- give agencies a framework for the assurance needed to share information and physical assets.

## 2.2 Relationship to other documents

These guidelines support the implementation of the Protective Security Policy Framework (PSPF). In particular, they support the *Australian Government physical security protocol*. They are part of a suite of documents that aid agencies to meet their physical security requirements.

The protocol and guidelines are available from www.ag.gov.au/pspf.

## 2.3 Structure of these guidelines

These guidelines are broadly divided into four sections:

- risk mitigation and assurance measures
- the Security Zones methodology and requirements
- details of individual control measures, and
- a checklist for agencies reviewing physical security measures.

# 3. Risk mitigation and assurance measures

Agencies are to base any physical security mitigation measures to protect people and physical assets on their identified risks.

To give assurance in information sharing arrangements an agency is required to:

- reduce the residual risks to an acceptable level to the agency, or where this is not possible, lower the likelihood of compromise, loss of availability, or loss of integrity as much as possible, then
- apply minimum controls determined by the business impact level of the compromise, loss of availability or loss of integrity of the information.

## 3.1 The risk management process

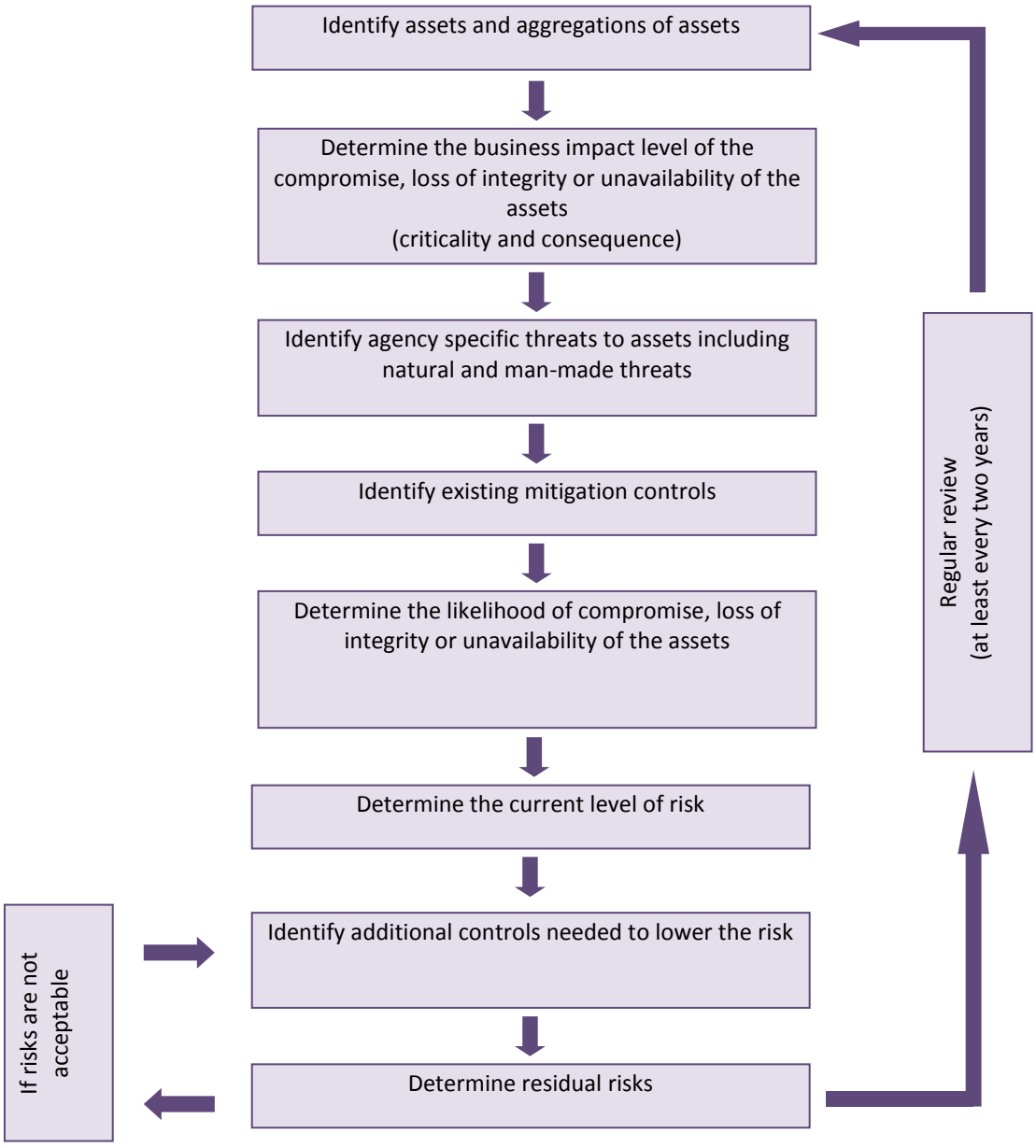
Agencies are to undertake a full security risk assessment in accordance with:

- the Australian Standard AS/NZS ISO 31000:2009 *Risk Management – Principles and guidelines*, and
- the Australian Standards HB 167:2006 *Security risk management*

when deciding which risk mitigation controls are required. See PSPF Governance arrangements—Security risk management (GOV-6).

A summary of the steps used to identify and value assets (including information and people), determine and mitigate the risks of compromise or loss of integrity or unavailability of those assets is in Figure 1. The full risk management process is detailed in HB 167:2006 *Security risk management*.

**Figure 1: Risk mitigation component of the risk assessment process**




### *3.1.1 Additional requirements to meet specific threats*

Threat assessments are used to inform agency risk assessments.

Some threats increase the likelihood of harm to people, or compromise information or physical assets; these will need additional or higher level controls to mitigate the threats.

Threats may affect the whole agency or be site or area specific. Specific threats to members of staff, clients and the public or individual assets should be considered. For further advice on identifying threats, see the HB 167:2006 *Security risk management*, section 4.

Agencies are to assess threats using internal and, if appropriate, external sources such as local police and other authorities.

Threat assessments are to be obtained for all facilities holding TOP SECRET or Codeword information from the ASIO National Threat Assessment Centre (NTAC). NTAC threat assessments may be sought for other facilities where there are national security risks.

Specialist advice should be sought about the risk of natural disasters and suitable mitigation strategies when selecting sites. Agencies at risk from natural disasters should select security products that protect against these when hardening facilities against physical security risks.

**Some threats to facilities that may require additional physical controls**

The following list identifies some possible additional threats that may increase the likelihood of compromise of information or physical assets, or harm to people within agencies. This list is indicative, not definitive:

- **Agency programs**—inherent risks in agency programs.
- **Public knowledge of facility uses**—ranging from no public knowledge to full public knowledge of contentious programs undertaken at the facility.
- **Level of neighbourhood crime**—ranging from occasional minor crime to regular major or organised crime.
- **Client violence**—ranging from occasional non-confrontational contact with clients to regular client contact which may lead to violence.
- **Public violence**—ranging from little to no public contact to regular public protests that may be violent.
- **Terrorism**—which may lead to violence against personnel or facilities, or covert access to sensitive information.
- **Shared facilities**—ranging from single use facilities to co-tenancies with private high risk tenants. (Work areas within an agency with diverse programs may also be considered as sharing facilities).
- **Attractiveness of information and physical assets**—ranging from little value to information and physical assets that are attractive to groups of security concern, including foreign intelligence services, issue motivated groups, trusted insiders.

## 3.2 Assurance required for information and physical asset sharing

To encourage information and physical asset sharing, agencies need to have a high level of assurance that other agencies will suitably protect their information and assets. Agencies are to determine business impact of the compromise, loss of integrity or unavailability of their information and assets as part of the security risk assessment to determine the assurance they require.

An agency's risk assessment may identify the need for security control measures that exceed the minimum control measures for security classified information.

Table 1 gives broad descriptions of business impact levels. For details on determining business impact levels see the *Australian Government protective security governance management guidelines—Business impact levels*.

**Table 1: Business impact levels**

| Business impact | Description |
|---|---|
| Low | Could be expected to harm government agency operations, commercial entities or members of the public |
| Medium | Could be expected to cause limited damage to national security, government agency operations, commercial entities or members of the public |
| High | Could be expected to damage government agency operations, commercial entities or members of the public |
| Very high | Could be expected to damage national security |
| Extreme | Could be expected to seriously damage national security |
| Catastrophic | Could be expected to cause exceptionally grave damage to national security |

### *3.2.1 Assurance for security classified physical assets*

An agency holding security classified physical assets—that is, assets that are classified in their own right, not because of any information held on them—are to determine the physical controls required on a case-by-case basis based on:

- any requirements imposed by the asset owner, or
- the agency's risk assessment and the consequences of the assets compromise loss or damage

whichever is the higher.

## 3.3 Site security plans

Agencies are to evaluate each of their sites separately. These may be further subdivided into separate work areas where there is considerable variation in risks to each work area.

A site security plan documents measures to counter identified risks to an agency's functions, information, people and physical assets at a designated site.

Agencies are to evaluate the different risks to their facilities, people, information functions and physical assets during business hours and out-of-hours. Controls needed during operating hours should take into account the increased risks from public and client contact as well as insider threats. While these risks still exist out-of-hours, there may be a higher risk from external sources such as break and enters.

Agencies are to assess the impact of the compromise, loss of integrity or unavailability of their site security plans to their security and operations, and apply a suitable Dissemination Limiting Marker (DLM) or security classification. See the *Australian Government information security management guidelines—Security classification system*.

A site security plan should include:

- measures that are scalable to meet increases in threat levels
- the location and nature of the site

- whether the agency has sole or shared ownership or tenancy of the site
- whether the public or other non-agency personnel have a right of entry to the site
- what security classification of information is to be stored, handled, processed or otherwise used in each part of the site
- ICT assets, including, but not limited to, data, software, hardware and portable equipment such as laptops, personal electronic devices
- ICT-related equipment (for example, file servers, workstations, terminals, main distribution frames and cabling) and utilities
- any other resources that will be on the site
- an indication of whether every part of the site is intended to have the same level of security
- what protective measures will be required for:
  - the site as a whole
  - particular areas within the site (for example, part of a floor which will hold information of a higher classification than the rest of the site)
- what differing measures will be required for:
  - storage, handling and processing of security classified information, and
  - security classified or otherwise sensitive discussions and meetings.

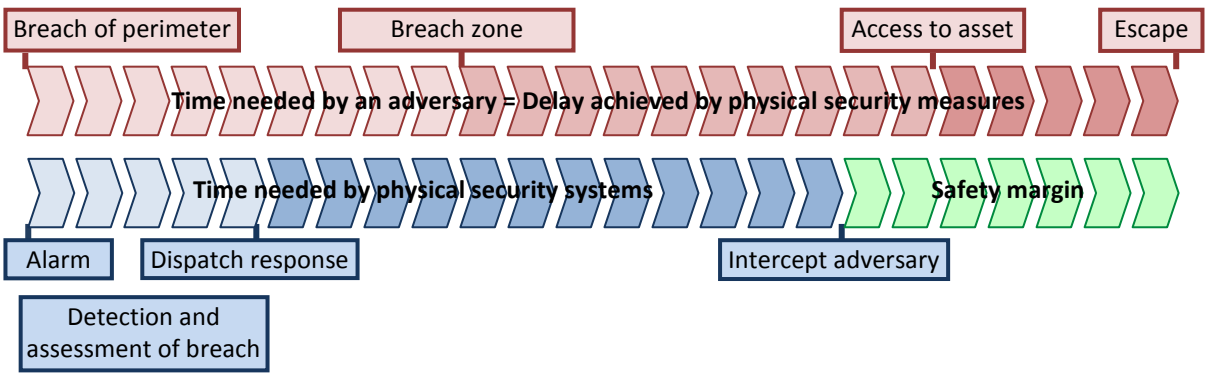
### *3.3.1 Critical path*

The effectiveness of security controls is measured by the probability of detection at the point where there is enough time for a response team to interrupt an adversary. The critical path is the adversary path with the lowest probability of interruption.

An adversary path is an ordered sequence of actions against an asset that could result in it being compromised. Adversaries could normally be expected to take the easiest and most direct route.

Early detection of unauthorised access enables a quicker response. Ideally interception should occur before access to the asset, but this depends on the asset and the security objectives. Interruption may not be required if tamper evidence is the objective for protecting the asset. This concept is illustrated in Figure 2.

**Figure 2: Relationship between detecting, delaying and responding to a perimeter security breach**



The effectiveness of security elements will influence:

- probability of detection—the cumulative probability of detecting an adversary
- cumulative delay—the combined minimum delay time along the adversary path
- response—the time for a response to reach a point of detection, and
- interruption—occurs when the response time is less than the delay provided, measured from the first point of detection.

Further information on applying critical path analysis is available in *Physical Protection Systems* by Mary Lynn Garcia and the companion assessment tool.

### *3.3.2 Crime prevention through environmental design (CPTED)*

CPTED should be an integral part of facility planning. The approach emphasises the importance of identifying which aspects of the physical environment could affect the behaviour of people and uses these aspects to minimise crime. Many publications (such as the two referenced below) deal with CPTED in the domain of private housing and public areas, but it is equally applicable in government agencies.

CPTED principles may identify different solutions that those identified for other security needs, for example counter-terrorism. The mitigations used should be based on an agency's risk assessment.

More information on CPTED can be found at:

- *Designing Out Crime: crime prevention through environmental design* an early publication from the Australian Institute of Criminology focusing on household crime; the concepts are transferable to organisations.
- *Crime Prevention through Environmental Design Guidelines for Queensland* a Queensland Police publication released in 2007.

# 4. Security Zones

Security Zones provide a methodology for physical security mitigation based on the security risk assessment.

The Zones are a guide to developing a facility, building and rooms physical security plan. Application of requirements based on the business impact level of any compromise, loss of integrity or unavailability of information and physical assets within zones gives assurance in information and asset sharing arrangements.

The primary outcomes of the zones methodology are to give a scalable level of protection from:

- unauthorised or covert access, and
- forcible attack.

The physical security measures in higher level zones should include tamper evidence and also be:

- highly resistant to covert attack to protect information, or
- highly resistant to forcible attack to protect assets.

For further information see Layering of Zones.

Table 2 provides broad descriptions of the functions that agencies can undertake in the Zones, the information and assets they can handle and store in the Zones, and some examples of Security Zones.

**Table 2: Security Zones**

| Zone type | Description | Examples |
|---|---|---|
| Zone One | Public access areas<br>• Zone includes perimeter access control measures.<br>• Storage of information and physical assets with low to medium business impact levels needed to do business.<br>• Use of information and physical assets of which the compromise, loss of integrity or unavailability would have a high or very high business impact is permitted. Storage not recommended but is permitted if unavoidable.<br>• Use of information and physical assets above very high only under exceptional circumstances with approval of the originating/owning agency. No storage permitted.<br>(The inner perimeter of zone one may move to the building or premise perimeter out of hours if exterior doors are secured.) | Building perimeters and public foyers.<br>Interview and front-desk areas where there is no segregation of staff from clients and the public.<br>Out-of-office temporary work areas where the agency has no control over access.<br>Field work including most vehicle-based work.<br>Exhibition areas with no security controls.<br>Public access parts of multi-building facilities. |

| Zone type | Description | Examples |
|---|---|---|
| Zone Two | Unrestricted employee and contractor access with restricted public access.<br>• Storage of information and physical assets of which the compromise, loss of integrity or unavailability would have a business impact up to very high is permitted.<br>• Use of information and physical assets with an extreme business impact is permitted, but not normally stored in area. No storage of these assets without originator's approval.<br>• Use of information and physical assets with a catastrophic business impact only under exceptional circumstances to meet operational imperatives with approval of the originating agency. No storage permitted.<br>(The outer perimeter of Zone Two may move to the building or premise perimeter out of hours if exterior doors are secured.) | Normal agency office environments.<br>Normal out-of-office or home-based worksites where the agency has control of access to the part of the site used for agency business.<br>Military bases and airside work areas.<br>Interview and front-desk areas where there is segregation of staff from clients and the public.<br>Court houses.<br>Vehicle-based work where the vehicle is fitted with a security container, alarm and immobiliser.<br>Exhibition areas with security controls and controlled public access. |
| Zone Three | Limited employee and contractor access with escorted or closely controlled visitors only.<br>• If security classified information is held, all employees with ongoing access are to hold a security clearance at the highest level of the information they access in the Zone.<br>• Storage of information or physical assets of which the compromise, loss of integrity or unavailability would have a business impact up to extreme is permitted.<br>• Use of information with catastrophic impact level is permitted, but not normally stored in area. | Security areas within agency premises with additional access controls on staff.<br>Exhibition areas for very valuable assets with specific item asset protection controls and closely controlled public access.<br>Areas used to store art works or items of cultural significance when not on display.<br>Court rooms. |

| Zone type | Description | Examples |
|---|---|---|
| Zone Four | Strictly controlled employee access with personal identity verification as well as card access. Only contractors and visitors with a need to know and closely escorted given access.<br>• If security classified information is held, all employees with ongoing access are to hold a security clearance at the highest level of the information held in the Zone.<br>• Storage of information of which the compromise, loss of integrity or unavailability would have a business impact up to extreme is permitted.<br>• Storage of or physical assets of which the compromise, loss of integrity or unavailability would have a business impact up to catastrophic is permitted.<br>• Use of information with catastrophic impact level is permitted, but not normally stored in area.<br>(These areas are normally only constructed as an alternative to Zone Three where the facility also has a Zone Five.) | Security areas within agency premises with additional access controls on staff.<br>Exhibition areas for very valuable assets with specific item asset protection controls and closely controlled public access.<br>Areas used to store art works or items of cultural significance when not on display. |
| Zone Five | Strictly controlled employee access with personal identity verification as well as card access. Only contractors and visitors with a need to know and closely escorted given access.<br>• All employees with ongoing access are to hold a security clearance at the highest level of the information held in the Zone.<br>• Storage of information classified TOP SECRET, Codeword information or large quantities of other information where the compromise, loss of integrity or unavailability of the aggregate of the information would have a catastrophic business impact. | Highest security areas in agency premises.<br>Australian Intelligence Community facilities. |

### *4.1.1 Layering of Zones*

Agencies should layer the Zones working in from Zone One—that is, public access areas—increasing the protection with each new Zone. Multiple layers will give agencies a greater delay to allow response to any unauthorised entry.

Zones should give greater periods of delay as levels increase. By layering Zones within Zones the delay is cumulative giving the agency greater time to respond before unauthorised access to the inner Zone. Figure 3 provides some examples of Zone configurations.

In some instances it is not possible for higher Zones to be located fully within lower Zones. Agencies may need to additionally strengthen external walls of the higher Zones.

Zone One may also include perimeter protection measures, for example blast mitigation, counter-terrorism protection, etc. As zone levels increase, the protective security measures progressively change to protect information and physical assets.

The number of Zones that individual agencies need depends on the different levels of assurance and segregation required.

Agencies should determine the minimum and maximum Zones required in facilities, for example agencies with:

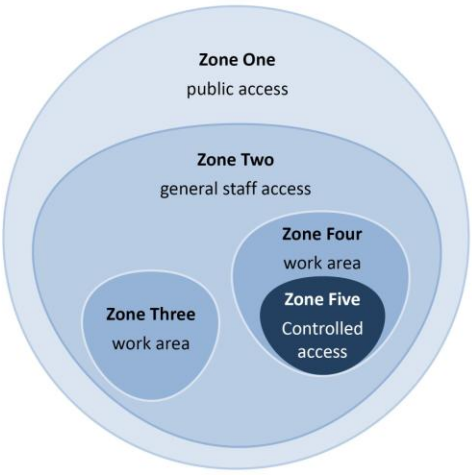
- low to medium business impact levels—may only need Zone One or Zone Two
- up to and including high to very high business impact levels—may need Zone One and Zone Two
- up to and including extreme business impact levels—may need Zones One to Three, and
- up to and including catastrophic business impact levels—may need Zones One to Five.

See the *Australian Government protective security governance management guidelines—Business impact levels*.

Agencies holding information or physical assets of which the compromise, loss of integrity or loss of availability would have an extreme business impact may choose to use Zones Three or Four for all their general staff access areas, rather than Zone Two.

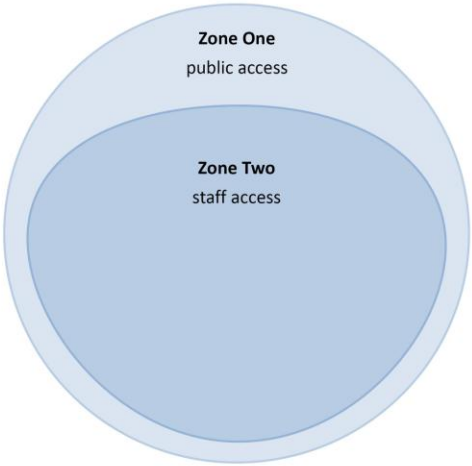
Agencies with information of which the compromise, loss of integrity or loss of availability would have a catastrophic business impact may choose to use Zone Four for all their general staff access.

## Figure 3: Indicative layering of Zones

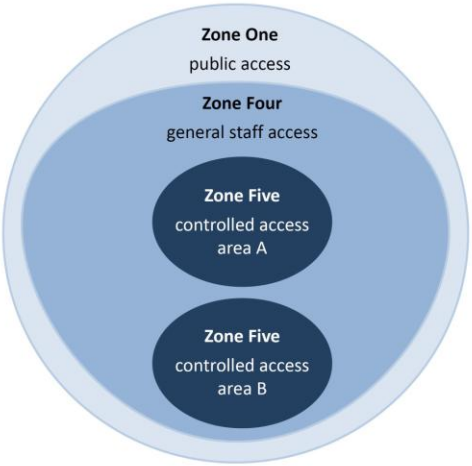



**Agency with all levels of business impact**

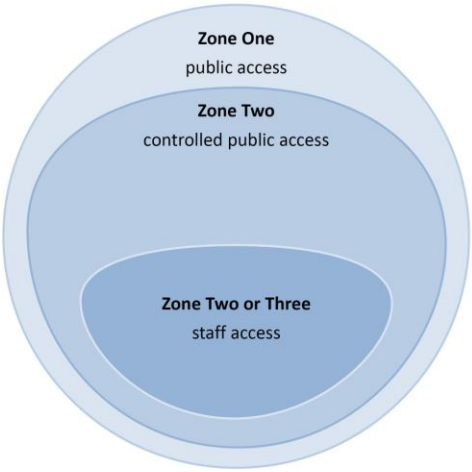

**Agency with low to medium business impact levels and high public interaction**



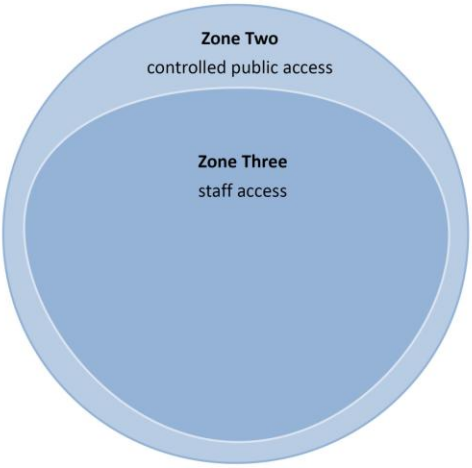

**Agency with high to very high business impact levels**




**Agency with mostly extreme to catastrophic business impact levels**




**Agency with potentially difficult clients or valuable assets**




**Facility where all public access is controlled at the outer perimeter**

### *4.1.2 Zone requirements*

Agencies are to use controls to treat their identified risks. They are to then apply the controls in the following table which identifies the requirements for each zone to give assurance in information or physical asset sharing arrangements.

The zone requirements provide a level of assurance against:

- the compromise, loss of integrity or unavailability of information, and
- the compromise, loss or damage of physical assets.

These objectives may not encapsulate all types of protection required for people, information and physical assets. Agencies should determine additional treatments based on their risk assessments.

Zone requirements are detailed in Table 3.

**Table 3: Zone requirements**

Further details on each type of control can be found in section 5 (by following the links in control components below).

| Control components | Level of assurance required for information and physical asset sharing | | | | |
|---|---|---|---|---|---|
| | **Zone One** | **Zone Two** | **Zone Three** | **Zone Four** | **Zone Five** |
| Building construction | Determined by an agency's risk assessment | **During business hours**<br>Normal construction to the Australian Building Code<br>**Out-of-hours**<br>Normal construction and:<br>• Slab-to-slab construction, or<br>• tamper evident ceilings, or<br>• construction to ASIO *Technical Note – Physical Security of Intruder Resistant Areas/SR2 Rooms* | Construction:<br>• to ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms* or information only, or<br>• using elements tested to AS 3555.1–2003 level 4 or above for valuable physical assets | Construction:<br>• to ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms* or information only, or<br>• using elements tested to AS 3555.1–2003 level 4 or above for valuable physical assets | Construction to:<br>• ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms*, and<br>• *Supplement to the Technical Note – Physical Security of TOP SECRET areas* |
| Out of hours Alarm systems[1, 2] | Determined by an agency's risk assessment | Determined by an agency's risk assessment, recommended for office environments AS 2201 Class 3–4 alarm which should be hard wired within the Zone | AS 2201 Class 5 alarm which should be hard wired within the Zone (use of SCEC approved detection devices is recommended) | SCEC Type 1 (using SCEC approved detection devices) | SCEC Type 1 (using SCEC approved detection devices) |
| Out of hours alarm response[2] | • Determined by an agency's risk assessment | | • Determined by an agency's risk assessment (response should be within the achieved delay from other physical security measures) | | |
| Access control systems[1] | Determined by an agency's risk assessment | Determined by an agency's risk assessment, recommended for office environments<br>ID card required for access | ID card and sectionalised access control system | ID card and sectionalised access control system with full audit trail | ID card and sectionalised access control system with Dual authentication |

| Control components | Level of assurance required for information and physical asset sharing | | | | |
|---|---|---|---|---|---|
| | **Zone One** | **Zone Two** | **Zone Three** | **Zone Four** | **Zone Five** |
| Locks | Determined by an agency's risk assessment. Agency's buildings should be locked out of hours | Commercial locking system | Commercial locking system | SCEC approved locking system | SCEC approved locking system |
| Keying systems | Determined by an agency's risk assessment | Commercial restricted keying system recommended | SCEC approved keying system | SCEC approved keying system | SCEC approved keying system |
| Interoperability of alarm system and other building management systems[3] | Determined by an agency's risk assessment | If an alarm is used it cannot be disabled by the access control system | Alarm cannot be disabled by the access control system | Limited one way in accordance with the *Type 1 SAS for Australian Government—Integration specification* | The alarm is a standalone system and may disable access control system when activated |
| Visitor control | Determined by an agency's risk assessment | Visitor register with visitors escorted in sensitive parts of facility | Escorted visitors in whole of zone | Visitors excluded unless there is an identified need | Visitors excluded unless there is an identified need |
| Storage of official information | Determined by an agency's information holdings, see Table 5: Selecting security containers or rooms to store official information | | | | |
| Storage of valuable physical assets | Determined by an agency's physical asset holdings, see Table 6: Selecting safes or vaults to protect valuable physical assets | | | | |
| CCTV coverage[4] | Determined by an agency's risk assessment | | | | |
| Security lighting[5] | Determined by an agency's risk assessment | | | | |
| Perimeter access control | Determined by an agency's risk assessment | | | | |
| Individual alarm options | Determined by an agency's risk assessment | | | | |
| Other controls to address specific risks | Determined by an agency's risk assessment. Some examples of additional control measures for specific risks are at Table 7: Additional controls to address specific risks | | | | |

**Notes:**

1. Agencies are to use sectionalised alarm and access control systems when there are Zones Three and above in a facility. The alarm and access control systems are to meet the needs of the highest Zone in the facility. Alternatively agencies may use separate alarm and access control systems for different Zones.
2. Out-of-hours guards, performing regular information container and physical asset inspections and patrols of facilities may be a suitable replacement for an alarm system in Zones One to Three. Response time for off-site guards should be less than the delay given by the total of other controls.
3. Interoperability of the alarm system and electronic access control systems (EACS) is to meet the highest requirement for all zones covered by the alarm system and EACS. Where SCEC-approved Type 1 SAS are used, any integration with building management systems is to be in accordance with the *Type 1 SAS for Australian Government—Integration specification.*
4. There may be specific jurisdictional legislation that applies to CCTV coverage of public areas, see Annex E: Legislation covering CCTV installation and usage.
5. Agencies should ensure they use lighting that at least meets the minimum requirements for any CCTV systems used.

### *4.1.3 Accreditation of Zones*

Agency security advisers (ASAs) may accredit agency facilities as Zone One to Zone Four when the controls meet the requirements of Table 4: Summary of certification requirements.

For further information on accreditation requirements for Zones holding TOP SECRET security classified information, certain Codeword information, or aggregations of information where the compromise, loss of integrity or unavailability of the information would have a catastrophic business impact see the *Australian Government physical security management protocol,* section 6.4.

If security classified information is held in Zones Four or Five all employees with ongoing access are to hold a security clearance at the highest level of the information held in the Zone. See the Australian Government personnel security protocol.

**Table 4: Summary of certification requirements**

| Control needed | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|---|---|---|---|---|---|
| NTAC threat assessment | N/A | N/A | Recommended if national security is impacted | Recommended if national security is impacted | Yes |
| Agency security risk assessment | ASA | ASA | ASA | ASA | ASA |
| Agency specific threat assessments eg. police threat assessment, etc | ASA—if need identified in agency risk assessment | ASA—if need identified in agency risk assessment | ASA—if need identified in agency risk assessment | ASA—if need identified in agency risk assessment | ASA—if need identified in agency risk assessment |
| Site security plan | ASA | ASA | ASA | ASA | ASA |
| SCEC type 1 alarm system | SCEC endorsed consultant (if used) | SCEC endorsed consultant (if used) [1] | SCEC endorsed consultant (if used)[1] | SCEC endorsed consultant | SCEC endorsed consultant |
| Commercial alarm system | Suitably qualified system installer/designer[2] | Suitably qualified system installer/designer[1, 2] | Suitably qualified system installer/designer[1] | N/A | N/A |
| Electronic access control system | Suitably qualified system installer/designer[2] | Suitably qualified system installer/designer[2] | Suitably qualified system installer/designer | Suitably qualified system installer/designer | Suitably qualified system installer/designer |
| Other Zone requirements[3] | ASA | ASA | ASA | ASA | ASA |
| Site inspection and certification of suitability to hold TOP SECRET | N/A | N/A | N/A | N/A | ASIO-T4 |
| Site inspection and certification of suitability to hold information below TS | ASA | ASA | ASA | ASA | N/A |
| Accreditation of overall measures | ASA | ASA | ASA | ASA | ASA |

Notes:

1. If Out-of-hours guarding patrols are not used instead.
2. Inclusion of an alarm system and/or EACS in Zones One and Two are at the agency's discretion.
3. See Table 7: Additional controls to address specific risks.

# 5. Individual control elements

This section provides guidance on selecting control measures identified in Table 6.

Agencies may select extra controls not identified in this section in accordance with their risk assessment. Some indicative additional controls are in Table 7.

## 5.1 Use of SCEC-approved products

The Security Construction Equipment Committee (SCEC) tests and approves:

- security products that primarily focus on protecting security classified information of which the compromise, loss of integrity or unavailability would result in a business impact level of high or above
- products that prevent widespread loss of life, and
- other security products that require specialist testing.

These approved items are listed in the SCEC *Security Equipment Catalogue*.

Even where not required an agency may still use SCEC-approved security equipment, or use suitable commercial equipment that complies with identified security related Australian or International Standards, for the protection of people, information or physical assets.

The SCEC is developing the *Security equipment evaluated product list* and SCEC *Guidelines on equipment selection* which will progressively replace the SEC, see Annex C: Summary of equipment tested by the Security Construction and Equipment Committee and guidelines to assist agencies in selecting commercial equipment.

## 5.2 Building construction

### *5.2.1 Construction of buildings*

Agencies should assess the suitability of construction methods and materials to give the protection needed before leasing or constructing premises. Increasing the level of building security—that is, the level of delay provided—afterwards may be expensive or impossible.

Typically buildings are constructed to the *Building Code of Australia*. Some older buildings may not meet this Code.

Buildings are normally classified as domestic or commercial.

Domestic construction provides little protection from unauthorised access; however, intrusion is normally evident as the most common unauthorised access is for theft. Skilled covert access is normally very hard to detect in domestic situations.

Standard commercial office premises normally provide an increased level of perimeter protection over domestic buildings. However, in normal office accommodation internal walls, false ceilings and other normal building techniques reduce the ability of agencies to protect their information and physical

assets. Most commercial office spaces provide protection suitable for assets and information where the compromise, loss of integrity or unavailability would have a business impact of medium or below.

Agencies should include additional building elements to address any specific risks identified in their risk assessment where building hardening may provide some level of mitigation. For example:

- blast mitigation measures
- forcible attack and ballistic resistance
- road and public access paths
- lighting (in addition to security lighting)
- hostile vehicle mitigation, and
- elements of crime prevention through environmental design (CPTED).

Related Australian Standards:

- AS 3555.1:2003 *Building elements—Testing and rating for intruder resistance—Intruder-resistant panels.* (This standard provides guidance on very high grade intruder resistance such as for high security vaults).
- AS/NZS 2343:1997 *Bullet-resistant panels and elements*.

**Slab-to-slab construction**

The use of slab-to-slab construction—that is, the walls are joined directly to the floor and bottom of the next floor or the roof structure—prevents access through false ceilings. Agencies should use slab-to-slab construction at the perimeter of Zones including all access points. The ASIO *Technical Note – Physical Security of Intruder Resistant Areas/SR2 Rooms* provides details on methods to achieve slab-to-slab construction.

As structural changes may have an impact on the integrity of buildings, agencies should seek structural engineering advice before implementing slab-to-slab construction.

The access points for Zone One and Two may vary between business and out of hours; the Zone Two access point may move from an internal access point during business hours to the perimeter of the building or premise out of hours. Agencies may use access points for Zone Two during business hours without slab-to-slab construction when the out-of-hours access point has slab-to-slab construction.

Alternatively agencies may install an intruder-resistant layer in the ceiling, such as metal mesh, to address the problem of removable false ceiling panels where they require intrusion delay for specific rooms. These measures do not give any protection from over-hearing and are not to be used where speech security is needed.

Agencies may also use tamper-evident building techniques to provide some indication of unauthorised access.

**Construction of Zone Five perimeter**

For further information on constructing Zone Five areas to store TOP SECRET information or aggregation of information of which the compromise, loss of integrity or loss of availability may cause catastrophic damage see:

- ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms*, and

- *Supplement to the Technical Note – Physical Security of TOP SECRET Areas*

These guides are only available to ASAs from ASIO-T4.

## 5.3 Alarm systems

Alarm systems can provide early warning of unauthorised access to agencies' facilities.

An alarm system is only of value in conjunction with other measures designed to detect, delay and respond. All alarm systems are to be monitored and linked to a pre-determined response.

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.

Agencies should, where possible, configure alarm systems to continuously monitor detection devices in high risk areas, for example irregularly accessed areas, roof spaces, inspection hatches and underfloor cavities.

Each agency is to have direct management and control of alarm systems in Zone Three and above. Agencies should have direct management and administration of other alarm systems.

Each agency is to use appropriately cleared and trained agency staff as privileged alarm system operators and users in Zone Three and above. Agencies should only use appropriately cleared and trained agency staff as privileged operators and users of other alarm systems.

However, operation functions, such as monitoring and maintenance, may be outsourced.

Agencies are to ensure all alarm system arming and disarming personal identification numbers (PINs) are:

- uniquely identifiable to an individual
- not recorded by the individual, and
- regularly changed in accordance with the agency's risk assessment.

Employees are to advise the ASA of any suspected compromise of PINs as soon as the suspected compromise is identified. The ASA is to disable the PIN and investigate any potential security breach. For details on conducting an investigation see the *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations* to be released shortly.

Agencies should have the default/engineering user codes removed from alarm systems at commissioning.

Agencies should develop appropriate testing and maintenance procedures to ensure the alarm system is continually operational.

Alarm systems can be broadly divided into two types:

- perimeter (or external) intrusion detection systems (PIDS) or alarms, and
- internal security alarm systems (SAS).

Agencies may use out-of-hours guard patrols instead of an alarm system in all Zones up to and including Zone Three, see Out-of-hours guarding.

### *5.3.1 External alarms*

PIDS may be of value to agencies that have facilities enclosed in a perimeter fence. They provide early warning of unauthorised breaches of a facility perimeter. Agencies should seek specialist advice when designing and installing PIDS.

The SCEC *Security Equipment Catalogue* contains approved external alarm components suitable for use.

### *5.3.2 SCEC Type 1 SAS*

The SCEC approves SCEC Type 1 SAS which provide internal system protections not given by commercial systems. Agencies are to use a SCEC Type 1 SAS for the protection of TOP SECRET and certain Codeword information, or where the compromise, loss of integrity or unavailability of the aggregate of information would cause catastrophic damage to Australia's national security—unless ASIO-T4 has approved other site specific arrangements.

Agencies are to use:

- SCEC-approved Type 1 SAS in all Zones Four and Five
- SCEC-endorsed consultants to design and commission SCEC Type 1 SAS, and
- SCEC-approved detection devices with any SCEC Type 1 SAS.

See the SCEC *Security Equipment Catalogue*.

Contractors used to maintain these systems are to be cleared at the appropriate level for the information held within the Zones covered by the SAS in accordance with the *Type 1 SAS Implementation and Operation Guide*.

Agencies contemplating the installation of a SCEC Type 1 SAS are to contact ASIO-T4 to determine current applicable standards.

### *5.3.3 Commercial alarm systems*

Commercial SAS are graded on their level of protection and complexity. Base level systems are only suitable for domestic use—that is, AS 2201.1:2007 Class 1 or 2. Alarm systems that do not comply with AS 2201.1 should not be used.

Mid range SAS are suitable for the protection of normal business operations in most agencies—that is, AS 2201.1:2007 Class 3 or 4.

The highest level of SAS is suitable for the protection of all information and physical assets unless their compromise, loss of integrity or unavailability would cause catastrophic damage.

Where a SCEC Type 1 SAS is not needed, agencies are to determine

- whether a commercial SAS is required at their facilities, including any temporary sites, as part of their risk mitigation strategies, and
- the specifications for any such system.

Agencies are to use AS 2201.1:2007 Class 5 SAS, or SCEC Type1 SAS in Zone Three areas. Alternatively agencies may use guard patrols.

If agencies use a commercial SAS in Zone Two it should meet AS 2201.1:2007 Class 3 or better.

Agencies are to develop procedures to support the use, management, monitoring and response arrangements of a commercial grade alarm system. Where possible, agencies should adopt the administration and management principles set out in the *Type 1 SAS Implementation and Operation Guide.*

Any contractors used to maintain commercial SAS should be cleared to a level appropriate to the information to which they could reasonably be expected to have incidental access in the Zones covered by the alarm system.

Agencies should use SCEC-approved detection devices in Zone Three with a commercial SAS. They may use SCEC-approved detection devices in lower Zones covered by a commercial alarm system. See the SCEC *Security Equipment Catalogue*.

Agencies should use a suitably qualified designer or installer to design and commission any selected commercial alarm systems.

Related Australian Standards:

- AS/NZS 2201 Set:2008 *Intruder alarm systems* set:
  - AS/NZS 2201.1:2007 Intruder alarm systems—Client's premises—Design, installation, commissioning and maintenance
  - AS 2201.2:2004 Intruder alarm systems—Monitoring centres
  - AS 2201.3:1991 Intruder alarm systems—Detection devices for internal use
  - AS/NZS 2201.5:2008 Intruder alarm systems—Alarm transmission systems.

## 5.4 Individual alarm options

The use of building alarm systems, EACS or other facility-wide measures may not be ideal in some situations. This includes, but is not limited to, working away from the office, areas with a high potential for personal violence and protection from the compromise of physical assets in public areas.

There are a number of individual alarm options that may be suitable in some situations, including:

- duress alarms
- individual item alarms, or alarm circuits, and
- vehicle alarms.

### *5.4.1 Duress alarms*

Duress alarms enable employees to call for assistance in response to a threatening incident.

Agencies may be required to use duress alarms activated by dual action duress buttons—that is, depressing two separate buttons to trigger the alarm to reduce the occurrence of false alarms—when a police response is required in some jurisdictions.

**Individual duress alarm**

Individual or mobile duress alarms provide some deterrence to violence when employees are outside the office or circulating in public areas.

Personal duress alarms fall into two broad categories:

- remotely monitored duress alarms, and
- alarms that produce loud noise on activation.

Remotely monitored alarms are suitable for use within facilities where there is a dedicated monitoring and response force. The alarms consist of a personal alarm transmitter linked to the facility, or a separate alarm system.

Noise producing duress alarms rely on response by bystanders. They are more suited for applications external to the agency facilities than monitored duress alarms where there could be considerable delay in response to the alarm. Agencies may use these alarms within a facility where they desire immediate notice of an incident by the people in the immediate area.

**Hidden/fixed duress alarm**

Fixed duress alarms are a type of remotely monitored individual duress alarm. They are normally hard wired and fixed to a location. Agencies should consider equipping public contact areas, including the reception area, counters and interview rooms, with duress alarms where the risk assessment has identified a potential problem.

Hidden duress alarms should**:**

- enable employees to raise an alarm discreetly, and
- be augmented by procedures that provide an appropriate response**.**

Agencies should ensure that:

- all relevant staff are aware of and have regular training and trials with the duress alarm
- the duress alarm is configured as part of an intruder alarm system that complies with AS/NZS 2201 Set:2008, and
- the alarm panel is located within the protection zones of the alarm system in accordance with AS/NZS 2201 Set:2008.

Additional information on installation and monitoring of duress alarms is on the West Australian Police webpage *Standard code for supply and installation of hold-up and duress alarm devices*.

### *5.4.2 Individual item alarm/alarm circuit*

Valuable items, particularly when in public areas such as exhibitions, may not be able to be protected by normal alarm systems. An option is to install individual item alarm circuits or a separate alarm system to monitor individual items. Some possible alarm sensor types that may be suitable are:

- pressure switches
- motion sensors
- CCTV activated alarms, and

- radio frequency identification (RFID) tag systems.

Agencies should seek specialist advice when designing alarm systems for individual items.

### *5.4.3 Vehicle alarm*

Agencies that have field workers often require these employees to work from vehicles that can contain large quantities of valuable equipment.

Most vehicle alarms rely on noise and have similar deterrent value to noise producing personal duress alarms. However, they rely on a response by bystanders if the employee is outside hearing range.

Agencies may consider fitting remotely monitored vehicle alarms where the business impact level of loss of the 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 immobilisation systems.

## 5.5 Access control systems

An access control system is a measure or group of measures designed to allow authorised personnel, vehicles and equipment to pass through protective barriers, while preventing unauthorised access.

They limit access through openings in barriers, such as walls, and give authorised access to information and physical assets being protected.

Access control can be achieved in several ways with the most common being:

- psychological or symbolic barriers—for example, Crime prevention through environmental design (CPTED)
- security staff physically located at entry and exit points
- security staff located at central points who monitor and control entry and exit points using intercoms, videophones, closed circuit television cameras and similar devices
- mechanical locking devices operated by keys or codes, and
- electronic access control systems (EACS).

Each approach has advantages and disadvantages, and the precise method used will depend on the particular application in which access control is required.

Access control systems should provide identity validation by using authentication factors of:

- what you have—keys, ID cards, passes, etc.
- what you know—PINs, etc.
- who you are—visual recognition, biometrics, etc.

### *5.5.1 Dual authentication*

Dual authentication requires the use of two of the factors of access control systems.

Agencies are to use dual authentication to control access to Zone Five.

Agencies may use dual authentication in other circumstances where their risk assessment identifies a significant risk of unauthorised access.

### *5.5.2 Electronic access control systems*

Agencies are to use EACS 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.

Agencies may use sectionalised EACS in a facility to control access to specific areas. EACS sections would normally be the same as sections of agencies' alarm systems, but may also have additional operational access control points not covered by individual alarm sections.

Where EACS and/or other access control measures are implemented to cover a whole facility, agencies are to design them to meet the highest perceived threat and risk level.

Where agencies use multiple EACS and/or other access control measures, the design of each system is to meet the highest perceived threat and risk level in the areas covered by the system.

When used, EACS should typically commence at Zone Two perimeters, but may be used in Zone One for example to control access to car parking.

Agencies should:

- seek specialist advice when selecting EACS, and
- use a designer or installer recommended by the manufacturer to design and commission them.

Agencies are to verify the identity of all people who are issued with access cards for their EACS at the time of issue. See Further information.

Agencies are to regularly audit EACS. Audits should occur in accordance with the agency's risk assessment to determine whether people with access have a continued need to access the system and that any access for people who have left has been disabled/removed.

#### Anti pass back

Anti pass back is designed to prevent misuse of access control systems. Anti pass back establishes a specific sequence in which access cards must be used for the system to grant access.

Anti-pass back controls may also be achieved by linking access control to various other access systems, such as information systems and other physical access controls.

#### Two person access system

Some EACS can be enabled to only allow access to areas when two people are present and will activate an alarm if one leaves the area. This is known as a no-lone-zone. It requires two authorised people to access and exit a designated area.

Agencies should consider using a two person access system when they require a very high level of assurance against compromise or loss of highly classified information or extremely valuable physical assets.

#### Further information

For further advice on personal identity verification (PIV) for access control systems see:

- The National Institute of Standards and Technology (US Dept of Commerce) publication, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems* (PACS), and

- AS 5815:2010 *Protocol for lightweight authentication of identity (PLAID)*, which gives advice on confirming identity for access to logical systems.

There are currently no Australian Standards that provide guidance on designing or installing EACS. The US FIPS 201 and Canadian CAN/ULC-S319 may provide some guidance.

EACS may be integrated with electronic alarm systems. See Interoperability of alarm system and other building management systems.

### *5.5.3 Identity cards*

Identity (ID) cards allow for speedy recognition of employees in agency facilities. Agencies are to use ID cards in Security Zones Three to Five; however, they should be used in all facilities.

Agencies should issue ID cards to all people who have regular access to their facilities, subject to meeting any personnel security requirements.

Agencies are to verify the identity of all people who are issued with identity cards using the *The gold standard enrolment framework*.

ID cards should be:

- worn by employees and clearly displayed at all times in agency premises
- uniquely identifiable, and
- audited regularly in accordance with the agency's risk assessment.

Agencies should discourage employees from wearing ID cards outside agency premises.

ID cards should include a return address for lost cards; it should not identify the facility to which the card gives access. Agencies may include other information on ID cards to improve control of access, such as names, photographs and colours.

EACS access cards can be used as ID cards.

Agencies are to secure all:

- card making equipment, and
- spare, blank or returned cards

within a Zone Two or higher area.

## 5.6 Interoperability of alarm system and other building management systems

SCEC Type 1 SAS may be integrated with EACS and other building management systems in accordance with the principles outlined in the SCEC *Type 1 Alarm system integration specification* available to ASAs from ASIO-T4.

As the level of interoperability between SAS and any external integrated system (EIS)—for example, building management systems, CCTV, EACS—increases, the susceptibility of the SAS to unauthorised access and tampering also increases. In all instances, where an agency SAS has interoperability with other building systems, those other systems is not to be able to disable the SAS while it is operating.

Designers of EIS or sub-systems should be aware of the need to secure EIS to prevent unauthorised access or manipulation, especially when interconnected with an SAS. EIS should be designed with appropriate logical and physical controls.

## 5.7 Visitor control

Visitor control is normally an administrative process; however, this can be augmented by use of EACS. Visitors can be issued with EACS access cards specifically enabled for the areas they may access. In more advanced EACS it is possible to require validation at all EACS access points from the escorting officer.

Regardless of the entry control method used, people should only be given unescorted entry if they:

- are able to show a suitable form of identification
- have a legitimate need for unescorted entry to the area, and
- have the appropriate security clearance; see the *Australian Government personnel security protocol*.

Agencies should consider anyone who is not an employee in a facility or area, or has otherwise been granted normal access to the facility or area, as a visitor. This may include employees from other areas of the agency.

Agencies are to issue visitors accessing Zones Three to Five areas with visitor passes. Agencies should also issue visitors to Zone Two with visitor passes when other controls to limit access are not in place. Passes are to be:

- worn at all times
- collected at the end of the visit
- disabled on return if the passes give access to any agency access control systems, and
- checked at the end of the day and, where the passes are reusable, action taken to disable and recover any not returned.

Agencies are to record details of all visitors to Zone Three to Five areas. Agencies should also record visitor access to Zone Two areas if other control measures are not in place. An agency employee or authorised person should escort visitors.

Agencies may, based on their risk assessment, record visitor details at the:

- facility reception areas, or
- entry to individual security zones.

### *5.7.1 Visitor registers*

Agencies should use visitor registers signed by each visitor and the agency employee authorising the visit. The register may include:

- the name of the visitor
- the visitor's agency or firm or, in the case of private individuals, their private address
- the name of the employee to be visited
- the times of the visitor's arrival and departure, and

- the reason for visit.

The visitor register would normally be located at the facility reception desk unless the desk is unmanned, in which case it should be held by a designated employee within the facility.

Where agencies manage the control of access to specific areas at the entry to the area then those areas should have their own visitor registers.

### *5.7.2 Removal of persons from agency premises*

Agencies are to have documented procedures for dealing with members of the public behaving unacceptably on agency premises or who are present in a restricted area. Employees are to be informed of these procedures.

Police officers have certain powers to respond to these situations. In addition, under section 12(2)(c) of the *Public Order (Protection of Persons and Property) Act 1971*, a person authorised in writing by a Minister or the public authority under the Commonwealth occupying the premises may also be able to exercise certain powers. Section 89 of the *Crimes Act 1914* also allows for the appointment of Authorised Commonwealth Officers by a Minister.

If a member of the public behaves in an unacceptable manner the agency head, person authorised or an Authorised Commonwealth Officer should take the following steps when they consider it necessary for the person to leave the premises:

- advise the person that the officer is a person authorised under the *Public Order (Protection of Persons and Property) Act 1971*, or an Authorised Commonwealth Officer under the *Crimes Act 1914*
- initially seek the person's cooperation to cease the behaviour and/or to leave the premises
- ask the person to stop the behaviour and warn them they could be required to leave the premises immediately
- if the person does not stop the unacceptable behaviour, advise them that due to their behaviour the agency head, person authorised or an Authorised Commonwealth Officer is withdrawing permission for them to be on the premises
- request the person to leave the premises immediately, and
- warn the person that the police will be called if they remain, and of the possible legal consequences of non-compliance with the request to leave.

In most cases the person will agree to leave. If the agency head, authorised person or an Authorised Commonwealth Officer assesses it is safe to do so the person should be accompanied until they have left. However, if they refuse to leave, the agency should contact the police immediately.

No employee or guard is to attempt to physically remove a person from agency premises, unless permitted to do so under legislation. This would normally be left to a police officer. The police contact telephone number should be available to all employees.

### *5.7.3 Access by the media*

Agency employees considering giving access to media representatives should consult the ASA before granting access to agency premises.

In addition to the agency standard visitor control procedures, the following procedures should be followed:

- a designated employee should accompany media representatives throughout the visit
- security classified information is locked away (preferable) or at least protected from view
- additional restrictions are considered when appropriate, such as handing in mobile phones and other recording and communications equipment, and
- the agency media liaison unit or public affairs area is consulted about the arrangements.

The agency may consider additional controls to be necessary for particular sites.

If an agency grants permission for a visit to areas where security classified information is being used or handled, the employee responsible for the media representatives is to remind them that no photographs or recordings of any type can be taken at any time during the visit except with specific agency approval.

## 5.8 Receptionists and guards

Agencies that have regular public or client contact should have receptionists or guards to greet, assist and direct visitors.

Guards provide deterrence against loss of information and physical assets and can provide a rapid response to security incidents. Guards may either be directly employed by an agency, or be employed through a commercial guarding company. Agencies are to ensure that contracted guards are licenced in the jurisdictions they are employed. See Annex D: Summary of jurisdictional guard licencing legislation.

Agencies are to provide receptionists and guards with detailed visitor control instructions.

They should be able to easily lock all access to the reception area and/or non-public areas of the building in an emergency.

They may only perform other duties, such as CCTV and alarm monitoring, if it does not interfere with their primary task of controlling building access through the reception area. If performing other duties they are to be suitably trained and competent.

Receptionists and guards are to have a method of calling for immediate assistance if threatened—for instance, a duress alarm, radio—as they are most at risk from disgruntled members of the public.

Agencies are to identify any security concerns for receptionists and guards and people using agency reception areas in their security risk assessment and mitigate these concerns. For further information on safe reception area design see Comcare—Virtual Office—Reception.

### *5.8.1 Out-of-hours guarding*

Guards and patrols may be used separately or in conjunction with other security measures. The requirement for guards, their duties and the need for, and frequency of, patrols should be based on the level of threat and any other security systems or equipment that are already in place.

Agencies may use out-of-hours guarding or patrols instead of alarm systems in Zones Two to Three. These guards may be permanently on site or visit facilities as part of regular mobile patrolling arrangements.

Agencies are not to use guards instead of a SCEC-approved Type 1 SAS in Zones Four and Five. However, guard patrols may be used as an extra measure.

Guard patrols used instead of an alarm system are to check all security cabinets and access points as part of their patrols.

Guard patrols are to be performed at random intervals:

- for Zone Three—within every four hours, and
- for other areas based on an agency's risk assessment.

Guards should hold security clearances at the highest level of information to which they may reasonably be expected to have incidental contact. See the *Australian Government protective security governance guidelines—Security of outsourced functions* (to be released shortly) for details of security elements to be included in contracts.

**Out-of-hours guard response**

Agencies may use out-of-hours guard services in response to alarms in all Zones. The response time should be within the delay period given by the physical security controls. The highest level of assurance is given by 24/7 on-site guards who can respond immediately to any alarms.

## 5.9 Locks and door hardware

### *5.9.1 Locks*

Locks can deter or delay unauthorised access to information and physical assets.

Agencies are to:

- secure all access points to their premises including doors and operable windows, using commercial grade or SCEC-approved locks and hardware; these locks may be electronic, combination or keyed
- give combinations, keys and electronic tokens the same level of protection as the most valuable information or physical asset contained by the lock, and
- use SCEC-approved locks and hardware in Zones Four and Five, see the SCEC *Security Equipment Catalogue*.

Agencies may use suitable commercial locking systems in other areas.

Locks are only as strong as the fittings and hardware surrounding them. Agencies should also assess the level of protection needed from Doors and frames when selecting locks.

When using SCEC-approved locks agencies should use SCEC-endorsed locksmiths.

Related Australian Standards:

- AS 4145.2:2008 *Locksets and hardware for doors and windows—Mechanical locksets for doors and windows in buildings*.

### *5.9.2 Keying systems*

Keying systems are designed to provide a level of assurance to the administrator that:

- unauthorised duplicate keys have not been made, and
- provide mitigation to common keying system compromises.

They do this by using various controls such as:

- legal controls, for example registered designs, patents
- levels of difficulty in obtaining or manufacturing key blanks and the machinery used to cut duplicate keys, and
- levels of protection against compromise techniques, for example picking, impressioning, decoding.

When selecting a keying system agencies should evaluate:

- the level of protection provided against common forms of compromise
- the length of legal protection offered by the manufacturer
- supplier protection of agency keying data within supplier facility
- the transferability of the system and any associated costs, and
- commissioning and ongoing maintenance costs.

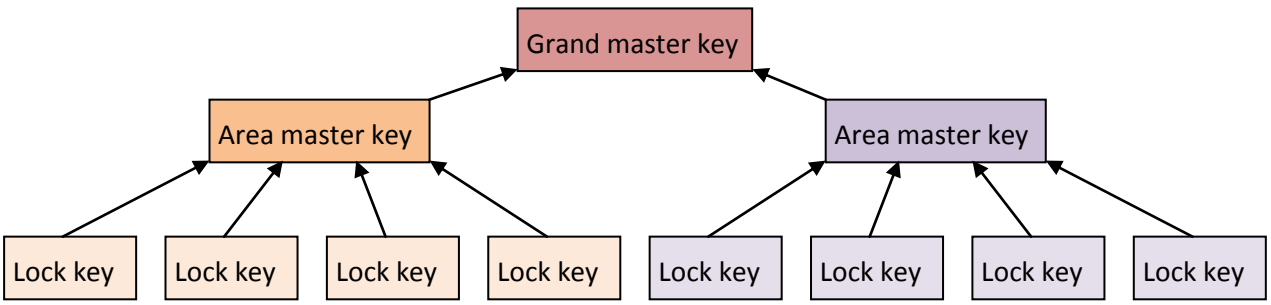
Agencies are to use SCEC-approved keying systems in Zones Three to Five. See the SCEC *Security Equipment Catalogue*. Agencies may use SCEC-approved keying systems in other areas based on their risk assessment. When using SCEC-approved keying systems agencies should use SCEC-endorsed locksmiths.

In Zone Two agencies are to use commercial restricted keying systems—that is, keys that are not able to be readily copied—or combination locks. Agencies should also use restricted keying systems in lower level applications where there is a risk of theft.

Agencies should use mastered key systems with sufficient levels so that separate area master keys control any locks within EACS and/or alarm system control points. Figure 3 outlines an indicative master keying tree.

Before selecting a qualified locksmith to provide a keying system, agencies should consider whether the keying system is proprietary to the installing locksmith, or will incur a cost if transferred to another locksmith.

**Figure 3: Indicative master keying tree**



### *5.9.3 Key control*

Agencies should maintain a register of all keys held and issued. Key registers should be appropriately secured and only available to authorised employees. Registers should include:

- key number
- name, position and location of person holding the key
- date and time issued, and
- date and time returned or reported lost.

Agencies are to limit the number of, and strictly control, all master keys as the loss of a master key may require the re-keying of all locks under that master. ASAs should control the issuing of all grand master keys as they may give access to all areas of a facility.

Agencies should audit key registers to confirm the location of all keys regularly in accordance with the agency's risk assessment.

Agencies' decisions to allow the removal of keys from their facilities are to be based on their risk assessment as this significantly increases the risk of loss. Where agencies allow keys to be taken out of their facilities:

- managers should approve the removal, and
- agencies should increase the frequency of key audits.

Agencies should provide all employees with training on their key management policy.

**Key cabinets**

Agencies should locate key cabinets within a facility's secure perimeter and where possible within the perimeter of the Zone where the locks are located. Key cabinets may be manual or electronic.

Commercial grade key cabinets provide very little protection from forced or covert access. SCEC-approved Class B key cabinets provide the same level of protection as other SCEC-approved Class B cabinets.

Electronic key cabinets may have automatic audit capacity and replace the need to maintain a key register. They may be able to be integrated into the EACS. However, there are currently no electronic key containers suitable for high security applications unless used in conjunction with other control measures such as locating the key container within a security room or area covered by a security alarm.

### *5.9.4 Combination settings*

Combination settings need to be memorised and agencies are to keep only one written record of each setting for use in an emergency. The record is to be held in an appropriately sealed envelope, classified with the highest security classification of the material held in the container, and stored appropriately. Copies of combinations would normally be kept by the ASA.

Agencies are to be change combination settings:

- when a container is first received by the agency
- after servicing the lock

- after a change of custodian or other person knowing the combination
- when there is reason to believe the setting has been, or may have been, compromised
- in any case, not less frequently than every six months, or
- when the container is disposed of by resetting the lock to the manufacturer's setting.

Employees are to immediately report the compromise or suspected compromise of a combination setting to the ASA.

Agencies should lock and service combination locks in accordance with the lock manufacturer's instructions.

### *5.9.5 Doors*

Agencies should select doors that provide a similar level of protection to the locks and hardware fitted.

There is significant variation in commercial office door types. These include, but are not limited to:

- solid core timber
- metal framed insert panel
- metal clad solid core or hollow core
- glass swing opening
- rotating glass, and
- glass sliding, single and double.

Solid core wooden or metal clad doors may also have glass or grill insert panels. The panels and fixings are to provide the same level of protection as the door.

Door types and thicknesses for Zones Three to Five are specified in the ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms.*

Automatic sliding glass doors normally operate through an electric motor and guide fitted to the top of the door. Some automatic sliding glass doors, particularly when unframed, may be levered open either at the centre joint for double sliding doors or sides for double and single sliding doors. This can make them difficult to secure without fitting drop bolts, lower guides, and/or door jambs.

Domestic hollow core doors—used for most internal domestic doors—and domestic sliding glass doors provide negligible delay as they are easily forced. However, if fitted with appropriate locks they will provide a degree of intruder evidence when broken.

When selecting security doors, agencies need to incorporate any requirements of the Building Code of Australia and any disability access requirements.

Related Standards:

BS EN1154:1997 *Building hardware. Controlled door closing devices. Requirements and test methods*

AS 4145.5 *Building hardware—Controlled door closing devices—Part 5: Requirements and test methods* (soon to be released).

## 5.10 CCTV coverage

Agencies can use closed circuit television (CCTV) as a visual deterrent to unauthorised access, theft or violence and as an auditable access record. Agencies should seek specialist advice in the design of CCTV management systems.

Agencies should consider the costs of CCTV systems as they can represent a significant capital cost. In addition, the ongoing monitoring, maintenance and support costs may be high.

Agencies can use CCTV to cover and give a visual record of:

- site access points, including internal access to higher security zones
- full site perimeter coverage, or
- access to specific physical assets or work areas.

Agencies are to comply with all relevant jurisdictional legislation as well as Commonwealth legislation governing CCTV usage. See Annex E: Legislation covering CCTV installation and usage.

CCTV monitoring may be event-activated and used in conjunction with a security alarm system to help those responsible for responding to the alarm. Or it may be used in conjunction with an access control system to aid personal identification for remote entry control. Motion detectors, left item (lack of motion detectors), etc. can also be incorporated into CCTV monitoring systems. Considerations on the use of CCTV include:

- how its use fits into the context of the overall security plan of the site
- the type of incident anticipated and in what way it will be expected to help the response to these incidents
- the need to advise staff and clients that it is in use on the premises, and
- the functional requirement.

Agencies should seek specialist advice before designing and installing a CCTV system to ensure the proposed system meets agency needs.

If it is expected that CCTV images may be used in court, the quality of images or data should be suitable for use as evidence in criminal proceedings.

The computers used to store images may require significant memory space to preserve images at the quality required by the agency. Excessive compression may lower the quality to the point where the images are no longer usable.

Agencies should also consider the period that images need to be retained when designing their system.

For further information see the Council of Australian Governments publication, *A national approach to closed circuit television—National code of practice for CCTV systems for the mass passenger transport sector for counter-terrorism*.

Related Australian Standards:

- AS 4806 Set:2008 CCTV Set:
  - AS 4806.1:2006 *Closed circuit television (CCTV)—Management*

— AS 4806.2:2006 *Closed circuit television (CCTV)—Application guidelines*

— AS 4806.3:2006 *Closed circuit television (CCTV)—PAL signal timings*

— AS 4806.4:2008 *Closed circuit television (CCTV)—Remote video*.

## 5.11 Security lighting

Agencies should consider, at the design stage, what the lighting is intended to achieve, for example deter unauthorised entry, assist guards conducting patrols, illuminate areas with CCTV coverage and provide employees with safety lighting in car parks.

Lighting, both internal and external, can make an important contribution to physical security. Security lighting can also provide deterrence and help guards to detect intruders.

Motion detection devices can also be set up so any detected movement will activate lighting and/or CCTV.

Agencies should ensure that lighting meets the illumination requirements of any CCTV systems installed.

The Illuminating Engineering Society publication *IES-G-1-03 Guidelines on Security Lighting for People, Property and Public Spaces* provides further advice on security lighting.

## 5.12 Perimeter access control

Agencies with significant threats or larger, multi-building, facilities may require perimeter access controls to restrict access to their facilities, for example Defence establishments. Types of perimeter control include but are not limited to:

- fences and walls
- pedestrian barriers, and
- vehicular barriers.

### *5.12.1 Fences and walls*

Fences and walls can be used to define and secure the perimeter of a facility. Agencies should determine the need for perimeter fencing during their initial security risk assessment, before finalising the selection of a site. Fences may be impractical for sites in the urban environment, particularly in central business districts.

The level of protection a fence will give depends on its height, construction, the material used, access control and any additional features used to increase its performance or effectiveness such as topping, lighting or connection to an External alarms or CCTV system.

Agencies that use fences and walls to prevent or deter unauthorised access are to develop supporting procedures to monitor and maintain the fences and monitor the grounds for unauthorised access.

Agencies should ensure that access points are at least as strong as any fence or wall used.

The SCEC *Security Equipment Catalogue* contains fences and PIDS suitable for high threat environments.

Related British and Australian Standards:

- BS1722—12:2006 *Fences - Specification for steel palisade fences*
- BS1722–14:2006 *Fences—Specification for open mesh steel panel fences*
- AS 1725:2003 *Chain-link fabric security fencing and gates* (Chain link fences provide minimal security unless used in conjunction with other security measures such as PIDS)
- AS/NZS 3016:2002 *Electrical installations—Electric security fences*.

### *5.12.2 Pedestrian barriers*

Agencies may need to restrict pedestrian access through fences or walls by installing controlled entry and exit points. This may include locked gates, gates connected to EACS or alarm systems, manned guard stations and turnstiles.

The SCEC *Security Equipment Catalogue* contains some pedestrian barriers suitable for high threat environments.

### *5.12.3 Vehicle barriers*

Agencies should assess whether vehicle barriers are warranted at their premises. British Standard PAS 69:2006 *Guidelines for the specification and installation of vehicle security barriers* provides some advice on selecting suitable fixed barriers.

The SCEC *Security Equipment Catalogue* contains some movable barriers suitable for high threat environments.

## 5.13 Security containers and cabinets

When selecting security containers and cabinets, agencies are to evaluate the insider threat—that is, the risk of theft, damage or other compromise of physical assets and information—by people with legitimate access to agency premises; as well as external threat sources.

Agencies should secure official information, portable valuable physical assets and money in suitably assessed containers appropriate to the business impact of the compromise, loss of integrity or unavailability of the information and assets, and the identified risks. Factors that will affect the class of security container or secure room required include:

- the level of classification
- the value and attractiveness of the information or physical assets to be stored
- the location of the information or physical assets within a facility
- the structure and location of the building
- access control systems, and
- other physical protection systems—for example, locks and alarms.

Agencies are to store security classified information separately from other physical assets. This will:

- lower the likelihood of compromise of information when physical assets are stolen, and
- help investigators determine the reason for any incidents involving unauthorised access.

Agencies should ensure valuable physical assets that contain official information, such as computers and other ICT equipment, are protected from:

- compromise of the aggregation of information on the physical asset, or
- loss of the physical asset

whichever has the higher business impact level.

### *5.13.1 SCEC-approved security containers*

SCEC-approved security containers are designed for storage of security classified information. They are not suitable for the storage of valuable physical assets. Due to their design these containers provide a high level of tamper evidence of covert attack and significant delay from surreptitious attack, but limited protection from forcible attack.

There are three levels of SCEC-approved containers:

- **Class A—**Designed to protect information that has a severe or catastrophic business impact level in high risk situations. These containers are extremely heavy and may not be suitable for use in some buildings with limited floor loadings.
- **Class B—**Designed to protect information that has a severe or catastrophic business impact level in low risk situations and information that has a high or very high business impact level in higher risk situations. These containers are robust filing cabinets or compactuses fitted with a combination lock. There are broadly two types:
  - — heavy types suitable for use where there are minimal other physical controls, and
  - — lighter models designed for use in conjunction with other physical security measures.

  Agencies should consider the siting of Class B containers as the weight may be an issue, particularly in older buildings.
- **Class C—**Designed to protect information that has up to an extreme business impact level in low risk situations, and information that has a medium business impact level in higher risk situations. These containers are fitted with a SCEC-approved restricted keyed lock and are of similar construction to the lighter Class B containers.

Agencies may, where their risk assessments indicate, use lockable commercial containers for:

- information with a low to medium business impact and a SCEC-approved container is not required, or
- higher level information within a SCEC-approved security room.

### *5.13.2 Commercial safes and vaults*

Agencies should store valuable physical assets in commercial safes and vaults designed to give a level of protection against forced entry commensurate with the business impact level of the assets.

As commercial grade security safes and vaults can provide varying degrees of protection, agencies should seek the advice of a qualified locksmith or manufacturer when determining the criteria they need to apply when selecting commercial safes and vaults.

Safes and vaults can be:

- fire resistant (either document or data)
- burglary resistant, or
- a combination of both.

See Annex F: Safe and vault types for more details on safe and vault types and functions.

The Australian Standard AS/NZS 3809:1998 *Safes and strongrooms* provides advice on design criteria for safes and strongrooms used to protect valuable physical assets. It categorises safes and vaults as:

- **Basic**: suitable for homes, small businesses, offices, etc.
- **Commercial:** suitable for medium retail, real estate agents, etc.
- **Medium security**: suitable for large retail, post offices, etc.
- **High security**: suitable for financial institutions, clubs, etc.
- **Extra high security** (vaults only): suitable for high volume financial institutions, etc.

Agencies may use safes and vaults from the following International Standards that meet similar design criteria as the Australian Standard:

- EN 14450—*Secure storage units. Requirements, classifications and methods of test for resistance to burglary. Secure safe cabinets*
- UL 687—*Burglary-resistant safes*.

The following International Standards provide advice on testing for fire resistance in safes:

- UL 72—*Tests for fire resistance of records protection equipment*
- JIS S 1037—*Standard fire test*
- KSG 4500—*Fire resistant*.

### *5.13.3 Vehicle safes*

Agencies should consider fitting vehicle safes to vehicles used by field staff when they are carrying valuable physical assets or official information. These safes are of similar construction to low grade commercial security containers or SCEC Class C containers and are bolted to the floor of vehicles. They give some protection against opportunist theft.

Vehicle safes are only of value when vehicles are fitted with other anti-theft controls such as alarms and immobilisers. They should be fitted out of sight in the boot of sedans or the luggage area of other vehicles.

## 5.14 Security rooms, strongrooms and vaults

Agencies with large quantities of official information or valuable physical assets, where their compromise, loss of integrity or unavailability would have a business impact, may use a security room, strongroom or vault, instead of containers to protect the information or physical assets. See Security containers and cabinets for guidance on determining the type of room required.

Security rooms are suitable for the storage of large quantities of official information. The ASIO Technical Notes *Technical Note – Physical Security of Intruder Resistant Areas/SR2 Rooms* and *Technical Note – Physical Security of Secure Areas/SR1 Rooms* provide advice on construction of security rooms. SCEC-approved demountable class A and B security rooms are listed in the SEC.

Agencies should seek advice from a reputable manufacturer before installing a commercial vault or strong room for the protection of valuable physical assets.

**Table 5: Selecting security containers or rooms to store official information**

Agencies are to use the following table when selecting the minimum level of security containers or security rooms for storing official information where the compromise, loss of integrity or unavailability of the information has a business impact level.

Agencies are to assess the business impact of the compromise, loss of integrity or unavailability the aggregation of information before determining the level of container required. A limited holding of information is an amount where compromise, loss of integrity or unavailability does not increase the business impact level.

| | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|---|---|---|---|---|---|
| Unclassified official information the compromise, loss of integrity or unavailability of which would have a low business impact | Determined by agency risk assessment, locked commercial container recommended | Determined by agency risk assessment | Determined by agency risk assessment | Determined by agency risk assessment | Determined by agency risk assessment |
| Aggregated information the compromise, loss of integrity or unavailability of which would have a medium business impact level. Or limited holdings of information with an FOUO or Sensitive[1] DLM | SCEC Class C | Determined by agency risk assessment, secured from unauthorised access | Determined by agency risk assessment | Determined by agency risk assessment | Determined by agency risk assessment |
| Aggregated information the compromise, loss of integrity or unavailability of which would have a high business impact level. Or limited holdings of PROTECTED information | Ongoing storage not recommended, if unavoidable SCEC Class C | SCEC Class C | Determined by agency risk assessment, SCEC Class C recommended | Determined by agency risk assessment | Determined by agency risk assessment |
| Aggregated information the compromise, loss of integrity or unavailability of which would have a very high business impact level. Or limited holdings of CONFIDENTIAL information | Not permitted | SCEC Class B | SCEC Class C | Determined by agency risk assessment SCEC Class C is recommended | Determined by agency risk assessment |

| | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|---|---|---|---|---|---|
| Aggregated information the compromise, loss of integrity or unavailability of which would have an extreme business impact level. Or limited holdings of SECRET information | Not permitted | SCEC Class A | SCEC Class B | SCEC Class C | SCEC Class C |
| TOP SECRET classified information information the compromise, loss of integrity or unavailability of which would have an catastrophic business impact level | Not permitted | Not permitted | Not normally permitted.[2] (In exceptional circumstances SCEC Class A) | Not normally permitted.[2] (In exceptional circumstances SCEC Class B) | SCEC Class B |

Notes:

1. Information with a Sensitive DLM will have specific handling requirements included as a footer or cover page to the document. Where these handling requirements exceed the requirements of this table the higher is required to be applied, See the *Information security management guidelines—Protectively marking and handling sensitive and security classified information*.

2. In exceptional circumstances to meet an operational requirement—for example, where TOP SECRET information cannot be returned to a Zone Five area—agencies may store TOP SECRET information for a period not to exceed five days in a Zone Three or Four area. ASAs should initially seek advice from ASIO-T4 before implementing arrangements for the temporary storage of TOP SECRET information outside a Zone Five area.

**Table 6: Selecting safes or vaults to protect valuable physical assets**

Agencies should use the following table as a guide to selecting commercial safes and vaults for storing valuable physical assets where their compromise, loss of integrity or unavailability has a business impact level on the agency. Agencies should use other controls that give the same level of intrusion resistance and delay for items that cannot be secured in safes or vaults, such as large items.

Agencies should consult with a suitably qualified locksmith or vault manufacturer to determine the appropriate safe or vault for their needs.

| | Zone One | Zone Two | Zone Three | Zone Four |
|---|---|---|---|---|
| Physical assets the loss of which would have a low business impact level | Determined by agency risk assessment, locked commercial container recommended | Determined by agency risk assessment, locked commercial container recommended | Determined by agency risk assessment | Determined by agency risk assessment |
| Physical assets the loss of which would have a medium business impact level | Determined by agency risk assessment, commercial safe or vault recommended | Determined by agency risk assessment | Determined by agency risk assessment | Determined by agency risk assessment |
| Physical assets the loss of which would have a high business impact level | Commercial safe or vault | Commercial safe or vault | Determined by agency risk assessment, commercial safe or vault recommended | Determined by agency risk assessment |
| Physical assets the loss of which would have a very high business impact level | AS 3809 commercial safe or vault | Commercial safe or vault | Commercial safe or vault | Determined by agency risk assessment, commercial safe or vault recommended |
| Physical assets the loss of which would have an extreme business impact level | AS 3809 high security safe or vault | AS 3809 medium security safe or vault | AS 3809 commercial safe or vault | Commercial safe or vault |
| Physical assets the loss of which would have a catastrophic business impact level | Should not be held unless unavoidable | Should not be held unless unavoidable | AS 3809 high or very high security safe or vault | AS 3809 medium or high security safe or vault |

## 5.15 Other controls

There are a number of other control measures that agencies can be use in specific situations. The following are some indicative examples and agencies should determine which controls best meets their requirements.

**Table 7: Additional controls to address specific risks**

The following list provides examples of additional measures that may be used to address specific threats. It is not exhaustive.

| Measure | Specific risks addressed |
|---|---|
| Individual duress alarm | Personal safety concerns for personnel in the field or unpatrolled public areas.<br>May be of value for tele-workers |
| Hidden/fixed duress alarm | Personnel safety concerns for reception areas and meeting rooms.<br>May be of value for home based workers |
| Vehicle alarm | Deter vehicle theft or theft of information and physical assets from vehicles |
| Vehicle immobilisation | Prevent vehicle theft |
| Vehicle safe | Deter theft of information and physical assets from vehicles |
| Individual item alarm/alarm circuit | Provide additional protection to valuable physical assets in premises.<br>Provide protection for physical assets on display |
| Two person access system | Protection of extremely sensitive information |
| Front counters and interview or meeting rooms | Restrict access by aggressive clients or members of the public.<br>Allow regular meetings with clients or the public without accessing security areas |
| Mailrooms and delivery areas | Provide a single point of entry for all deliveries.<br>Control mail-born threats from entering a facility without screening |
| Technical surveillance counter and audio security | Reduce vulnerability to, or detect, the unauthorised interception of sensitive or security classified information.<br>Reduce vulnerability to electronic eavesdropping on sensitive conversations |
| Conference security | Extra measures taken for a conference where security classified information is being discussed or handled. |

### *5.15.1 Vehicle immobilisation*

Agencies should consider vehicle immobilisation to reduce the loss of vehicles to theft. Vehicle immobilisation can be broadly divided into two types:

- automatic immobilisation of a vehicle when not in use and requires the key or electronic token to start the vehicle, or
- remote immobilisation, normally in conjunction with a remote tracking and alarm system that can disable a vehicle while in use.

### *5.15.2 Front counters and interview or meeting rooms*

Agencies that have interaction with the public or clients who may become agitated are to install measures that mitigate the risks to employee safety. This could include, but is not limited to, a specialised front counter that limits physical access to employees, and interview/meeting rooms that are monitored by guards or fitted with duress alarms.

Agencies with regular client or public interaction should consider establishing interview or meeting rooms accessible from their public areas.

For further advice see Comcare—Virtual office—Visitor aggression.

### *5.15.3 Mailrooms and delivery areas*

Mailrooms and parcel delivery areas are areas of significant risk to agencies from improvised explosive devices, chemical, radiological and biological attacks.

Agencies are to assess the likelihood of mail borne attack and, if warranted, apply suitable physical mitigations—for example, mail screening devices, a standalone delivery area, using a commercial mail receiving and sorting service.

Agencies are to have mail handling policies and procedures that are available to all staff. Agencies are to give mailroom staff detailed training in the use of any mail handling procedures and/or screening equipment used in their agency.

Agencies should select mail and parcel screening and handling equipment that meets its needs and complies with Australian Standard Handbook HB328–2009: *Mailroom security*.

### *5.15.4 Technical surveillance counter measures and audio security*

Technical surveillance counter measures (TSCM) services are used to provide a high level of assurance that sensitive agency information is free from unauthorised surveillance and access.

TSCM is mainly a detection function that seeks to locate and identify covert surveillance devices:

- before an event
- as part of a programmed technical security inspection or survey, or
- as a result of a concern following a security breach—for example, the unauthorised disclosure of a sensitive discussion.

A TSCM survey also seeks to identify technical security weaknesses and vulnerabilities including the evaluation of physical security controls such as locks, alarms and EACS.

Agencies are to have TSCM surveys carried out for:

- areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact, and
- before conferences and meetings where TOP SECRET discussions are to be held.

Agencies should initially seek advice from ASIO-T4 on the TSCM measures required.

Agencies that need to hold classified or sensitive telephone conversations are required to meet the logical controls in the ISM.

### *5.15.5 Conference security*

The aims of conference security are to:

- prevent unauthorised people gaining access to official information or physical assets
- protect the people attending the conference
- protect property from damage, and
- ensure the proceedings are conducted without disruption.

Agencies should undertake a security risk assessment before holding a conference to identify and mitigate any identified risks and, if warranted, develop a specific conference security plan.

Conference security will be included in the *Australian Government physical security management guidelines—Working away from the office*, due for release shortly. Until then additional information on conference security is available in the PSM *Part E: Annex A—Conference security guideline*.

# 6. Physical security elements in administrative security

Agencies use physical security equipment in administrative security procedures. These can include, but are not limited to:

- agency personnel transporting small physical assets and information out of agency premises, or transferring hard copy information to other agencies using:
  - security briefcases
  - single use pouches
  - reusable pouches and containers, and
  - seals
- destruction of classified information, using, for example, disintegrators and shredders.

Agencies should refer to the SCEC *Security Equipment Catalogue* when selecting this physical security equipment.

## 6.1 Transporting information and physical assets

### *6.1.1 Valuable physical assets*

Agencies should seek advice from their insurers when developing procedures to transport valuable physical assets.

While there is little risk from covert access most physical assets are more at risk from theft during transport than when housed in an agency facility. Some control measures may include escorts or guards, or use of secure transport specialists.

### *6.1.2 Classified information*

Physical security equipment used to transport security classified information provides some protection from opportunist access, but very limited protection from covert access.

Agencies should develop procedures that minimise the possibility of unauthorised access during transport. This could include ensuring that classified information is kept under the control of an employee or by using a SCEC-approved overnight or safehand courier.

For further details on carriage of information outside agency premises see *Australian Government information security management guidelines—Marking and handling sensitive and security classified information*.

**Security briefcase**

Agencies should use security briefcases when carrying small amounts of security classified information, or aggregations of information with a high business impact level or above. Employees using security briefcases should keep the briefcase in their possession at all times.

Security briefcases are designed to give limited protection against opportunist access and some evidence of tampering. They are not a replacement for security containers. They do not protect against forced

entry. A skilled person may also covertly open a security briefcase. See the SCEC *Security Equipment Catalogue*.

**Single use pouches**

Agencies may use SCEC-approved single use pouches in lieu of:

- paper envelopes and seals for inner envelopes, or
- outer envelopes in double enveloping.

**Wafer seals**

There are currently no SCEC-approved wafer seals for use in transporting classified information using double enveloping.

**Reusable pouches**

Agencies may use reusable pouches instead of outer envelopes when double enveloping.

## 6.2 Destruction equipment

Destruction equipment is used to destroy security classified information (paper-based and ICT media) so that the resultant waste particles cannot be re-constructed to enable the recovery of information. The main methods of destroying paper or ICT media are:

- shredding
- pulverising, and
- disintegrating.

Pulping may used for paper-based information.

Agencies are to destroy security classified information using SCEC-approved destruction equipment, unless using an ASIO approved destruction service.

To ensure all paper-based information is destroyed to the required particle size for the business impact of the compromise of the information, agencies should refer to the ASIO Protective Security Circulars (PSCs):

- PSC No. 53 *External Destruction of National Security Classified Matter*, and
- PSC No. 73 *Classified Waste Destruction*.

Both documents are available to ASAs from ASIO-T4.

Agencies should refer to the SCEC SEC for further details on destruction equipment.

The Defence Signals Directorate can advise on selection and use of destruction equipment for ICT media. See the ISM—Product security and media security.

### *6.2.1 Shredders*

Agencies may use shredders to destroy paper and ICT media—for example, CDs, single and dual layer DVDs.

### Paper shredders

Commercial strip shredders are not suitable for the destruction of classified or sensitive waste. Anybody wishing to access the information will have little difficulty reconstructing the pages from the resultant strips.

Cross cut shredders produce smaller pieces that are harder to reconstruct. The smaller the particle size the more secure the results.

Agencies are to use the following shredders to destroy paper-based security classified information:

- **Class A shredder**: maximum particle size 1 mm x 20 mm—suitable for all levels of business impact.
- **Class B shredder**: maximum particle size 2.3 mm x 25 mm—suitable for business impact levels up to and including high.

Where possible agencies should use a commercial crosscut shredder for paper waste for official information where the compromise has a business impact level up to and including medium.

Alternatively they may use an ASIO-approved destruction company for all levels of classified information up to SECRET, or TOP SECRET when directly supervised by an agency officer.

For further details on selecting shredders see the SCEC *Security Equipment Catalogue*.

### ICT media shredders

Agencies should refer to the SEC to select SCEC-approved media shredders to destroy ICT media.

Further details on procedures for the destruction of official information is in the *Australian Government information security management guidelines—Marking and handling sensitive and security classified information*.

# Annex A: Physical security measures checklist

The following self assessment tool has been developed to assist agencies in determining the Security Zone designation for their facilities or areas. From this agencies can decide the types of physical assets and classification of information that can be handled in the facility.

Agencies should modify this tool to meet their policies and agency construction guidelines.

## Facility/Area details

| | |
|---|---|
| Facility/area name | |
| Address | |
| Details of current/ proposed uses | |

## Additional risks

Agencies are to consider any risks to their people, information and physical assets within their work spaces.

Where possible agencies are to reduce any residual risks to an acceptable level. Where that is not possible agencies are to reduce the likelihood of any threats eventuating to an acceptable level, by applying additional controls. See **Error! Reference source not found.** and Table 7: Additional controls to address specific risks for some examples of threats and controls.

| No. | Specific risks | Additional controls required to meet the risks |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Zone ratings assessment tool

In addition to the controls required for agency specific threats, agencies are to apply some minimum controls to accredit their Zones.

The effectiveness of controls can be categorised as negligible to low, medium, high and very high.

The following self assessment tool will assist agencies in identifying existing controls and their level of effectiveness to determine a Zone rating.

Agencies should modify this tool to meet their policies and agency construction guidelines.

| No. | Control type | Minimum required for Zones | | | | | Effectiveness achieved | Zone achieved |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | | |
| | *Building construction elements*<br>• Normal construction to the Australian Building Code—**Low (L)**<br>• Normal construction to the Australian Building Code and:<br>– slab-to-slab construction at all egress points, or<br>– tamper evident ceiling, or<br>– Construction to ASIO *Technical Note – Physical Security of Intruder Resistant Areas/SR2 rooms*—**Medium (M)**<br>• Construction to ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms* or using elements tested to AS 3555.1–2003—**High (H)**<br>• Construction to ASIO *Technical Note – Physical Security of Secure Areas/SR1 Rooms* and Supplement to the Technical Note – *Physical Security of TOP SECRET areas*—**Very high (VH)** | Determined by agency risk assessment | L—business hours M—out-of-hours | H | H | VH | | |
| | *Out of hours alarm system*<br>• Part of access control system or AS 2201 class 1 or 2—**L**<br>• AS 2201 class 3–4—**M**<br>• AS 2201 class 5—**H**<br>• SCEC Type 1—**VH**<br>(On site guards may be used in lieu of an alarm system in Zones Two and Three) | Determined by agency risk assessment | Determined by agency risk assessment (M) | H | VH | VH | | |

| No. | Control type | Minimum required for Zones | | | | | Effectiveness achieved | Zone achieved |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | | |
| | *Out of hours alarm response*<br>• Out of hours response from offsite > 30 minutes—**M**<br>• Out of hours response from offsite < 30 minutes—**H**<br>• 24/7 onsite guards with immediate response—**VH**<br>(may be used in lieu of an alarm system in Zones Two and Three) | Determined by agency risk assessment | | | | | | |
| | *Access control system*<br>• Card only required for access—**L**<br>• Sectionalised access system—**M**<br>• Dual authentication—**H** | Determined by agency risk assessment | Determined by agency risk assessment (L) | M | H | H | | |
| | *Integration of alarm and access control systems*<br>• Fully integrated with building management systems—**L**<br>• Alarm system cannot be disabled by access control system—**M**<br>• Limited one way information exchange from access control system and disables access control system when activated—**H**<br>• Alarm system is a standalone system and disables the access control system when activated—**VH** | Determined by agency risk | If an alarm is used (M) | M | H | VH | | |
| | *Visitor control*<br>• Visitor register—**L**<br>• Visitor register and escorted visitors in sensitive part of facility—**M**<br>• Visitor register and escorted visitors in whole of zone—**H**<br>• Visitor register and visitors excluded unless there is an identified need—**VH** | Determined by agency risk assessment | M | H | VH | VH | | |

| No. | Control type | Minimum required for Zones | | | | | Effectiveness achieved | Zone achieved |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | | |
| | *Locks and hardware*<br>• Commercial grade locks fitted to doors—**Negligible (N)**<br>• Commercial grade locks and hardware fitted to all access points—**M**<br>• SCEC-approved locks and hardware fitted to all access points—**H** | Buildings locked out of hours | M | M | H | H | | |
| | *Keying systems*<br>• Commercial keying system—**L**<br>• Commercial restricted keying system—**M**<br>• SCEC approved keying system—**H** | Determined by agency risk assessment | M | H | H | H | | |
| | *Security containers and cabinets*<br>See Table 5: Selecting security containers or rooms to store official information | Determined by agency information holdings | | | | | | |
| | *Safes and vaults*<br>See Table 6: Selecting safes or vaults to protect valuable physical assets | Determined by agency physical asset holdings | | | | | | |
| | *CCTV coverage*<br>• Entry/exit coverage—**L**<br>• Full perimeter coverage—**M**<br>• Internal access point coverage—**M**<br>• CCTV integrated with electronic management system—**H** | Determined by agency risk assessment | | | | | | |
| | *Security lighting*<br>• Internal office lighting only—**N**<br>• Lighting of exterior egress points—**L**<br>• Full perimeter lighting—**H** | Determined by agency risk assessment | | | | | | |

| No. | Control type | Minimum required for Zones | | | | | Effectiveness achieved | Zone achieved |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | | |
| | *Perimeter access control*<br>• Vehicle control measures—**L**<br>• Pedestrian control measures—**L**<br>• Perimeter fences at least 2.4 m high—**N**<br>• Electronic monitoring incorporated into fences—**M to H** | Determined by agency risk assessment | | | | | | |
| | *Individual alarms*<br>• Duress alarms with 24/7 monitoring and immediate response—**M**<br>• Individual physical asset alarm circuit with response > 30 minutes—**L**<br>• Individual physical asset alarm circuit with response < 30 minutes—**M** | Determined by agency risk assessment | | | | | | |

| | | | | |
|---|---|---|---|---|
| | *Additional controls to address specific risks*<br>Insert details ( See Table 7: Additional controls to address specific risks for examples) | Determined by agency risk assessment | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Zone accreditation

**Lowest Zone achieved in any control type**
(This the maximum zone rating achievable for the facility/area) ----------

**Additional controls implemented to mitigate additional threats**

| No. | Control |
|---|---|
| 1. | |
| 2. | |
| 3. | |
| 4. | |

Zone rating depends on meeting all required certification. (See Table 4: Summary of certification requirements.)

Assessing officer's name and position: ----------

Assessing officer's signature: ----------

Date: ----------/----------/----------.

**Additional certifications required**

| No. | Certification requirement | Date certified | Certifying officer's name |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |

Accrediting officer's name and position: ----------

Accrediting officer's signature: ----------

Date: ----------/----------/----------.

# Annex B: Physical security terms for inclusion in the Australian Government lexicon of security terms

The following physical security-related terms are defined as they are used for the Protective Security Policy Framework (PSPF), including this protocol. Common security abbreviations and acronyms are also listed.

**Access control system**: A system designed to limit access to facilities to authorised personnel

**Accreditation**: A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system

**Aggregation**: A term used to describe compilations of classified or unclassified official information that may require a higher level of protection than their component parts. This is because the combination of the information generates a greater value, and the consequence of compromise, loss of integrity, or unavailability creates an increase in the business impact level

**ASA**: Agency security adviser

**Asset**: An item that has a financial value, or the loss or compromise has a business impact level, including personnel, information and physical assets

**ASIO**: Australian Security Intelligence Organisation

**BCP**: Business continuity plan

**Business impact level**: The level of impact on an agency's ability to operate or on the national interest resulting from the compromise, loss of integrity or loss of availability of an asset

**CCTV**: Closed circuit television

**Certification**: A procedure by which a formal assurance statement is given that a deliverable conforms to a specified standard

**CPNI**: Centre for the Protection of National Infrastructure (UK Government)

**CPTED**: Crime prevention through environmental design

**DIO**: Defence Intelligence Organisation

**DRP**: Disaster recovery plan

**DSD**: Defence Signals Directorate

**DSB**: Diplomatic Security Branch (part of DFAT)

**EACS:** Electronic access control system

**EIS**: External integrated system. Systems that may be integrated or interoperable with an SAS—for example, CCTV, building management systems, EACS

**Employee (or staff)**: See personnel

**EPL**: Evaluated product list

**Exceptional circumstances**: Where the exception is critical to the agency meeting its outcomes and the risks to the agency can be mitigated or managed in another way

**Facility**: A building, part of a building, or complex of buildings, in which an agency is located and which is designed to allow an agency to perform its functions

**ICT**: Information and communication technology

**ID card**: Identification card

**INFOSEC**: Information security

**ISM**: The Australian Government Information Security Manual (previously known as ASCI 33)

**ITSA**: Information technology security adviser

**NCTC**: National Counter Terrorism Committee

**Need to go**: access to an area should be limited to those who require access to do their work—for example, cleaners. They do not have a need to know but they do have a need to go to do their work

**Need to know**: Refers to a need to access information based on an operational requirement

**NTAC**: National Threat Assessment Centre

**Official information:** Any information generated by an agency that is not publicly available including sensitive information and security classified information

**PERSEC**: Personnel security

**Personnel**: Any member of an agency's staff and contracted service provider's staff used to service agency contracts, or other people who provide services to the agency or access agency assets

**PHYSEC**: Physical security

**Physical asset**: Any asset that is not personnel and does not contain information

**PIDS**: Perimeter intrusion detection system. A security alarm system, or part of an SAS that covers areas external to a building envelope

**PIN**: Personal identification number

**PIV**: Personal identity verification

**PSC**: Protective Security Circular – protective security advice circular only available to ASAs from ASIO-T4

**PSM**: Australian Government Protective Security Manual (precursor to the PSPF)

**PSPC**: Protective Security Policy Committee

**PSPF**: Protective Security Policy Framework (replaced the PSM)

**Qualified locksmith**: a practicing locksmith possessing a Certificate III Engineering (Locksmithing) or Certificate III (Locksmithing) or higher tertiary qualification

**Reasonable**: (in law) just, rational, appropriate, ordinary or usual in the circumstances. It may refer to care, cause, compensation, doubt (in a criminal trial), and a host of other actions or activities. Similarly a reasonable act is that which might fairly and properly be required of an individual

**Reasonably practicable**: (in OHS law) a judgment as to what is reasonably practicable is based on a consideration of the following general issues: severity of the hazard, probability of the risk, current knowledge regarding the hazard and the risk, availability of suitable hazard control/elimination methods, and cost of such control/elimination methods

**RFID**: Radio frequency identification

**SAS**: Security alarm system

**SCEC**: Security Construction Equipment Committee

**SCEC Endorsed Type 1 Alarm System**: Alarm system endorsed by SCEC to protect TOP SECRET information or aggregations of information where compromise would have a catastrophic impact on national security

**SEC**: Security Equipment Catalogue – the catalogue SCEC-approved security products (soon to be replaced by the Security equipment evaluated product list (SEEPL))

**Security classified information**: Official information that if compromised could have adverse consequences for the Australian Government. See the *Information security management guideline —Australian Government security classification system*.

**Security-in-depth**: A system of multiple layers, in which security counter-measures are combined to support and complement each other. This makes unauthorised access difficult—for example, physical barriers should complement and support procedural security measures and vice versa

**Security Zones**: Security areas for handling and storing information and physical assets based on security controls with Zones from One to Five

**Sensitive information**: Information that may be exempt from disclosure under the *Freedom of information Act 1982* Part IV

**Site**: The physical location of an agency's facilities

**T4 or ASIO-T4**: The area within ASIO responsible for providing protective security advice and services including testing of physical security equipment for SCEC

**Thin client technology**: Currently available technology which allows remote access to information without storing any information on the host computer

**TSCM**: Technical surveillance counter-measures

**Zone One**: Unsecured areas including out of the office working arrangements

**Zone Two**: Low security area with some controls and access control for visitors

**Zone Three**: Security area with high security controls, strict control of visitors on a needs basis and access to employees controlled

**Zone Four**: Security area with higher level of controls, and strict visitor and employee access controls on a needs basis

**Zone Five**: Security area with the highest level of controls, and strict visitor and employee access controls on a needs basis

# Annex C: Summary of equipment tested by the Security Construction and Equipment Committee and guidelines to assist agencies in selecting commercial equipment

The *Security Equipment Catalogue* (SEC) is being progressively replaced by the *Security equipment evaluated product list* (SEEPL). Some physical and administrative security equipment that was previously listed in the SEC will move to the SEEPL. Other equipment, where commercial equipment is suitable, will no longer be listed.

To assist agencies in selecting commercial equipment the Security Construction and Equipment Committee (SCEC) is developing the *Equipment selection guidelines*.

The following table is a summary of the equipment that will be tested by SCEC and appear in the SEEPL and guidelines.

This list will be periodically reviewed to meet the Australian Government's physical security needs.

| | SL1 | SL2 | SL3 | SL4 |
|---|---|---|---|---|
| **Information and asset security** | | | | |
| **Security detection systems** | | | | |
| Type 1 SAS | N/A | | | SCEC |
| Biometrics input devices and sub-systems | Guide to be developed | | SCEC | SCEC |
| Volumetric detection (internal) | Guide to be developed | | SCEC | SCEC |
| Volumetric detection (special purpose, e.g. Intrinsically safe devices) | SCEC | SCEC | SCEC | SCEC |
| Switches (balanced reed, etc.) | Guide to be developed | | SCEC | SCEC |
| Electronic access control systems sensor elements, input devices etc., excluding complete systems | Guide to be developed | | SCEC | SCEC |
| Electronic access control systems | Guide to be developed | | | |
| Key switches – electrical | Guide to be developed | | | |
| **Containers** | | | | |
| Container Locks | N/A | | SCEC | SCEC |
| Class A, B and C doors | SCEC | | | |
| Class A, B and C modular rooms | | | | |
| Class A, B and C containers | | | | |
| **Miscellaneous** | | | | |
| Key cabinets (base and intelligent cabinets) | Guide to be developed | | SCEC | SCEC |
| Safes – protection of assets | Guide to be developed | | | |
| **Doors** | | | | |
| Standalone access control devices | Guide to be developed | | SCEC | SCEC |

| | SL1 | SL2 | SL3 | SL4 |
|---|---|---|---|---|
| Mortice locks and strikes | Guide to be developed | | SCEC | SCEC |
| Magnetic locks | Guide to be developed | | SCEC | SCEC |
| Electric strikes | Guide to be developed | | SCEC | SCEC |
| Electric mortice locks | Guide to be developed | | SCEC | SCEC |
| **Peripheral locking hardware** | | | | |
| Keying systems | SCEC | SCEC | SCEC | SCEC |
| Padbolts | Guide to be developed | | SCEC | SCEC |
| Padlocks chains and harps | Commercial quality | | SCEC | SCEC |
| Hinge bolts | Commercial quality | | SCEC | SCEC |
| Strike shields and blocker plates | Commercial quality | | | |
| Cable transfer hinges | Commercial quality | | | |
| Door closers | Guide to be developed | | | |
| **Doors and access control portals** | | | | |
| Portals | Commercial quality | | SCEC | SCEC |
| Door operators | Commercial quality | | SCEC | SCEC |
| Doors | Not currently evaluated | | | |
| **Perimeter security (facility protection)** | | | | |
| **Barriers** | | | | |
| Cable pits and plinths | SCEC | SCEC | SCEC | SCEC |
| Active vehicle barriers | SCEC | SCEC | SCEC | SCEC |
| Fixed vehicle barriers | Guide to be developed | | | |
| Fences and gates | Guide to be developed | | | |
| **Windows** | | | | |
| Window grilles | Guide to be developed (ASIO Tech note No 2) | | | |
| Window locks | Guide to be developed | | | |
| Glazing anti-shatter film | Guide to be developed | | | |
| Window glazing and frames | Currently not evaluated | | | |
| **Perimeter intrusion devices detection (PIDS)** | | | | |
| Barrier mounted PIDS | SCEC | SCEC | SCEC | SCEC |
| Ground based PIDS | SCEC | SCEC | SCEC | SCEC |
| Volumetric PIDS | SCEC | SCEC | SCEC | SCEC |
| Video motion detection | Guide to be developed | | | |
| **Administrative** | | | | |
| Seals | SCEC | SCEC | SCEC | SCEC |
| Single use pouches | SCEC | SCEC | SCEC | SCEC |
| Shredders | Guide to be developed | | | |

| | SL1 | SL2 | SL3 | SL4 |
|---|---|---|---|---|
| Destructors | Guide to be developed | | | |
| Mail security | Guide to be developed | | | |
| Briefcases | Guide to be developed | | | |

# Annex D: Summary of jurisdictional guard licencing legislation

| Jurisdiction | Act | Regulation |
|---|---|---|
| Australian Capital Territory | Security Industry Act 2003 | Security Industry Regulation 2003 |
| Commonwealth | Aviation Transport Security Act 2004<br>Maritime Transport and Offshore Facilities Security Act 2003 | Maritime Transport and Offshore Facilities Security Regulations 2003<br>Aviation Transport Security Regulations 2005 |
| New South Wales | Security Industry Act 1997 | Security Industry Regulation 2007 |
| Northern Territory | Private Security Act 1995 | Private Security (Crowd Controllers) Regulations 2006<br>Private Security (Miscellaneous) Regulations 2006<br>Private Security (Security Firms) Regulations 2006<br>Private Security (Security Officers) Regulations 2006 |
| Queensland | Security Providers Act 1993 | Security Providers Regulation 1995 |
| South Australia | Security and Investigation Agents Act 1995 | Security and Investigation Agents Regulations 1996 |
| Tasmania | Security and Investigations Agents Act 2002 | Security and Investigations Agents Regulation 2005 |
| Victoria | Private Security Act 2004 | Private Security Regulations 2005 |
| Western Australia | Security and Related Activities (Control) Act 1996 | Security and Related Activities (Control) Regulations 1997 |

# Annex E: Legislation covering CCTV installation and usage

| Relevant Commonwealth, state and territory legislation and regulations | |
|---|---|
| Commonwealth and general | Privacy Act 1988 |
| | Privacy Amendment Act 2000 |
| | Privacy Amendment Act 2004 |
| | Privacy (Private Sector) Regulations 2001 |
| ACT | Listening Devices Act 1992 |
| | Security Industry Act 2003 (ACT) |
| | Security Industry Regulation 2003 (ACT) |
| | ACT OH&S legislation and regulations |
| NSW | Privacy and Personal Information Protection Act 1998 |
| | Privacy and Personal Information Protection Regulation 2005 |
| | Privacy Code of Practice (General) 2003 |
| | Security Industry Act 1997 (NSW) |
| | Security Industry Amendment Act 2005 |
| | Security Industry Amendment Act 2008 |
| | Security Industry Regulation 2007 (NSW) |
| | Workplace Surveillance Act 2005 |
| | Workplace Surveillance Regulation 2005 |
| | NSW OH&S legislation and regulations |
| NT | Surveillance Devices Act 2007 |
| | Surveillance Devices Regulations (NT) |
| | Private Security Act (NT) |
| | Private Security Regulations (NT) |
| | NT OH&S legislation and regulations |
| QLD | Invasion of Privacy Act 1971 |
| | Security Providers Act 1993 (QLD) |
| | Security Providers Regulation 2008 |
| | QLD OH&S legislation and regulations |
| SA | Listening and Surveillance Devices Act 1972 |
| | Listening and Surveillance Devices Regulations 2003 |
| | Security and Investigation Agents Act 1995 (SA) |
| | Security and Investigation Agents Regulations 1996 (SA) |
| | SA OH&S legislation and regulations |
| TAS | Listening Devices Act 1991 |
| | Listening Devices Regulations 2004 |
| | Security and Investigations Agents Act 2002 (Tas) |

| Relevant Commonwealth, state and territory legislation and regulations | |
|---|---|
| | Security and Investigations Agents Regulations 2005 (Tas) |
| | TAS OH&S legislation and regulations |
| VIC | Surveillance Devices Act 1999 |
| | Surveillance Devices Regulations 2006 |
| | Private Security Act 2004 (VIC) |
| | Private Security Regulations 2005 (VIC) |
| | VIC OH&S legislation and regulations |
| WA | Surveillance Devices Act 1998 |
| | Surveillance Devices Regulations 1999 |
| | Security and Related Activities (Control) Act 1996 (WA) |
| | Security and Related Activities (Control) Regulations 1997 (WA) |
| | WA OH&S legislation and regulations |
| Electrical safety Acts and Regulations applicable in the relevant state or territory also need to be considered | |

# Annex F: Safe and vault types

Safes and vaults are generally split up into three distinct categories. These are:

- Burglary resistant
- Fire resistant (documents)
- Media (data) safes

Hybrid safes that cross between fire resistant and burglary resistant provide a level of delay from fire and theft.

The majority of safes will fall into one of the above categories, with little cross over to other categories. A burglary resistant safe should not be used to protect documents or media from fire, just as fire safes should not be used to protect cash.

## Burglary resistant safes

Burglary resistant safes are primarily designed to protect valuables from physical attack. They are generally of solid construction, with thick walls designed to resist various physical attack methods. The materials used to manufacture them are usually good conductors of heat, so they generally offer minimal fire resistance.

## Fire resistant safes

Fire resistant safes are designed to protect paper documents (excluding photographs) from fire. They are usually constructed with thin metal walls sandwiched around a soft filling which offers insulation from heat, and emit moisture into the safe at high temperature, thus increasing the combustion temperature of paper (to about 170°C).

Fire resistant safes are usually tested against a standard, which specifies the external temperature, time the safe is subjected to the temperature, maximum internal temperature that can be reached, and percentage of documents inside the safe that are allowed to be destroyed. Some Standards conduct additional tests such as drop testing the safe midway through the fire test to simulate a floor collapsing.

The thin metal walls are used to reduce the heat retained by the safe after the heat source is removed; this will lower the level of physical protection offered. Thicker walls would generally increase the heat retained by the safe, and thus increase the time taken to cool down.

## Media safes

Media safes (or data safes) are designed to protect photographs, hard drives, optical media and other media types from fire. They are generally an extension of a fire safe, in that they offer the same amount of fire resistance with extra conditions. The maximum internal temperature that can be

reached is much lower (around 50°C) and the humidity must remain low. This is because moisture and heat corrupt or destroy data carriers.

The achievement of the low heat, low humidity safe is usually achieved by inserting a special box inside an existing fire safe, or by building it in. A water resistant seal ensures that water used to extinguish the fire does not affect the contents.

Fire resistant and or data safes that are measured against Standards generally offer little protection from physical attack.

## Hybrid safes (burglary and fire resistant)

Hybrid safes are generally manufacturer rated and will offer a level of delay from fire or theft.

These are usually achieved by fitting a burglary resistant safe with seals around all openings that expand with heat. As the safe is still primarily designed to resist burglary (with thicker walls) the fire resistance is lower than that of a rated fire or media safe.

## Vaults

Vaults or strongrooms are rooms that are designed to provide the same delay for the door and walls. These are used where a high storage capacity is required. Manufacturers offer either modular or base building construction depending on the requirements. They are normally designed and manufactured by safe manufacturers.

## Cash ratings

In Australia most manufacturers rely upon insurable ratings that are accepted by insurance companies if there is a loss. Insurable ratings are normally stated as supported or unsupported, suggesting whether or not an alarm system is providing adequate protection of the safe or vault. The supported insurable rating may increase the insurable rating each insurer provides for their minimum level before accepting a risk.

These insurable ratings are a good indication of the security offered by the safe; the higher the value the higher the security. The insurable rating of the safe should reflect the value of the contents being held.

Most Australian manufacturers will use insurable ratings in lieu of a recognised Standard.