



Australian Government

Physical security management guidelines

Event security

Approved
13 December 2011

Version 1.0

© Commonwealth of Australia 2011

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia (<http://creativecommons.org/licenses/by/3.0/au/deed.en>) licence.

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 3.0 AU licence (<http://creativecommons.org/licenses/by/3.0/legalcode>).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour (<http://www.itsanhonour.gov.au/coat-arms/index.cfm>) website.

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	Publically available
Date of security classification review	December 2013
Authority	Protective Security Policy Committee
Author	Protective Security Policy Section Attorney-General's Department
Document status	Approved 13 December 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	2
2. Background.....	4
2.1 Why the guidelines were developed.....	4
2.2 Relationship to other documents	4
2.3 How are these guidelines structured	4
3. Event security	5
3.1 Aims of event security.....	5
3.1.1 Overseas events.....	6
4. Before the event	7
4.1 Event security officer.....	7
4.2 Threats.....	7
4.3 High level and foreign guests	8
4.4 Risk management.....	9
4.5 Event security plan	9
4.5.1 Site selection.....	10
4.5.2 Site inspection.....	10
4.6 Other preparations before the event	11
5. During the event	13
5.1 Access passes and identity cards	13
5.2 Restricted areas.....	14
5.3 Information security.....	14
5.3.1 Classified waste.....	14
5.3.2 Security containers	14
5.4 Technical security.....	15
5.5 Guards and guard patrols.....	15
5.6 Security incidents	15
5.7 Security and emergency instructions.....	15
5.8 Receipt of mail.....	15

5.9	Demonstrations.....	16
5.10	Media.....	16
6.	After the event.....	17
	Annex A—Australian Government event levels	18
	Tier 1—Venue/Event Security.....	18
	Tier 2—State Police/Government Overlay	18
	Tier 3—National Overlay.....	18

Amendments

No.	Location	Amendment

1. Introduction

1.1 Purpose

The provision of a safe and secure environment is fundamentally important for the delivery of successful Australian Government events. The Australian Government expects that its agencies give due consideration to the security of all events they manage, plan or host, whether organised by the agency or outsourced.

The *Australian Government physical security management guidelines—Event security* provides guidance to Australian Government agencies to ensure a consistent approach to protective security measures applied to protect the people attending a planned event and the information and physical assets needed for the event.

Agencies should also use these guidelines to the extent possible for any unplanned events.

1.2 Audience

This document is intended for:

- Australian Government security management staff
- event managers, and
- any other body or person responsible for the security of people, information or physical assets at an Australian Government event.

1.3 Scope

These guidelines relate to the protective security measures Australian Government agencies employ to protect the people, information and assets at events they organise, including where the agency has contracted a service provider to facilitate the event.

These guidelines do not apply to major or special events that are the responsibility of:

- a jurisdictional (State or Territory) government—advice should be sought from the jurisdictional police or the jurisdictional agency that has the coordination role on behalf of their government, or
- the Australian Government—the whole of government approach is normally coordinated by Security Coordination Branch, Emergency Management Australia, Attorney-General's Department, contact EMASpecialEvents@ag.gov.au.

Agencies may find these guidelines useful when liaising with jurisdictional agencies or EMA on security requirements for special events.

See [Annex A—Australian Government event levels](#) for more details of the three tiers of event levels used by the Australian Government.

Where legislative requirements prescribe higher controls than identified in these guidelines then the controls required by legislation take precedence and need to be applied.

Agencies need to also consider their obligations under Australian legislation and conventions for the protection of foreign dignitaries attending their events.

1.3.1 Use of specific terms in these guidelines

In these guidelines the use of the terms:

- 'need to' refers to a legislative requirement that agencies must meet
- 'are required to' or 'is required to' refers 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 *PSPF - Australian Government Physical Security Management Protocol* (section 1.4).

The following terms are also used in these guidelines:

- **Australian Government involvement**—could include strategic planning advice, tactical support or the deployment of operational elements. All Australian Government involvement is provided in collaboration with the event organisers, the relevant jurisdictional police and other agencies.
- **Event**—includes both planned and unplanned events run by, or on behalf of, an Australian Government agency.
- **Event attendees**—all people attending the event including delegates, speakers, visitors and support staff.
- **Event manager**—the person in overall control of an event, this may be an agency employee or outsourced provider.
- **Event security officer (ESO)**—the agency officer, or contractor responsible for the security of people—attendees, staff and the public; information and assets at an event.
- **National interest**—the maintenance of Australia's good international reputation and bilateral relations, public confidence in the areas of tourism, trade, the economy and government, and the security and safety of all Australians.
- **Jurisdictional**—Australian states or territories.
- **Planned event**—an event that allows relevant agencies sufficient lead-time to consider, discuss and implement security arrangements.

- **Special event**—a planned event of such a nature that the national interest is served by the Australian Government’s involvement in whole-of-government coordination of security, normally through EMA.
- **Unplanned event**—an event that occurs on short notice, is routine or otherwise does not allow, or require, for detailed planning, including security planning.

2. Background

2.1 Why the guidelines were developed

The *Australian Government physical security management guidelines—Event security* have been developed to provide a safe and secure environment for the delivery of successful Australian Government events. These guidelines provide a consistent and structured approach to determining the security measures for events planned, organised and managed by Australian Government agencies.

These guidelines will:

- assist in establishing consistent terminology relating to event security across the Australian Government, and
- give agencies a framework for the assurance needed to ensure the safety of people, information and assets at an event.

2.2 Relationship to other documents

These guidelines support the implementation of the *Protective Security Policy Framework* (PSPF). In particular, it supports the *PSPF - Australian Government physical security management protocol*, the *Australian Government information security management protocol* and associated guidelines.

Agencies are to apply the controls identified in the protocols and guidelines to address identified security risks.

Agencies may also reference the National Counter-Terrorism Committee publication *National guidelines for the protection of places of mass gatherings from terrorism* for events involving the public and where there is a risk of terrorism.

These guidelines were developed to replace the *Australian Government Protective Security Manual, Part E—Physical Security—Annex A—Conference security*.

2.3 How are these guidelines structured

These guidelines are divided into:

- Event security overview
- Before event planning
- During the event, and
- After the event

3. Event security

Events that need security may include, but are not limited to:

- international and domestic conferences
- major meetings
- remembrance services/ parades
- sporting fixtures, or
- any other gathering where Australian Government people, information or physical assets are involved.

Events may be held at a single venue or multiple venues, these may be agency managed or commercial run venues.

3.1 Aims of event security

A secure environment is fundamentally important for a successful event. The aims of event security are to:

- base any controls on a risk assessment
- protect people from violence and intimidation
- protect official resources and information from unauthorised access, disclosure or compromise
- prevent unauthorised people gaining access to official resources that could cause embarrassment to the agency or government, including:
 - security classified and other official information, and
 - physical assets
- protect property from damage
- anticipate any changes in the National Threat Level, or event specific threats, and provide for rapid escalation of security measures, and
- ensure the proceedings are conducted without disruption, and minimising any disruptions to the public.

As events have specialised organisational requirements, an agency's normal protective security measures might not provide the full security measures required for the event or venue.

Agencies should as part of the event risk assessment determine whether a specific security plan to cover each event or venue is required. A security plan will help to identify which protective security measures are appropriate for each event or venue.

3.1.1 Overseas events

If the event is to be held overseas agencies should consult with the Department of Foreign Affairs and Trade (DFAT) in the early planning stages to determine the appropriateness of the proposed location and venue. This is particularly important if the event will involve accessing or using security classified information, or if the event is to be attended by Australian dignitaries.

4. Before the event

Event organisers have common law duties as well as statutory obligations under Australian and/or state or territory legislation to protect people attending events.

Protective security and safety should be considered in the earliest stages of event planning. Any protective security arrangements are to be identified as part of the event costing.

Agencies should also identify before the event any need to exercise event security arrangements, whether prior to, or during the event.

4.1 Event security officer

The person arranging the event is responsible for its security and should appoint an event security officer (ESO). The ESO may be the agency security adviser (ASA), but if not, he or she should be competent in security management. The ESO should seek advice from the ASA, especially during the site selection and preparation stages.

The ESO will have overall responsibility for security of the event and the event venue. He or she should be appointed as early as possible so he or she can be included in the planning processes. The ESO should:

- be sufficiently senior to exercise the necessary authority
- have direct access to the event manager, and
- have a sound knowledge of protective security.

Depending on the expected size and duration of the event, it might be necessary to allocate employees to assist the ESO.

The duties of the ESO may include, but are not limited to:

- seeking advice on the possible threats to the event
- completing a security risk assessment for the event or venue(s)
- preparing any security plans based on the risk assessment activity
- making necessary security preparations for the event
- coordinating security during the event, and
- liaising with appropriate agency and external authorities before, during and after the event.

4.2 Threats

Usually, the consideration of the possible threats to the event and the preliminary work on the plan will occur at the same time. The ESO should seek advice on possible threats from the part of the agency coordinating the event, other relevant areas in the agency and from external

agencies such as the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and State or Territory police.

The ESO should seek a threat assessment from the ASIO—National Threat Assessment Centre (NTAC) if:

- the event could be the subject of terrorism or violent protest
- previous similar events have been subject to terrorism or violent protest
- the information to be discussed is classified SECRET or above, and it is considered there may be a risk of compromise, or
- previous experience indicates this is appropriate.

Any request for a threat assessment is to include enough details on the event to enable a robust and thorough assessment of the terrorist or violent protest threats specific to the event.

If agencies become aware of any additional relevant information after the original threat assessment is issued agencies are to advise NTAC who will publish an updated threat assessment. NTAC may also issue updated threat assessments if they become aware of any relevant information

Agencies may also reference the National Counter-Terrorism Committee publication *National guidelines for the protection of places of mass gatherings from terrorism* for general advice on events involving large numbers of attendees, or the public, and where there is a risk of terrorism.

4.3 High level and foreign guests

Australia's obligations under the following conventions and legislation may impact on event security:

- *Convention on the prevention and punishment of crimes against internationally protected persons, including diplomatic agents 1973*
- *Vienna Conventions on Diplomatic and Consular Relations*
- *Crimes (Internationally Protected Persons) Act 1976*
- *Diplomatic Privileges and Immunities Act*
- *Consular Privileges and Immunities Act*, and
- *Foreign States Immunities Act 1985*.

Agencies responsible for planning, organising or managing an event should, based on their risk assessment, contact Emergency Management Australia, Security Coordination Branch, where the event is of a non-routine nature and is to be attended by high level officials such as:

- Australian holders of high office—for example federal ministers
- high level visiting foreign dignitaries—for example heads of state/heads of government/foreign ministers or other senior level ministers

- members of the diplomatic or consular corps—at ambassador level, or
- controversial visitors who could attract protest activity.

Event organisers should also seek advice from DFAT, Protocol Branch - protocol.branch@dfat.gov.au for any events that have high level foreign dignitary attendance.

4.4 Risk management

Agencies are to identify, assess and manage the risks to an event in accordance with the risk management methodology detailed in SAI Global - AS/NZS ISO 31000:2009 Risk management—Principles and guidelines and HB 167:2006 Security risk management.

4.5 Event security plan

The ESO should develop the security plan based on a risk assessment of the event. As details of the event become clearer, and preparations for the event develop, the plan will evolve and take into account matters including, but not limited to:

- the appropriate level of security for the event
- the duration, location and size of the event
- roles and responsibilities of event staff
- what needs to be protected—for example the proceedings themselves, documents (both those provided and notes taken during the event), people
- whether that need will stay constant throughout the event, or vary from session to session
- the nature of the threats
- the duration and location of the event
- who will be involved—for example host agency employees only, other agency employees, non-agency representatives, Australian office holders, office holders of other countries, other VIPs, media representatives, the public
- any security clearance or agency specific character check requirements for attendees
- whether close personal protection of VIPs may be required
- what special protective security measures could be necessary—for example audio counter-measures
- the need for contingency plans; including any communications, command and control arrangements; and alternate venues against particular incidents—for example bomb alerts and public demonstrations
- reception procedures and escort requirements for visitors
- event access and identity passes
- security containers and other security equipment that will be needed

- whether mail will be received or distributed at the event
- who is responsible for Australian Federal Police or local police liaison, and
- what event security and emergency instructions will be required.

The ESO should use the *PSPF - Australian Government Physical Security Management Guidelines—Security zones and risk mitigation control measures* to assess the venue(s) and determine any required security measures.

For events that will involve TOP SECRET, SECRET or certain Codeword security classified information the ESO should, based on the risk assessment, seek advice from ASIO-T4 - t4ps@t4.gov.au on protection of the information. In such cases the ESO should include in the event security plan what measures can be taken to:

- strictly limit the number of invitees to the overall event
- strictly limit the number of invitees to particular sessions
- limit the duration of the event to as short a period as practicable
- keep handouts to a minimum, and
- secure the meeting room from audio-visual recording devices—ASAs can seek advice from ASIO-T4 on Technical Surveillance Counter Measures.

4.5.1 Site selection

There may be a choice of sites, some within the agency's facilities and others at external venues. As far as possible, agencies should hold events involving TOP SECRET, SECRET or Codeword information on agency controlled or Australian Government controlled premises.

The less control the agency has over the proposed event venue, the more likely additional security measures will be needed.

Site selection should, based on the event risk assessment, also consider:

- the flow of the event—that is what happens and when and how it all fits together
- attendee safety, and
- transport.

4.5.2 Site inspection

The agency should carry out a preliminary security survey of possible venues at the earliest opportunity. Where possible the ESO should accompany the event organiser during the preliminary inspection. When preliminary security survey is undertaken by the event organiser the ESO or ASA should provide advice on security requirements.

If protest activity is a possibility the agency should involve the local police at an early stage of the event planning.

A more detailed inspection might be required later, once a particular venue is selected. At both stages, contact with local police and venue management can be useful to gain local knowledge.

In the site survey agencies should consider:

- what is adversely affecting physical security and how easy is it to remedy the problems, including door locks and window catches, curtain fittings, and exterior lights and light fittings
- the ability to maintain control of access to both the venue and to particular rooms, including any on-site parking
- the ability to provide for an area where suspicious articles can be examined (and where detonation of explosive devices would cause minimal damage to property and no injury to people), and
- the vulnerability of the venue to overhearing, overlooking and electronic eavesdropping.

Once the venue is selected, a more detailed survey might be needed.

4.6 Other preparations before the event

Based on the security plan and survey of the venue, agencies may need to address a number of matters before the event. These include:

- event set up schedules
- the preparation and issue of any event security instructions—for example:
 - entry control
 - storage and handling of official or security classified information
 - security classified waste disposal
 - key control procedures
 - emergency evacuation procedures
 - reporting of security incidents, and
 - communication plan
- arrangements for the supply and delivery of necessary security containers and other security equipment
- the preparation of event access and identity passes
- ensuring that all people present, including visitors and support staff, have the necessary security clearance
- the preparation of any visitor reception procedures and escort requirements for visitors
- the preparation of any key control measures
- the preparation and management of any event security exercises
- arrangements for:

- conducting technical surveillance counter measures
- employees or guards to control access, and
- any necessary searches to sanitise the premises.

5. During the event

As well as overseeing the overall security arrangements at the event, the ESO may have to conduct or oversee the following tasks:

- liaising with the event manager on communications, command and control issues
- ensuring security of, and issuing access and identity passes to accredited attendees, which should include identity verification if necessary
- advising attendees of the classification of the subject matter, the security arrangements and facilities available (the security classification of topics to be discussed should be displayed at the start of the event and again before each classified segment of the event)
- controlling entry to ensure that no unauthorised persons gain access to the building or event, or are able to observe or listen to proceedings
- supervising security aspects of visitor control
- providing security advice, including security and emergency procedures, to event attendees and venue employees
- arranging for receipt, recording, distribution, and return of security classified information used and produced at the event, and for its secure storage, including:
 - coordinating the use of security containers
 - arranging for the secure transmission of security classified information dispatched from the event, or for such information to be returned to the participants' agencies at the end of the event
 - coordinating security classified waste collection and disposal
- coordinating security procedures relating to cleaning and maintenance personnel
- coordinating the physical security and storage of equipment—for example: cameras, recording devices, audio recording devices, and mobile phones
- supervising people employed on security duties
- where competent conducting the initial investigation of security incidents, the ASA's assistance should be sought when this is beyond the expertise of the ESO, and
- supervising any necessary searches to sanitise the premises.

5.1 Access passes and identity cards

Access passes or identity cards provide speedy validation of a person's right to attend an event. For major events it is recommended that:

- photo identity cards be issued to all secretariat, administrative and support staff, accredited media representatives and where possible to delegates, and
- passes clearly indicate the dates of validity, are large enough to be easily checked visually by the guards or event staff, and designed so that they can be worn at all times.

5.2 Restricted areas

The ESO should decide which event areas are to have restricted access—that is, areas within the venue to which only certain attendees, authorised officials and security staff will have unescorted access. Restricted access areas should be clearly labelled, and access to them controlled.

5.3 Information security

Information used at an event could be in a variety of forms, including the proceedings themselves, documents brought to or produced at the event, or audio-visual presentations.

The ESO should consider, based on the risk assessment, the following measures to control security classified information:

- attendees do not bring any security classified information
- if security classified information is needed at the event, consider:
 - distributing the necessary number of copies at the beginning of the event, or if possible, the particular session
 - increasing accountability by numbering and recording the distribution of each copy, and
- arrange for attendees to leave all security classified documents, including any notes taken, at the end of the session or day, and send the documents by safe hand to each delegate after the event.

Whether these are practical will depend on the circumstances of the event. Whatever arrangements are decided upon the ESO should inform attendees of them as early as possible, and if necessary, remind attendees during the course of the event.

5.3.1 Classified waste

If it is necessary to generate classified waste at the venue, the ESO is responsible for ensuring that there are adequate facilities for its collection and disposal. It may be necessary to provide a SCEC-endorsed shredder at the venue.

5.3.2 Security containers

If it is necessary to store security classified information on-site, either during the proceedings or outside of the proceedings (if the event runs for more than one day). The ESO may need to ensure suitable security containers are provided, and will be responsible for controlling access to such containers. The ESO should use the *PSPF - Australian Government Physical Security Management Guidelines—Security zones and risk mitigation control measures* to determine the containers required.

5.4 Technical security

If the event involves TOP SECRET, SECRET or certain Codeword information, or the security plan or threat assessment otherwise indicates its need, technical surveillance counter-measures are to be taken before or during the event. The ESO is to contact ASIO-T4 for advice prior to any event involving TOP SECRET, SECRET or certain Codeword information.

The ESO should also seek advice from DSD if ICT equipment will be required for processing security classified information.

5.5 Guards and guard patrols

The use of guards and guard patrols during an event should be based on the event risk assessment.

If the event runs for longer than one day, the ESO should also consider regular guard patrols of the event venue to be conducted during hours the venue is not attended.

If technical surveillance counter measure sweeps or searches to sanitise the premises are required, guarding should be considered to minimise the risk of post sweep/search compromise.

5.6 Security incidents

Event attendees should be advised to report any security incident to the ESO, or security staff, as soon as possible to enable any necessary remedial measures to be implemented. Security staff should report any incidents to the ESO as soon as practical after becoming aware of the incident.

The ESO should report any incidents in accordance with the *PSPF - Protective Security Governance Guidelines—Reporting incidents and conducting security investigations*.

5.7 Security and emergency instructions

The ESO may consider it necessary to issue security and emergency instructions for attendees at the event. If needed the instructions should be provided to attendees before they arrive or on arrival (perhaps in the first session).

Separate instructions may be needed for staff and participants at the event.

5.8 Receipt of mail

The risk of a suspicious mail item should be considered and advice sought from the relevant jurisdictional police to manage the risk. The AFP - Australian Bomb Data Centre can provide general information kits on planning for and dealing with bomb threats and incidents.

5.9 Demonstrations

Control of demonstrations is the responsibility of the jurisdictional police. The ESO is responsible for ensuring that proper arrangements are agreed before the event begins. If the security risk assessment indicates that demonstrators may be a problem police advice should be sought.

5.10 Media

Media attention might be focused on the event. This could be because of the publicity given to the event beforehand, attendance by VIPs, or the subject matter. The ESO should be consulted by the event organisers when developing their media plan. The plan may include, based on the risk assessment:

- accreditation of, and passes for, media representatives
- a designated room at the venue to be made available for media representatives
- procedures for issue of any media releases and statements, and
- a requirement that, on arrival, media representatives report to the event security or reception area.

Agencies should:

- consider carefully whether any media representative is to be permitted into the venue or event rooms at any time while the event is in progress, and if so, under what conditions
- ensure that any release to the media is in accordance with the agency's media liaison procedures
- ensure that any access is under controlled conditions and with appropriate escort arrangements, and
- ensure that particular care is taken to prevent unescorted access to any room where security classified information could be left unattended, access to any room should be prevented until a check of the room for security classified information—for example: documents, projectors and electronic media; has been conducted.

6. After the event

Following the event the ESO should complete the following tasks:

- coordinate the retrieval of all event access and identity passes, if they give unescorted access to an agency venue. or if this is not possible the disabling of any access provided by the passes
- coordinate a thorough search of venues to ensure no official information or agency assets have been left behind—for example: documents, audio-visual recordings, whiteboards, projection equipment and electronic media equipment
- coordinate the return of security containers, including changing combination settings for container travel and storage
- submit a security report to the event organiser
- arrange secure transmission of security classified event papers and documentation to all attendees, and
- report any security incidents that occurred during the event that have not already been reported, in accordance with the *PSPF - Protective Security Governance Guidelines—Reporting incidents and conducting security investigations*.

Annex A—Australian Government event levels

The Australian Government uses three tiers of events to determine who has overall responsibility for an event.

Tier 1—Venue/Event Security

Security at the Tier 1 level is routinely provided within the venue by the event organiser or their subcontractor, with possible supplementation from local police. Many significant events will require only this level of security. However, larger events may require the overlay of Tier 2 or 3 security. Where Tier 2 or 3 security is required, the police may assume a greater role in Tier 1 security (on occasion on a user-pays basis). The provision of any Australian Government support or any support provided by other states/territories at Tier 1 level would be exceptional, and would be coordinated through the relevant jurisdictional police.

Examples of events requiring only Tier 1 security would include:

- the Security in Government Conference, and
- the Police Games.

Tier 2—State Police/Government Overlay

Tier 2 level security overlays Tier 1 and covers the immediate surrounds of the venues including the associated urban areas. Tier 2 security includes routes between venues and accommodation. It is usually the responsibility of the jurisdictional police and may be supplemented by other jurisdictional agencies, including emergency services. Support from external agencies (including other states/territories or the Australian Government) is coordinated by the relevant jurisdictional police.

The Australian Government may provide support to the State/Territory Government, on a case by case basis as required.

Examples of events requiring the Tier 2 overlay include:

- the World Trade Organisation Mini-Ministerial meeting in Sydney in 2002, and
- the Rugby World Cup in 2003.

Tier 3—National Overlay

Security at the Tier 3 level is provided by the Australian Government. The Australian Government has constitutional responsibility for a number of security functions relevant to special events. These include:

- preventing and responding to politically motivated violence
- the provision of intelligence derived from national and international sources
- protection of the national borders

- aviation and airport security
- the Government's support commitments to a response to terrorism under the National Counter Terrorism Plan
- coordination and delivery of dignitary protection services, and
- provision of support for emergency management and those aspects of law enforcement for which the Australian Government is responsible.

Examples of event requiring Tier 3 level security include:

- the Sydney 2000 Olympics, and
- APEC 2007.

Both of which were managed at the Australian Government level by special whole-of-Government task forces.