Protective security governance guidelines

Reporting incidents and conducting security investigations

Approved September 2011
Amended April 2015

Version 1.2
© 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

<table>
<thead>
<tr>
<th>Document details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security classification</td>
</tr>
<tr>
<td>Dissemination limiting marking</td>
</tr>
<tr>
<td>Date of next review</td>
</tr>
<tr>
<td>Authority</td>
</tr>
</tbody>
</table>
| Author | Protective Security Policy Section
Attorney-General’s Department |
| Document status | Approved by PSPC 13 September 2011
Amended April 2015 |
Contents

Amendments ................................................................................................................... iv

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 ............................................................................................................ 2
  2.1. Why the guidelines were developed ................................................................. 2
  2.2. Relationship to other documents ....................................................................... 2
  2.3. Structure of these guidelines ............................................................................. 2

3. Security incidents ................................................................................................... 3
  3.1. Examples of security incidents ........................................................................... 3
  3.2. Roles and responsibilities in security incident reporting ............................... 3
      3.2.1. Agency heads .......................................................................................... 4
      3.2.2. Program and senior executive managers .............................................. 4
      3.2.3. Managers ............................................................................................... 4
      3.2.4. Agency Security Adviser ....................................................................... 4
      3.2.5. IT Security Adviser .............................................................................. 4
      3.2.6. Agency employees ............................................................................... 4
  3.3. Procedures for ensuring staff report security incidents which are recorded ...... 5
      3.3.1. Agency security policy ........................................................................... 5
      3.3.2. Agency security awareness training to include reporting security incidents ........................................................................ 5
  3.4. Recording incidents ........................................................................................... 5
  3.5. Dealing with minor security incidents ............................................................... 6
      3.5.1. Notifying the Australian Government Security Vetting Agency (AGSVA) of security incidents involving holders of security clearances ........................................................................ 6
      3.5.2. Contact reporting scheme ...................................................................... 6
  3.6. Dealing with major security incidents ............................................................... 6
      3.6.1. Dealing with the compromise of Foreign Government information ...... 6
      3.6.2. Reporting major security incidents to ASIO ......................................... 7
      3.6.3. Reporting cyber security incidents to DSD ......................................... 7
      3.6.4. Reporting security incidents involving Cabinet material....................... 7
3.6.5. Reporting criminal incidents to law enforcement bodies ................. 8
3.6.6. Reporting critical incidents involving the safety of the public .......... 8
3.6.7. Occupational health and safety incidents ........................................ 8
3.6.8. Details to include when reporting major security incidents .......... 9

4. Investigations ........................................................................................................ 10

4.1. Principles of procedural fairness ..................................................................... 10
4.2. Types of investigations ...................................................................................... 10
  4.2.1. Security investigations .............................................................................. 10
  4.2.2. Criminal investigations ............................................................................. 11
4.3. Agency procedures for investigating security incidents ............................ 11
4.4. Appointing investigators .................................................................................. 12
4.5. Understand the role of an investigator ............................................................ 12
4.6. Determine the nature of an investigation ....................................................... 13
4.7. Terms of Reference for investigations ............................................................. 13
4.8. Conducting investigations ............................................................................... 13
  4.8.1. Assess the incident and develop an investigation plan ......................... 14
  4.8.2. Gather evidence ....................................................................................... 15
  4.8.3. Record and store evidence appropriately .............................................. 15
  4.8.4. Prepare the investigation report .............................................................. 15
  4.8.5. Close the investigation ............................................................................ 15
  4.8.6. Standard of proof .................................................................................... 15

Annex A—Categories of security incidents .............................................................. 17

Annex B—Other relevant Australian Government material and services .......... 19
## Amendments

| No. | Date    | Location   | Amendment                                                      |
|-----|---------|------------|                                                               |
| 1   | Oct 2011| Section 3.6| Additional detail for the compromise of foreign government information |
| 2   | April 2015| Throughout | Update links                                                  |
1. Introduction

1.1. Purpose
These guidelines aim to help agencies identify and address security incidents as part of the Australian Government’s protective security measures. They also detail a set of best practice standards in investigation methodology for security incidents.

The effective administration of security incidents and investigations is a basic part of good security management. Information gathered on security incidents and during investigations may highlight the need for agencies to re-assess the adequacy of current practices or arrangements, and is also a key input into continuous improvement activities. In turn, good security management helps to contain the effects of a security incident and enables agencies to manage the consequences of a security incident and to recover as quickly as possible.

1.2. Audience
These guidelines apply to anyone who has protective security responsibilities under the Protective Security Policy Framework (PSPF).

1.3. Scope
These guidelines amplify the PSPF governance requirements relating to incident reporting and investigative procedures and better practice that agencies should apply to meet the requirements of GOV 8.

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 Australian Government Physical Security Management Protocol (section 1.4)
2. **Background**

2.1. **Why the guidelines were developed**

These guidelines provide a flexible structure that enables agencies to manage the risk posed by a security incident. Not all security incidents are significant or warrant investigation and agencies are encouraged to seek guidance from the appropriate agencies identified as having key responsibilities within these guidelines.

The conduct of investigations is part of an agency’s security management process. A security investigation will establish the cause and extent of an incident that has, or could have, compromised the Australian Government. A security investigation should protect both the interests of the Australian Government and the rights of affected/implicated individuals.

The agency security policy should describe how the agency will conduct a security investigation. Agencies should maintain details of all security incidents and investigations. This detail will assist agencies to determine:

- the areas within their agencies requiring additional protection, and
- the type of security measures and procedures required.

2.2. **Relationship to other documents**

These guidelines explain mandatory requirement **GOV 8** which requires the appropriate training of investigators, and implementing procedures for reporting and investigating security incidents, and taking corrective action.

In addition to GOV 8, these guidelines complement other Governance mandatory requirements. Implementing these guidelines will assist agencies to meet their obligations under **GOV 5**, **GOV 7** and **GOV 12**.

**AS/NZS ISO/IEC 27002:2006 Information technology—Security techniques—Code of practice for information security management**, Section 13 details standards for information security incident management, including reporting security events and weaknesses, and management of information security incidents and improvements. In developing policies and procedures for managing and reporting information security incidents, agencies should be guided by the implementation guidance in this Standard.

2.3. **Structure of these guidelines**

These guidelines are broadly divided into two parts. The first part covers security incidents, their definition, as well as reporting and recording requirements. The second part details the conduct of investigations, in particular security investigations.
3. Security incidents

A security incident is:

- a Security violation, Security breach or Security infringement of protective security policy or procedure as defined in Annex A—Categories of security incidents.
- an approach from anybody seeking unauthorised access to official resources, or
- any other occurrence that results, or may result, in negative consequences for the security of the Australian Government, its institutions or programs.

The Australian Government personnel security guidelines—Agency personnel security responsibilities Section 14.3 – Contact reporting provides separate advice on recognising and reporting approaches by foreign officials seeking unauthorised access to official resources.

Agencies should assess the harm from any security incident to determine the impact on the Australian Government of the actual or suspected loss, compromise or disclosure. This will assist the agency to identify whether the incident is a Minor security incident (an infringement or breach) or a Major security incident (a violation, which the agency is to report to the Australian Security Intelligence Organisation (ASIO), and other relevant agencies, depending on the nature of the incident).

Agencies report and record security incidents in order to monitor security performance, and to help agencies identify security risks so they can implement appropriate treatments.

3.1. Examples of security incidents

Examples of incidents that agency employees and contractors should report to agency security staff are:

- criminal actions such as actual or attempted theft, break and enter, vandalism, fraud or assault
- natural occurrences such as fire or storm damage, which may compromise agency security
- incorrect handling of protectively marked information, such as failure to:
  - provide the required protection during transfer or transmission resulting in a data spill on an electronic information network or system
  - store security classified information in an appropriate security container, or
  - correctly secure security containers
- accessing official information without authorisation
- sharing official information with a person who is not authorised to access it
- sharing computer passwords or other access control mechanisms, and
- any unauthorised use of official resources.

3.2. Roles and responsibilities in security incident reporting

Agency security policies relating to the administration of security incidents and the conduct of security investigations should specify the roles and responsibilities of staff involved in the administration of security incidents and the conduct of security investigations.
3.2.1. Agency heads

An agency head answers to his or her Minister on all issues of protective security for that agency. The agency head is responsible for ensuring procedures are implemented to facilitate reporting of security incidents by agency employees, contractors and contractor employees. He or she should also ensure that adequate records are kept to report on the agency’s security performance and continuing security requirements.

3.2.2. Program and senior executive managers

Program and senior executive managers are responsible for, and should actively support, the implementation and maintenance of procedures for security incident reporting and recording within the areas under their control and within the agency in general. They should seek advice from the agency security adviser (ASA) to assist them to carry out these responsibilities.

The SES officer appointed as the Security Executive (GOV 2), or an SES officer independent of the incident, should be responsible for approving Terms of Reference and objectives for any security investigation, and should ensure that he or she receives regular reports on investigation progress.

3.2.3. Managers

Managers have an important role to play in security incident reporting. Their supervisory role makes it probable that they could be the first to detect a security incident. Also their detailed knowledge of their staff makes it likely they will become aware of any behaviour that may be of security concern. Managers should ensure that security incidents are reported to the ASA, and should liaise closely with the ASA on any security concerns. Managers should consult with the information technology security adviser (ITSA) regarding a security incident involving the agency’s ICT systems.

3.2.4. Agency Security Adviser

The ASA is responsible for receiving and actioning information regarding security incidents. The ASA is to record security incidents and investigation outcomes to enable regular reporting to senior management on agency security performance. Staff should inform the ASA of all security incidents, including those being dealt with by the ITSA.

3.2.5. IT Security Adviser

The ITSA is responsible for receiving and actioning incidents relating to ICT system or content security incidents. These include denial of service attacks, targeted malicious email attacks and loss of ICT assets or information. The ITSA is to report all major ICT security incidents to the Australian Signals Directorate.

The ITSA should inform the ASA of any ICT security incidents and the likely impacts to the agency. The ITSA may have a role in the investigation of any ICT security incident.

3.2.6. Agency employees

Agencies should advise all agency employees, including contractors and contractor employees, that they have a responsibility to comply with agency procedures for reporting security incidents. Agencies
are required to provide these same employees, contractors and contractor employees with security awareness training (see [GOV](#)).

Agencies and Security Construction and Equipment Committee (SCEC) endorsed service providers should report security incidents relating to SCEC services to ASIO T4. SCEC service providers include SCEC endorsed consultants, couriers and locksmiths. Agencies and destruction service contractors should advise ASIO of security incidents involving ASIO approved destruction services.

### 3.3. Procedures for ensuring staff report security incidents which are recorded

#### 3.3.1. Agency security policy
The agency security policy and procedures should make provisions for reporting and recording security incidents by:

- requiring agency staff and contractors to report security incidents
- including formal procedures and mechanisms to make it easy to report security incidents, and
- requiring the ASA to maintain records of any reported incidents and any other security incidents.

#### 3.3.2. Agency security awareness training to include reporting security incidents
An agency’s security awareness training should include details about the:

- agency’s procedures for reporting security incidents, and
- responsibility of staff to report security incidents.

### 3.4. Recording incidents

Agencies should develop a mechanism for recording incidents that best suit their security environment and operational requirements. Records of security incidents should include:

- time, date and location of security incident
- type of official resources involved
- description of the circumstances of the incident
- nature of the incident - deliberate or accidental
- assessment of the degree of compromise or harm, and
- summary of immediate and/or long term action taken.

Recording security incidents provides valuable insight into an agency’s security environment and performance. For instance, multiple minor security incidents could indicate poor security awareness and could alert the agency to the need for increased security training and education.

ASAs should regularly report details of security incidents and any trends to the agency Security Executive. The statistical information gathered by agencies through security investigations and contact reporting will assist an agency to determine if it requires additional protection and security measures.
3.5. **Dealing with minor security incidents**

Agencies should develop their own procedures and practices to investigate minor security incidents, which should take into account agency-specific issues.

3.5.1. **Notifying the Australian Government Security Vetting Agency (AGSVA) of security incidents involving holders of security clearances**

Agencies that use the services of AGSVA should advise AGSVA about repeated minor security incidents and any major security incidents that relate to a person’s suitability to hold a security clearance. Also, the agency is required to notify AGSVA, at the appropriate time, of the outcome of any investigation into a security incident that relates to a person’s suitability to hold a security clearance.

Where warranted AGSVA will record the details on the Personal Security File of the relevant individual. In some instances AGSVA may initiate a review for cause, see the Australian Government personnel security protocol.

3.5.2. **Contact reporting scheme**

All clearance holders are required to report defined contacts with foreign officials, or any requests from foreign officials to access agency assets or security classified information or resources. See the Australian Government personnel security guidelines—Agency personnel security responsibilities Section 14.3 – Contact reporting.

3.6. **Dealing with major security incidents**

Agency policies and procedures for dealing with a major security incident should be more formal to reflect the deliberate, reckless or negligent nature of actions that may compromise security.

Where a suspected major security incident involves the compromise of official information or other resources that originate from, or are the responsibility of another agency, agencies should seek advice from the originating agency prior to instigating any investigation. The originating agency may have operational security requirements that need to be applied to the investigation. In some cases it may be more appropriate that the originating or responsible agency carries out the investigation. The need-to-know principle will apply.

3.6.1. **Dealing with the compromise of Foreign Government information**

Where a suspected major security incident involves the compromise of information or other resources that originate from a foreign government or governments, agencies are required to comply with the arrangements as outlined in the articles of any bilateral or multilateral agreement. Where no agreement exists, agencies should inform the relevant foreign government or governments in writing.

Where the foreign government information has been provided by another agency, the providing agency should be informed of the major security incident. The providing agency may have obligations it needs to apply under a bilateral or multilateral arrangement.
3.6.2. **Reporting major security incidents to ASIO**

Agencies are required to report to ASIO any security incidents that involve suspected:

- espionage
- sabotage
- acts of foreign interference
- attacks on Australia’s defence system
- politically motivated violence
- promotion of communal violence, or
- serious threats to Australia’s territorial and border integrity.

See the Definition section of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

For security incidents that are reportable to ASIO (see GOV 7), ASIO and the agency will conduct an initial assessment of the potential compromise. Dependent upon the assessment, ASIO will either:

- recommend the agency continue with its own investigation and advise ASIO of the outcome, or
- conduct the investigation, in close consultation with the agency, and possibly in conjunction with the Australian Federal Police (AFP).

The agency should strictly observe the need-to-know principle in relation to the details of a major security incident and the fact that it has occurred in the agency until ASIO advises otherwise.

3.6.3. **Reporting cyber security incidents to DSD**

Agencies are required to report suspected cyber security incidents to ASD including:

- suspicious or seemingly targeted emails with attachments or links
- any compromise or corruption of information
- unauthorised hacking
- any viruses
- any disruption or damage to services or equipment, and
- data spills.

Agency ICT security policies and plans should require early contact with DSD to avoid inadvertently compromising any investigation into a cybersecurity incident.

3.6.4. **Reporting security incidents involving Cabinet material**

Agencies are required to report suspected security incidents involving Cabinet material to the Cabinet Secretariat in the Department of the Prime Minister and Cabinet. The *Cabinet Handbook* provides information about the security and handling of Cabinet documents.
3.6.5. **Reporting criminal incidents to law enforcement bodies**

Where the incident may constitute a criminal offence, the agency may need to report to the appropriate law enforcement body. Agencies should seek advice from the Australian Federal Police or State or Territory police in such matters. The [AFP website](https://www.afp.gov.au) has useful advice on the type of criminal incidents that are reported to the AFP or the State/Territory police, or if an incident is best handled within an agency.

3.6.6. **Reporting critical incidents involving the safety of the public**

Any critical incidents requiring immediate response, in particular where lives are at risk, should be reported to the appropriate emergency services on '000'. Agency security plans should provide for reporting critical incidents when they occur to the [Australian Government Crisis Coordination Centre](https://www.ag.gov.au) (CCC). These critical incidents, which may affect public safety and require a coordinated response in support of the Australian Government and/or state and territory governments, include:

- assault, including armed or military-style assault
- arson, including suspected arson
- assassination, including suspected assassination
- bombing, including suspected use of explosive ordnance or improvised explosive devices
- chemical, biological or radiological (CBR) attack, including suspected CBR attack
- attack on the National Information Infrastructure (NII), or critical infrastructure using the NII
- violent demonstration involving serious disruption of public order
- hijacking, including suspected hijacking
- hostage situation, including suspected hostage situation
- kidnapping, including suspected kidnapping
- mail bomb, including suspected mail bomb, or
- white powder incident, including real or significant hoax incidents.

Reports to the CCC should be made on telephone number 1300 243 222 or via e-mail at ccc@ag.gov.au. The CCC will advise the AFP, ASIO, local police and/or other agencies as appropriate of the incident.

3.6.7. **Occupational health and safety incidents**

Agencies need to report major occupational health and safety incidents (which involve serious injury or death) to Comcare. Occupational health and safety incidents are the responsibility of Comcare, or the relevant jurisdictional equivalent. For further advice see the [Work Health and Safety Act 2011, WHS Regulations and WHS Codes of practice](https://www.worksafe.gov.au).
3.6.8. Details to include when reporting major security incidents

When reporting suspected major security incidents the agency should provide the following details:

- date/time of the incident or when it was reported or discovered
- brief details of the incident
- what may have been compromised (type and level of classification)
- names of those involved in the incident (if known)
- name and contact details of the agency for follow up
- an initial assessment of the harm or damage, and
- what action has already been taken or measures implemented.

Agencies should also notify any changes or updates to incidents to the same agency to which they reported the incident unless otherwise advised by that agency.

Agencies are responsible for distributing information about incidents within their agencies.

Further details of contacts for advice and assistance about security incident recording and reporting are listed at Annex B—Other relevant Australian Government material and services.
4. Investigations

4.1. Principles of procedural fairness

The principles of procedural fairness apply to all investigations. These principles require that individuals whose rights, interests or expectations are adversely affected should be informed of the case against them and be given an opportunity to be heard by an unbiased decision maker. Procedural fairness also applies to actions taken as the result of an investigation. (See the Australian Government personnel security guidelines—Vetting Practices Section 6.2 – Procedural fairness guidelines)

4.2. Types of investigations

Broadly, there are two types of investigation: administrative and criminal. These guidelines mainly focus on Security investigations, which are a specific type of administrative investigation.

Agencies may also need to conduct other administrative investigations such as those that relate to:

- disciplinary matters, where there are possible breaches of the APS code of conduct, or equivalent in non-APS agencies, or
- incidents that affect the health and safety of people within agency premises or who are carrying out duties in the field.

If the incident requires more than one type of investigation, the agency is to assess which type of investigation takes precedence. Usually a criminal investigation takes precedence; however, in some security incidents it may be more urgent to discover the damage and method of compromise, and a security investigation will take precedence. See 4.2.1.

4.2.1. Security investigations

It is not necessarily the purpose of a security investigation to establish whether a criminal offence has been committed, or to aid in the prosecution of a suspect. Rules of evidence may not apply, where gathering information, not necessarily admissible evidence, is the primary focus of a security investigation. The outcomes of a security investigation focus on risk and damage assessment to establish:

- the nature of the incident
- how the incident occurred
- what the circumstances were that led to the incident occurring
- person/s involved
- the degree of damage to national security interests, and
- procedures needed to remove or reduce the likelihood of a future similar event.

However, if a security investigation gives way to a criminal investigation and a subsequent prosecution, then at that point agencies are to apply the procedures for conducting criminal investigations and gathering evidence. Agencies may need to seek advice from ASIO and/or AFP to establish whether a violation involves national security, and whether there is a possible offence against Commonwealth law. Where other agencies have investigative powers based on legislation, e.g. Comcare and ASIO,
these agencies may have primacy in the decision over which investigation takes precedence. ASIO or other agencies may have a major role in such an investigation.

4.2.2. Criminal investigations

A criminal offence refers to an act that will generally be an offence under the *Crimes Act 1914* (Cth) or the *Criminal Code Act 1995* (Cth), or other specific legislation including relevant State or Territory criminal offences. Agencies may need to conduct criminal investigations, such as in cases of fraud, theft and unauthorised disclosure of official information.

The purpose of a criminal investigation is gathering admissible evidence which may lead to placing the offender/s before the court. The AFP can provide guidance and may have significant involvement in such investigations. The [AFP website](#) provides advice on:

- crimes that fall under the AFP’s jurisdiction
- crimes that fall under the jurisdiction of a State or Territory government, and
- some types of Commonwealth crimes that may, at least initially, be the responsibility of another government agency, such as:
  - crimes against an Australian Government agency, for instance fraud against a specific Government program administered by the agency, and
  - cases where another agency has the expertise to prosecute the crime.

The [AFP website](#) also provides advice on referring matters to the AFP. The AFP has negotiated special arrangements with some agencies for referring matters.

4.3. Agency procedures for investigating security incidents

Agencies should establish policy and procedures for investigating security incidents that detail the:

- responsibilities of the agency investigator
- responsibilities of senior management
- actions on receiving a complaint or allegation, including anonymous allegations or reports from whistleblowers
- Terms of Reference for the investigation
- points at which security investigations are to be referred to ASIO, the relevant police service and/or DSD
- requirement to maintain detailed file notes
- standards of ethical behaviour by agency investigators, activity recording, and the preferred investigation case management system
- requirement to keep senior management informed of the progress of security investigations and future options
- requirement for a final report from the agency investigator incorporating background information
- involvement of other agencies (especially ASIO, AFP and DSD)
• summary of major findings and recommendations, and
• procedures for operational practices such as interviewing anyone whose interests could be adversely affected by the outcome of a security investigation, or anyone who may be able to assist with a security investigation.

Agency procedures should clearly distinguish between a security investigation and its remedies, and investigations into incidents and matters not related to security (eg, incidents that require other types of administrative, or criminal, investigation). Refer to Types of investigations.

Those responsible for security investigations should be aware of the extent and limits of their responsibilities and powers during a security investigation.

4.4. Appointing investigators

The person authorising an investigation should be the Security Executive officer (or other SES officer) who will approve the Terms of Reference and the investigation plan. In the interests of procedural fairness the investigator should be impartial, and not have an actual or apparent conflict of interest in the matter being investigated. See the Australian Government personnel security guidelines—Vetting Practices Section 6.2 – Procedural fairness guidelines and ICAC Guidelines on conflict of interest.

Agencies should provide relevant and appropriate training for investigators. For a criminal investigation, the appointed investigator should be:

• qualified to Certificate Level IV in Government (Fraud Control) or Certificate IV in Government (Investigation), or hold equivalent tertiary qualifications, or
• a sworn police officer.

A qualified investigator or a sworn police officer may supervise a person without the necessary investigative qualifications appointed to conduct an investigation.

4.5. Understand the role of an investigator

An investigator’s key tasks include:

• understand the incident being investigated and the Terms of Reference
• identify the relevant law, policy or procedures that apply
• make sufficient inquiries to ascertain all relevant facts about the incident
• ascertain whether an offence or incident has occurred based on the relevant facts
• report the findings, identifying the reasons for the findings, and
• make relevant recommendations.
4.6. Determine the nature of an investigation

Agencies should assess at the outset:

- whether the investigation is likely to be a criminal, security or other investigation
- the resources needed to conduct the investigation
- the authorisation needed to undertake the investigation, and
- the nature of the possible outcome of the investigation.

4.7. Terms of Reference for investigations

Agencies should detail a clear and comprehensive statement of the aims and Terms of Reference for each investigation including any limits on the investigation. The Terms of Reference could include:

- the background
- resources allocated (people, financial, etc)
- timeframes
- types of inquiries to be conducted
- powers of the investigating officer to collect evidence by:
  - obtaining information from people about policies, procedures and practices
  - accessing relevant records and other material
  - interviewing witnesses and suspects, and
  - search and surveillance
- the format of progress reporting and the final report, and
- any special requirements or factors specific to the investigation.

Agencies need to ensure the powers of the investigating officer are consistent with all relevant Commonwealth and jurisdictional legislation.

4.8. Conducting investigations

The Australian Government Investigations Standards (AGIS) provide an investigations best practice framework. However, compliance with AGIS is not mandatory when conducting security investigations. Agencies may wish to use the AGIS as a guide when developing their own procedures. The standards and model procedures in the AGIS cover such matters as:

- general and agency specific legislation and powers
- inter-agency relationships
- receipt of allegation (initial consideration and subsequent action)
- investigation management methodologies and support
- investigation practices
- investigation report or brief of evidence
• investigation result and review, and
• recovery actions.

Only some of the standards and model procedures in the AGIS may be relevant to security investigations.

The AGIS is available in hard copy from the AFP Client Services Team, at AOCC-Client-Liaison@afp.gov.au. Agency libraries may also hold copies.

Other useful guidance on conducting investigations is available at:

• NSW Ombudsman, *Investigating complaints—A manual for investigators*, and
• Ombudsman Western Australia, *Guidelines: Conducting administrative investigations*.

### 4.8.1. Assess the incident and develop an investigation plan

The investigator should assess:

• applicable legislation which may determine the nature of and set the framework for the investigation
• the nature of the incident
• how serious the incident is and therefore the possible level of harm it has for the agency, or more widely for Government
• whether the incident indicates the existence of a systemic problem
• whether it is part of a pattern of conduct, and
• whether it may breach any Australian law, especially any criminal provision.

Where insufficient power to collect any available or required evidence is identified, or if a conflict of interest is identified, the investigator should refer the investigation to another person or agency with the necessary powers.

The investigator should use the incident assessment to develop an investigation plan. The plan should identify:

• the key issues to be investigated
• any relevant legislation, particular provisions of a code of conduct, agency policy and procedures, particular standards and guidelines
• required evidence
• methods and avenues to collect the evidence
• legal requirements and procedures to be followed in collecting evidence, and
• the allocation of tasks, resources and timings.

The investigator should seek agreement from the officer authorising the investigation if the Terms of Reference and the investigation plan need to be amended as a result of the issues that develop during the course of the investigation.
4.8.2. **Gather evidence**

An investigator identifies, collects and presents information or evidence that goes to proving or disproving any matters of fact relating to an incident. In an investigation, the types of evidence are:

- physical evidence
- documentary evidence (records)
- oral evidence (recollections), and
- expert evidence (technical advice).

Evidence gathered in a security investigation may not be satisfactory in a criminal investigation. For guidance on evidence refer to the AGIS.

4.8.3. **Record and store evidence appropriately**

Investigators should maintain a separate file for each investigation which is a complete record of the investigation, documenting every step, including dates and times, all discussions, phone calls, interviews, decisions and conclusions made during the course of the investigation. The record should include the handling of the physical evidence. Investigators should store this file and any physical evidence securely to prevent unauthorised access, damage or alteration, to maintain confidentiality and to ensure continuity of evidence. The record should include any tampering with the file or physical evidence.

4.8.4. **Prepare the investigation report**

At the conclusion of the investigation the investigator is to report findings to the commissioning body or the decision maker, identify the reasons for the findings according to the Terms of Reference using supporting material, and make relevant recommendations.

An investigation may lead to a range of possible outcomes, including:

- disciplinary action
- dismissal of a disciplinary charge following a constituted hearing
- referral of a matter to an external agency for further investigation or prosecution, and
- changes to administrative or security policies, procedures or practices.

4.8.5. **Close the investigation**

The investigation is closed when all reports are completed and evidence is documented and filed. It is better practice for an independent person, preferably more experienced than the investigator, to review the closed investigation. This allows an impartial assessment of the investigation that may identify improvements to investigation practices.

4.8.6. **Standard of proof**

In administrative investigations, whether conducted for security or other reasons such as disciplinary purposes, the decision maker needs to be satisfied that the allegations are proved ‘on the balance of probabilities’.
For criminal investigations, the burden of proof for the elements of the charge is ‘beyond reasonable doubt’.
### Annex A—Categories of security incidents

Security incidents are categorised as follows:

<table>
<thead>
<tr>
<th>Type of incident</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Major security incident</strong></td>
<td><strong>Security violation</strong></td>
<td>A deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of official resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Examples are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• espionage or suspected espionage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• loss of material classified CONFIDENTIAL or above, or significant quantities of material of a lower classification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• actual or suspected compromise of material at any level including tampering with security containers or systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• actual or suspected hacking into any information and communications technology (ICT) system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• loss, compromise, suspected compromise, theft or attempted theft of classified equipment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• compromise of keys to security locks or of combination settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• recovery of previously unreported missing classified material or equipment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• unauthorised disclosure of official or classified information, significant loss or compromise of cryptographic keying material or a significant breach of ICT systems as assessed by DSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• loss, theft, attempted theft, recovery or suspicious incidents involving weapons, munitions, explosives, or hazardous materials whether nuclear, chemical, radiological or biological, or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• continuous breaches involving the same person or work area where the combination of the incidents warrants an investigation.</td>
</tr>
<tr>
<td>Type of incident</td>
<td>Definition</td>
<td>Examples</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| **Security breach** | An accidental or unintentional failure to observe the protective security mandatory requirements | Examples are:  
  - access passes or identification documents lost or left insecure  
  - security classified material left in UNCLASSIFIED waste bins, or  
  - security classified material not properly secured or stored. |
| **Security infringement** | Any incident that violates internal protective security procedures outlined in internal agency protective security procedures, other than those that can be categorised as a security breach or security violation | No examples as these are agency specific. |
Annex B—Other relevant Australian Government material and services

Contacts for advice and assistance about security incident recording and reporting and security investigations:

**Australian Security Intelligence Organisation (ASIO)**
Contact: 02-6249 6299 (24hrs)

**Australian Federal Police (AFP)**
Contact: Client Services Team
(02) 6256 7777

**Defence Signals Directorate (DSD)**
Contact: 1300 292 371

**Attorney-General’s Department**
For guidance on the Australian Government Fraud Control Policy and all aspects of fraud control refer to [http://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/default.aspx](http://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/default.aspx)

**Commonwealth Director of Public Prosecutions**

**Australian Government Crisis Coordination Centre**
ccc@ag.gov.au
Phone: 1300 243 222
Fax: 1300 004 650