2 Management structures and responsibilities

Table of Contents

2 Management structures and responsibilities 1
A. Purpose 2
B. Requirements 2
B.1 Core requirement 2
B.2 Supporting requirements 2
C. Guidance 3
C.1 Management structures 3
C.2 Chief Security Officer 3
C.3 Chief Information Security Officer 5
C.4 Security governance committee 6
C.5 Appointing security advisors 6
C.6 Protective security planning 9
C.7 Protective security practices and procedures 9
C.8 Investigating, responding to and reporting on security incidents 10
C.9 Foster a positive security culture 14
C.10 Security awareness training 15
D. Find out more 18
D.1 Change log 18
Annex A. Managing security incidents 1
Step 1: Report and record 1
Step 2: Assess and decide 1
Step 3: Respond and recover 2
Step 4: Learn 2
Annex B. Conducting security investigations 1
Determining the nature of an investigation 1
Step 1: Appoint investigator 2
Step 2: Develop an investigation plan 3
Step 3: Gather evidence 3
Step 4: Record and store evidence 4
Step 5: Prepare the investigation report 4
Step 6: Close the investigation 4

A. Purpose

1. This policy describes the management structures and responsibilities that determine how security decisions are made in accordance with security practices. This provides a governance base for entities to protect their people, information and assets.
2. Effective management structures and responsibilities require people to be appropriately skilled, empowered and resourced. This is essential to achieving security outcomes.

B. Requirements

B.1 Core requirement

The accountable authority must:

- ***a. appoint a Chief Security Officer (CSO) at the Senior Executive Service[1] level with a minimum security clearance of Negative Vetting Level 1, to be responsible for protective security in the entity***
- ***b. empower the CSO to make decisions about:***
  - ***i. appointing security advisors within the entity***
  - ***ii. the entity's protective security planning***
  - ***iii. the entity's protective security practices and procedures***
  - ***iv. investigating, responding to, and reporting on security incidents (other than cyber incidents)***
- ***c. appoint a Chief Information Security Officer (CISO) with appropriate capability and experience and a minimum security clearance of Negative Vetting Level 1, to be responsible for cyber security in the entity***
- ***d. empower the CISO to make decisions about:***
  - ***i. the entity's cyber security strategy and associated implementation program***
  - ***ii. appointing cyber security advisors within the entity***
  - ***iii. the entity's data and systems that process, store or communicate data***
  - ***iv. the entity's implementation of the Information Security Manual***
  - ***v. investigating, responding to, and reporting on cyber incidents.***
- ***e. ensure personnel and contractors are aware of their collective responsibility to foster a positive security culture, and are provided sufficient information and training to support this.***

B.2 Supporting requirements

Supporting requirements for management structures and responsibilities

#	Supporting requirements
Requirement 1. Security advisors	a. The CSO **must** be responsible for directing all areas of security to protect the entity's people, information and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services. b. The CISO **must** be responsible for the entity's cyber security program and associated implementation program. This includes appointing cyber security advisors to support them in the day-to-day delivery of cyber security, and to perform specialist services.
Requirement 2. Security procedures	Entities **must** develop and use procedures that ensure: a. all elements of the entity's security plan are achieved b. security incidents are investigated, responded to, and reported c. relevant security policy or legislative obligations are met.
Requirement 3. Security training	Entities **must** provide all personnel, including contractors, with security awareness training at engagement and annually thereafter.

[1] Where an entity has fewer than 100 employees the accountable authority may appoint their Chief Security Officer at the Executive Level 2 (EL2), providing the EL2:

- reports directly to the accountable authority on security matters, and
- has the sufficient authority and capability to perform the responsibilities of the CSO role.

#	Supporting requirements
Requirement 4. Specific training	Entities **must** provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training targeted to the scope and nature of the position.
Requirement 5. General email	Entities **must** maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information, cyber and physical security.

C. Guidance

C.1 Management structures

C.1.1 Management structure accountability for protective security

3. **Accountable Authority** – Under section 12 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), the accountable authority is the person or group of persons responsible for, and with control over, each Commonwealth entity's operations – answerable to the portfolio minister for the security of their entity (see the PSPF policy: Role of accountable authority).
4. **Chief Security Officer (CSO)** – SES officer (with appropriate seniority and a minimum security clearance of Negative Vetting Level 1) responsible for oversight of entity protective security arrangements across governance, information (other than cyber security), personnel and physical security (refer section C.2).
5. **Chief Information Security Officer (CISO)** – officer (with appropriate seniority and a minimum security clearance of Negative Vetting Level 1) responsible for the entity's cyber security strategy, associated implementation program and ensuring compliance with cyber security policy, standards, regulations and legislation. The CISO complements the CSO role, and is also likely to report directly to the CSO or accountable authority on cyber security matters, and work with the entity's Chief Information Officer, Chief Operating Officer or other senior executives in the entity (refer section C.3).
6. **Security governance committee** – Senior committee to support the accountable authority, CSO and CISO in achieving protective security objectives and monitoring performance, particularly where the entity's arrangements are large or complex (refer section C.4).
7. **Security advisors** – Personnel appointed to perform security functions or specialist services (refer section C.5).
8. **Line managers** – Responsible for positively influencing the protective security behaviour of their personnel (including contractors). See the PSPF policy: Ongoing assessment of personnel.
9. **Entity personnel, including contractors** – Responsible for understanding and applying robust security practices to protect government people, information and assets. See the PSPF policy: Ongoing assessment of personnel.

C.2 Chief Security Officer

10. The PSPF mandates a CSO **must** be appointed at the Senior Executive Service (SES) level and be empowered to oversee security across the entity and make security-related decisions. The CSO supports the accountable authority to protect the entity's people, information and assets and achieve the requirements outlined in PSPF policy: Role of accountable authority. Refer to section C.2.1 for CSO role and responsibilities.
11. The Department of Home Affairs recommends that for entities that are large, complex or carry high-risk and require multiple senior officers to manage security-related functions, the CSO be appointed at an appropriately senior level to manage these responsibilities.
12. The Department of Home Affairs recommends that the CSO:
    a. be at an appropriately senior SES level, commensurate with managing critical security-related incidents and emergencies in the entity
    b. chair or oversee any security governance committees within the entity (if established), refer to section C.4

c. oversee the preparation of the entity's PSPF annual security report for the approval of the accountable authority

d. report to the accountable authority on security matters

e. only perform functions that are consistent with overseeing security for the entity

f. oversee[2] any security advisors (other than cyber security advisors) within the entity, and

g. works with the CISO to retain visibility of the entity's cyber security maturity, for example through a security governance committee.

C.2.1 Chief Security Officer responsibilities

13. The CSO supports the accountable authority by providing strategic oversight of protective security across governance, information, personnel and physical security to assist continuous delivery of business operations. The CSO is responsible for fostering a culture where personnel have a high-degree of security awareness, reinforced through practices that embed security into entity operations.

14. **Requirement 1** states that the CSO is responsible for directing all areas of security to protect people, information and assets. This includes tailoring security arrangements to the scale and complexity of the entity. The intention is that as a single senior officer with central oversight and responsibility for security arrangements (other than for cyber security) in the entity, they have the flexibility to delegate the day-to-day activities of protective security where required.

15. Specific security advisor roles and titles are not mandated under this policy, other than the CSO and CISO roles. This provides flexibility for the CSO to establish and scale security arrangements. The Department of Home Affairs recommends the CSO ensure sufficient security advisor positions are in place to perform security management functions and ensure continuous delivery of government business. Section C.5 sets out the recommended specific functions that security advisors be appointed to perform.

16. Key oversight responsibilities of the CSO include:

a. supporting the accountable authority to ensure the safety of personnel (including contractors, visitors and clients), information and assets

b. ensuring sufficient security advisors are appointed to perform specific security functions for the entity (see section C.5)

c. embedding efficient and effective security management awareness and practices by setting the strategic direction for protective security planning and risk management (refer section C.6)

d. establishing effective procedures to achieve security outcomes that are consistent with the PSPF and other Australian Government policies and legal requirements (refer section C.7)

e. managing the entity's response to security-related crises, incidents and emergencies in accordance with the entity's security incident and investigation procedures, and establishing monitoring mechanisms across the entity (refer section C.8)

f. fostering a positive security culture where personnel understand their responsibilities to manage security risk (refer section C.9)

g. ensuring information and security awareness training programs are in place so personnel (including personnel and contractors located or travelling overseas) understand their security obligations (refer section C.10)

h. establishing security performance measures to monitor procedures to achieve required protections, address risks, counter unacceptable security risks, and improve security maturity (see the PSPF policy: Security maturity monitoring)

i. disseminating and managing intelligence and threat information to stakeholders across the entity

[2] Where another legislative obligation or structural arrangement requires a security advisor to report to another position in the entity (eg the Chief Information Officer), the CSO is recommended to retain oversight of the advisor's security related functions.

j. overseeing preparation of the entity's PSPF annual security report to accurately reflect its security maturity position and detail how it is addressing areas of vulnerability (see the PSPF policy: Reporting on security).

17. The scope and complexity of the CSO role depends on the nature of the entity's business and its risk environment. For smaller entities, it may be that the accountable authority takes on the role of the CSO and delegates the day-to-day functions of protective security to appointed security advisors.

18. The Department of Home Affairs recommends that the CSO has sufficient experience or be trained to perform the required security leadership and oversight functions.

C.3 Chief Information Security Officer

19. The PSPF mandates a CISO **must** be appointed and empowered to provide leadership and make decisions about cyber security across the entity. The CISO role supports the accountable authority and complements the CSO role. Where preferred, the accountable authority may appoint the CSO and CISO roles to the same officer.

20. The CISO role requires a combination of technical and soft skills such as business acumen, leadership, communications and relationship building. The role requires the CSIO to adopt a continuous approach to learning and up-skilling in order to maintain pace with the cyber threat landscape and new technologies.

21. When appointing the CISO, the accountable authority is responsible for determining who the CISO reports to. Where the CISO does not report directly to the CSO or the accountable authority on cyber security matters, the Department of Home Affairs recommends the CSO and the accountable authority retains visibility of the entity's cyber security maturity through a security governance committee on which the CISO holds membership.

22. The CISO may be located in another government entity where the entity's cyber security services are wholly provided through a shared services arrangement with another government entity. In such cases, the supported entity's accountable authority and CSO is required to establish suitable arrangements to retain visibility of cyber security matters.

23. The Department of Home Affairs recommends that for entities that are large, complex or carry high-risk and require multiple officers to manage cyber security-related functions, they report to a single senior officer. For example, the CISO appoints multiple cyber security advisors (for example Deputy CISOs or cyber security managers) to perform specific cyber security functions, and all report directly to the CISO.

24. The Department of Home Affairs recommends the CISO:

a. be at an appropriate level of seniority in the entity to perform the functions of the CISO

b. hold a security clearance at a level commensurate with the data holdings of the entity with minimum being Negative Vetting level 1

c. possess sufficient capability (combination of technical and soft skills) and experience to provide cyber security leadership and make informed cyber security decisions for the entity

d. hold membership on any security governance committees within the entity, refer to section C.4

e. report to the CSO or the accountable authority on cyber security matters

f. oversee any cyber security advisors (including for example deputy CISOs or cyber security managers) in the entity.

25. For further information on the CISO role, see the ISM's Guidelines for Cyber Security Roles.

C.3.1 Chief Information Security Officer responsibilities

26. **The core requirement** states that the CISO is responsible for cyber security, and is empowered to make decisions about the entity's cyber strategy and associated implementation program.

27. Key responsibilities of the CISO include:

a. supporting the accountable authority and CSO by providing cyber security leadership

b. overseeing the cyber security strategy and ensuring compliance with cyber security policy, standards, regulations and legislation – including:
    i. implementing the Information Security Manual's principles and guidelines
    ii. implementing the Australian Signal's Directorate's Strategies to mitigate cyber security incidents
    iii. reviewing and updating the entity's cyber security program to ensure its relevance in addressing cyber threats and harnessing business and cyber security opportunities
    iv. coordinating cyber security to ensure alignment of cyber security and the entity's business objectives
c. ensuring sufficient cyber security advisors (for example deputy CISOs or cyber security managers) are appointed to perform specific security functions for the entity (see section C.5)
d. overseeing the entity's systems and the data they process, store or communicate, including to ensure the security risks associated with the system's operation are acceptable before it is granted authorisation to operate (see the PSPF policy: Robust ICT systems)
e. managing the entity's response to cyber-related crises, incidents and emergencies in accordance with the entity's security incident and investigation procedures, and establishing monitoring mechanisms across the entity (refer section C.8)
f. contributing to the preparation of the entity's PSPF annual security report cyber security components to accurately reflect its security maturity position and detail how it is addressing areas of vulnerability (see the PSPF policy: Reporting on security).

28. For further information on the CISO role, see the ISM's Guidelines for Cyber Security Roles.

C.4 Security governance committee

29. Under the Public Governance, Performance and Accountability Rule 2014, entities are required to have an audit committee to review systems of risk oversight and management. Audit committees perform an important role in oversight of risk management, including security risks.
30. In addition, entities may choose to establish a separate security governance committee to support the accountable authority and CSO by:
    a. providing a cohesive and coordinated approach to risk and security
    b. fostering a positive security culture
    c. establishing longer-term protective security goals and objectives
    d. monitoring security plans and identifying and managing risks
    e. considering outcomes of security incidents and investigations
    f. facilitating information sharing for security improvements.
31. While not mandatory, where an entity has a security governance oversight committee, the Department of Home Affairs recommends that the CSO be appointed as the Chair of the committee and that the CISO holds membership.

C.5 Appointing security advisors

32. Under the core requirement and **Requirement 1(a)**, the CSO is empowered to appoint security advisors and **Requirement 1(b)**, the CISO is empowered to appoint cyber security advisors. In making these decisions, the CSO and CISO are encouraged to:
    a. consider the scope and responsibilities delegated to each position within the context of the entity's risk environment, complexity of business, infrastructure, size and other relevant aspects
    b. establish appropriate arrangements for managing the responsibilities of advisors (where this results in security advisors **not** reporting directly to the CSO or the CISO, the CSO or CISO maintains visibility of performance and outcomes)

c. appoint advisors at a level that requires only broad direction in terms of delivering objectives, mission or functions

d. ensure delegations allow security advisors to undertake specific action in line with the policy of the entity, or to review previous actions or decisions in the work area

e. determine the appropriate competencies, experience and specialist skills or qualifications required to undertake the appointed security role/s, including comprehensive knowledge of the PSPF.

C.5.1 Suggested security advisor functions

33. The suggested functions listed below (sections C.5.1– C.5.1.5) align with the four security outcomes (governance, information, personnel and physical). CSOs and CISOs may determine what they delegate to advisors and what functions advisor roles cover. This may mean that an advisor is appointed to perform functions spanning the categories suggested below. They may also perform other functions where appropriate.

34. CSOs and CISOs are responsible for encouraging a collaborative approach between security advisors to enable governance, information, personnel and physical security measures that are complementary, promote robust security practices and achieve the entity's security objectives.

C.5.1.1 Governance security functions

35. Advisors may assist the CSO by:

a. identifying and managing governance security risks

b. ensuring security plans and procedures are effective in achieving specified security outcomes

c. monitoring security systems that facilitate the entity's capacity to function and identify security risks

d. providing advice on protective security and security risk management arrangements

e. preparing security reports for the CSO or security committees, and assisting with gathering information to meet annual security reporting obligations

f. coordinating and conducting security reviews

g. liaising with law enforcement and intelligence agencies, other emergency services, service providers, clients and stakeholders

h. responding to and coordinating security incident arrangements and being accessible for personnel to discuss security issues or concerns

i. managing simple security investigations and escalating complex investigations to the CSO

j. promoting the security and risk culture where personnel value and protect government information and assets

k. establishing networks and relationships to understand the entity's business functions and vulnerabilities

l. ensuring security requirements are considered in other entity plans such as business continuity, fraud control and awareness.

C.5.1.2 Information security functions

36. Advisors may assist the CSO by:

a. ensuring appropriate procedures are established (in accordance with the PSPF) for the handling and protective marking of information

b. managing access to information

c. contributing to personnel awareness of information security obligations around appropriate use of ICT equipment and official information

d. providing briefings and advice to entity personnel on information, including briefings to personnel located or travelling overseas

C.5.1.3 Information security - cyber security functions

37. Advisors may assist the CISO by:

    a. identifying and managing cyber security risks

    b. managing access to data and systems that process, store or communicate that data

    c. ensuring the entity's ICT systems are protected against unauthorised access or compromise (as defined in C.8.1), and information in electronic form is stored, processed and communicated in accordance with the law, Australian Government policies,[3] and the information security requirements detailed in the entity's security plan

    d. monitoring information security systems and managing cyber security contractors to ensure the continued delivery of secure services

    e. safeguarding information from cyber threats and ensuring robust ICT systems

    f. responding to and managing cyber incidents

    g. coordinating and conducting cyber security reviews

    h. liaising with and managing cyber security contractors in the delivery of secure services including:

        i. telephones

        ii. internet and email gateways

        iii. cloud-based services

        iv. data storage and recovery.

C.5.1.4 Personnel security functions

38. Advisors may assist the CSO by:

    a. identifying and managing personnel security risks

    b. managing the entity's personnel security program

    c. developing and conducting security awareness training programs (including refresher and specialised training)

    d. managing eligibility and suitability of personnel procedures

    e. monitoring ongoing assessment of personnel

    f. coordinating the personnel security aftercare program for separation of personnel, including withdrawing accesses and informing about ongoing security obligations

    g. providing advice on personnel security, including briefings to personnel located or travelling overseas.

C.5.1.5 Physical security functions

39. Advisors may assist the CSO by:

    a. identifying and managing physical security risks

    b. ensuring a safe and secure physical environment for entity personnel, contractors, clients and the public

    c. ensuring a secure physical environment for official resources

    d. managing physical security measures and access controls to protect facilities, information and physical assets, for example certification of security zones

    e. liaising with and managing security contractors in the delivery of security services, including:

        i. Security Construction and Equipment Committee (SCEC) endorsed consultants

[3] Entitles are encouraged to consider where other legislative obligations overlap with security advisor roles. For example, the Privacy (Australian Government Agencies — Governance) APP Code 2017 requires entities to appoint a dedicated privacy officer(s) to maintain a record of the entity's personal information holdings and a register of privacy impact assessments.

ii. security industry specialists
iii. security guards (guarding)
iv. safe hand and overnight couriers
v. secure destruction
vi. locksmithing services

f. undertaking strategic planning for preparation of new or green-field sites.

40. Given the range and complexity of security functions, it may be appropriate to the entity's operations or size to appoint separate advisors for information, personnel and physical security matters.

41. Many functions of a security advisor involve specialised skills. The Department of Home Affairs suggests such advisors demonstrate comprehensive knowledge or technical competencies in:

    a. the PSPF and supporting technical guidance, for example ASIO Technical Notes and the Australian Government Information Security Manual

    b. the application of security measures relevant to the advisor's functions (eg professional cyber security certifications)

    c. managing security risk assessments.

42. The knowledge, competencies and skills can be attained through on-the-job training, prior experience in a related field or formal qualifications (eg tertiary qualifications such as the Certificate IV, Diploma in Government Security or equivalent qualification). Where entities provide training towards formal qualifications for security advisors, the Department of Home Affairs recommends that this training be delivered by a Registered Training Organisation (RTO). RTOs are accredited training providers that offer nationally recognised training courses. A list of these organisations is available from www.training.gov.au.

43. Where the CSO or CISO contracts service providers for specific security functions, including where professional technical certification is required (eg SCEC security zone consultants for Type 1a security alarm system compliance and IRAP Assessors for ICT systems), the entity retains the security accountability. This does not transfer to the contractor. The Department of Home Affairs recommends the CSO, CSIO or appointed security advisor establishes arrangements to monitor any outsourced security service providers.

44. For information on ensuring contractors comply with security requirements, see the PSPF policy: Security governance for contracted goods and service providers.

C.6 Protective security planning

45. Security planning establishes the strategic direction and sets out the expectations for the efficient and effective security management practices in the entity. This includes ensuring security risks are managed effectively and consistently across the entity to adapt to change, minimise damage and disruption and build resilience.

46. The CSO defines the strategic direction and allocation of resources to deliver the strategy, strengthen operations and improve the entity's security maturity in order to make sound decisions about protective security planning. For information on preparing the security plan to manage risks, see the PSPF policy: Security planning and risk management.

C.7 Protective security practices and procedures

47. Protective security practices reflect the entity's implementation of the PSPF core and supporting governance, information, personnel and physical security requirements.

48. Protective security practices are more likely to be effective in achieving the required protection when they are demonstrated by senior management, embedded into day-to-day operations, and are well understood by all personnel with clear links to why they're important and what they're designed to accomplish.

49. **Requirement 2** mandates that entities must develop procedures to cover all elements of protective security consistent with relevant PSPF policy. The Department of Home Affairs recommends that entities develop security procedures in conjunction with other security and risk planning and update these

procedures when significant changes in the risk environment occur. The Department of Home Affairs also recommends entities put in place measures to monitor the effectiveness of procedures and security performance and update annual security awareness training with relevant messaging.

C.8 Investigating, responding to and reporting on security incidents

50. Managing security incidents and investigations helps monitor security performance, identify inadequacies in security procedure, and detect security risks in order to implement appropriate treatments. Through effective reporting and investigation of security incidents, entities can identify vulnerabilities and reduce the risk of future occurrence.

51. In addition to the annual security reporting obligations, certain security incidents are reportable to other entities (see the PSPF policy: Reporting on security). This includes reporting cyber incidents to the Australian Cyber Security Centre (ACSC) in Australian Signals Directorate as early as possible. Where the ACSC agrees to participate in an investigation following a cyber incident, it is important that no actions which could affect the integrity of evidence should be carried out before the ACSC becomes involved.

C.8.1 Security incidents

52. Security incident management is the process of identifying, managing, recording and analysing any irregular or adverse activities or events, threats and behaviours in a timely manner. Effective monitoring of security incidents is fundamental to good security management. In turn, good security management contains the effects of a security incident and enables recovery as quickly as possible.

53. Information gathered on security incidents assists the CSO or CISO (for cyber incidents) to determine the adequacy of protective security practices, measures security culture, highlights vulnerabilities in security awareness training and informs security improvement activities.

54. A security incident might have wide-ranging and critical consequences for the entity and the Australian Government. A security incident is defined as an:

    a. **action**, whether deliberate, reckless, negligent or accidental that fails to meet protective security requirements or entity-specific protective security practices and procedures that results, or may result in, the loss, damage, corruption or disclosure of official information or resources

        i. Information compromise includes, but is not limited to: loss, misuse, interference, unauthorised access, unauthorised modification, or unauthorised disclosure.

    b. **approach** from anybody seeking unauthorised access to official resources, or

    c. observable **occurrence or event** (including natural disaster events, terrorist attacks etc) that can harm Australian Government people, information or assets.

55. The Information Security Manual defines a cyber security incident as an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations. See the ISM's Guidelines for cyber incidents for further information.

56. A significant security incident is a deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, compromise, corruption or disclosure of official resources.

57. Examples of security incidents include:

    a. Criminal actions such as actual or attempted theft, break and enter, vandalism or assault.

    b. Loss of personal information that is likely to result in serious harm. In some circumstances, the loss of personal information may be considered a security breach – refer to The OAIC's Notifiable Data Breaches scheme.

    c. Security classified material not properly secured or stored.

    d. Security classified material left in inappropriate waste bins or government assets to be sold or disposed of.

    e. Deliberate disregard of implementing a PSPF requirement.

f. Access passes or identification documents lost or left unsecured.

g. Incorrect handling of security or classified 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.

h. Compromise of keys to security locks, or of combination settings.

i. Sharing computer passwords.

j. Vandalism.

58. Examples of significant security incidents:

a. Espionage or suspected espionage.

b. Actual or suspected compromise of material at any level, including tampering with security containers or systems.

c. Loss, compromise, suspected compromise, theft or attempted theft of classified equipment.

d. Actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored.

e. Loss of material classified PROTECTED or above, or significant quantities of material of a lower classification.

f. Recovery of previously unreported missing classified material or equipment.

g. 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 the Australian Signals Directorate (ASD).

h. Continuous breaches involving the same person or work area where the combination of the incidents warrants an investigation.

i. Loss, theft, attempted theft, recovery or suspicious incidents involving weapons, ammunitions, explosives or hazardous materials including nuclear, chemical, radiological or biological.

j. Actual or suspected unauthorised access to an ICT system.

59. PSPF policy: Reporting on security outlines an entity's obligation to report security incidents to external entities. Non-compliance with reporting of security incidents obligations is considered a security incident.

60. Where a suspected security incident involves the major compromise of official information or other resources that originate from, or are the responsibility of another entity, it is important to seek advice from the originating entity prior to instigating any investigation. The originating entity 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 entity carries out the investigation.

C.8.1.1 Detecting security incidents

61. Early detection of a security incident and timely reporting to the CSO, CISO or security advisor are critical in order to expedite protection, containment and recovery in response to the incident. Establishing simple channels for personnel (including contractors and personnel travelling or working remotely) to report security incidents, or suspected incidents, is an effective approach to ensuring timely reporting.

62. Many potential security incidents are observed by personnel. It is important that all personnel, including contractors, understand how and when to report potential incidents or concerns. The Department of Home Affairs recommends that security incident reporting and consequences, with practical examples, be included in security awareness training.

63. While reporting of security incidents by personnel is a common means of detection, the Department of Home Affairs recommends that the CSO and CISO consider other identification and monitoring methods to supplement reporting of incidents.

64. For details on security incident reporting involving contracted goods and service providers, see the PSPF policy: Security governance for contracted goods and service providers.

C.8.1.2 Managing security incidents

65. **Requirement 2** mandates the entity must establish procedures for managing security incidents.

66. The Department of Home Affairs recommends that procedures are consistent, appropriate and fair and ensure the entity is ready to respond to any security incidents that may arise. They may include:

    a. personnel, including contractors, immediately reporting security incidents to a centralised point in the entity (CSO, CISO or security advisors) and include arrangements for personnel travelling or working remotely

    b. formal procedures and mechanisms to make it easy to report security incidents (including responding to and investigating incidents that occur outside of the entity's premises)

    c. security advisors maintaining records of reported incidents and any other security incidents

    d. handling procedures once a security incident has been reported, including:

        i. clearly defined roles and responsibilities (of personnel involved in the administration of security incidents and the conduct of investigations)

        ii. escalation points, relationships and connection points (internal or external) and communication channels

        iii. timeframes for incident response and recovery

        iv. assessment and categorisation of the level of harm or compromise

        v. technical requirements and continuity

        vi. prioritisation where multiple incidents or events occur simultaneously

        vii. addressing entity-specific issues or incident types

        viii. linkages to other entity procedures such as business continuity or disaster recovery plans

        ix. reporting to the CSO, CISO (for cyber incidents) and security governance committee

        x. testing and review cycles

    e. suitable feedback processes to ensure that personnel reporting information security events are notified of results after the issue has been dealt with and closed.

67. Where security investigation functions are shared across entity work areas or with an outsourced service provider, the Department of Home Affairs recommends that the CSO, CSIO (or another delegated SES officer) maintain oversight of the investigation and establish mechanisms to monitor the investigation and ensure communication of issues, findings and decisions to all relevant parties.

68. Refer to **Annex B** for further guidance on security incident management.

C.8.1.3 Recording security incidents

69. Recording security incidents provides a valuable source of data to obtain insight into an entity's security environment and performance. For example, multiple minor security incidents could indicate poor security awareness and could alert the entity to the need for increased security training and education.

70. The Department of Home Affairs recommends that the CSO and CISO (for cyber incidents) maintains oversight of these records and regularly analyses security incidents to identify trends and systemic issues. Entities can develop mechanisms for recording incidents that best suit their security environment and operational requirements.

C.8.2 Security investigations

71. Not all security incidents warrant investigation.[4] The CSO or CISO (for cyber incidents) determines when a security incident is serious or significant enough to commence an investigation. Investigating security

[4] Noting that under the Notifiable Data Breach scheme a data breach likely to result in serious harm to any of the individuals to whom the information relates requires an objective assessment. Refer to guidance material on identifying eligible data breaches.

incidents (actual or suspected), may be necessary to resolve an existing breach or vulnerability and remediate the impact. An investigation may provide valuable information for future risk reviews and assessments and will help entities to evaluate current security plans and procedures.

72. When gathering evidence following a cyber security incident, it is important that it is gathered in an appropriate manner and that its integrity is maintained. In addition, if the ACSC is requested to assist with investigations, no actions which could affect the integrity of evidence should be carried out before the ACSC becomes involved.

C.8.2.1 Case Study – Australian National Audit Office audit Administration of security incidents, including the conduct of security investigations

The audit found that entities can encounter a wide range of security incidents including the theft or loss of assets, the inappropriate handling or suspected compromise of classified information, instances of unauthorised access to information or restricted work areas and the physical or threatened assault of staff. The number and type of security incidents generally reflects the nature of each entity's work, including the level of classified information. It may also be influenced by factors such as the conduct of regular security inspections, the strength of security awareness among staff, and the ease of reporting security incidents.

The audit also found that the majority of security incidents (recorded by the audited entities) related to matters that did not warrant a formal investigation. For example, many security incidents were of a minor or procedural nature and were dealt with by local managers or supervisors taking remedial action or were addressed through the conduct of routine inquiries.

Minor security incidents were generally addressed by less formal mechanisms, such as procedural inquiries, and more serious incidents were the subject of formal investigation. In some cases, preliminary investigations were conducted if, for example, all the details or the extent of the impact of a security incident were not known before deciding whether or not to conduct a formal investigation.

73. A security investigation:
    a. is a formal process of examining the cause and extent of a security incident that has, or could have, caused harm to individuals, the entity, another entity or the national interest
    b. gathers evidence that may be admissible for any subsequent action whether under criminal, civil penalty, civil, disciplinary or administrative sanctions
    c. prevents re-occurrence of the incident by implementing improvements to entity systems or procedures
    d. protects both the interests of the Australian Government and the rights of affected individuals.
74. Once the CSO, CISO or appointed security advisor has established the need for an investigation, they are encouraged to assess:
    a. the seriousness or complexity of the incident
    b. the nature of the possible outcome of the investigation (administrative, disciplinary, civil or criminal)
    c. if the incident is criminal in nature and needs to be referred to an external entity
    d. the resources needed to conduct the investigation
    e. who is the best placed or qualified person to complete the investigation and what support they need
    f. an agreed investigation process including timeframes
    g. the authorisation needed to undertake the investigation
    h. decision-makers and reporting obligations.
75. The Department of Home Affairs recommends that, where possible, entities apply the Australian Government Investigations Standards (AGIS) to maintain a minimum quality standard within investigations.
76. The principles of procedural fairness apply to all investigations. These principles require that individuals whose rights, interests or expectations are adversely affected, 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. Procedural fairness gives regard to ensuring the security integrity of any current or future investigation of the entity or of another entity.

77. **Requirement 2** mandates that the CSO must establish procedures to investigate, respond to, and report on security incidents. The Department of Home Affairs recommends investigation procedures cover:
    a. terms of reference and the investigation plan, authorised by the CSO, CISO or other SES officer
    b. responsibilities, including the investigator, approving officer and other relevant parties
    c. qualifications and training (as mandated in **Requirement 4**) required for investigators
    d. procedural fairness and standards of ethical behaviour to ensure the investigator is impartial, without actual or apparent conflict of interest in the matter being investigated
    e. actions on receiving a complaint or allegation, including anonymous allegations or reports from whistle blowers
    f. case management procedures to ensure any case records, activities, recommendations and decisions adhere to the agreed process (AGIS is the recommended standard)
    g. 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
    h. referral points to ASIO, the relevant law enforcement service and ASD
    i. decision points and agreed escalation and approval phases, including keeping the CSO, CISO or delegated officer informed of the investigation's progress
    j. major findings and recommendations
    k. final report requirements.
78. Refer to **Annex B** for guidance on conducting security investigations.

C.9 Foster a positive security culture

79. Fostering a positive protective security culture is critical to achieving security outcomes. Through a robust security culture, the threat to an entity and its assets can be significantly decreased.
80. As mandated in the core requirement, the accountable authority must ensure personnel, including contractors, are aware of their collective responsibility to foster a positive security culture and are provided sufficient information and training. The CSO, supported by any appointed security advisors, is responsible for providing security leadership and promoting a culture where personnel value, protect and use entity information and assets appropriately.
81. In addition to keeping an entity and its personnel safe, a strong and healthy security culture helps to increase internal and external trust, embed consistent positive behaviour and support personnel to engage productively with risk.
82. A positive security culture is one where:
    a. security is prioritised and promoted across the entity by the accountable authority and senior leadership
    b. security is built into an entity's business operations
    c. security is an enabler of business, supporting accessibility of services
    d. security risks are identified and managed and personnel understand those risks and their responsibilities in relation to them
    e. security awareness training is effective in ensuring personnel, including contractors, are:
        i. aware that security is everyone's business
        ii. able to understand and comply with security-related obligations and entity-specific practices and procedures
        iii. equipped and supported to engage with risk and make risk-based decisions

iv. aware of the consequences of non-compliance with security practices and procedures

v. comfortable to challenge others on non-compliance with entity security practices and procedures

vi. confident in making decisions on applying protective markings, storing and sharing government information

f. security incidents and breaches are reported, recorded and investigated appropriately according to clear entity procedures

g. implementation of protective security policies is mature and well-managed

h. entity security procedures are easy to understand, current and visible to all personnel

i. classified information is protected from unauthorised disclosure or compromise and personnel apply the need-to-know principles

j. security improvements are encouraged and promoted within the entity.

83. The Department of Home Affairs recommends the CSO establishes appropriate metrics to measure the maturity of the entity's security culture. See the PSPF policy: Security maturity monitoring.

C.10 Security awareness training

84. The core requirement mandates that entities ensure personnel and contractors are provided with sufficient information on their responsibilities under the PSPF, and their entity-specific security responsibilities.

85. The core requirement is supported by:

a. **Requirement 3** that mandates all personnel, including contractors, are provided with security awareness training upon engagement and annual refresher training

b. **Requirement 4** that mandates all personnel in specialist and high-risk positions, including contractors and security incident investigators, must be provided with specific security awareness training targeted to the scope and nature of the position.

86. Security awareness training is an important element of protective security and supports implementation of physical, information and personnel security policies, practices and procedures. The Department of Home Affairs recommends that entities use their security plan to identify areas to include in their security awareness training program.

87. Security awareness training is most effective when it:

a. delivers an ongoing security awareness program to inform and regularly remind individuals of security responsibilities, issues and concerns

b. briefs personnel on the access privileges and prohibitions attached to their security clearance level prior to being given access, or when required in the security clearance renewal cycle

c. ensures that personnel who have specific security duties receive appropriate and up-to-date training

d. fulfils security clearance renewal briefing requirements for all personnel and contracted service providers who hold a security clearance of Negative Vetting Level 1 or higher

e. clearly communicates to all personnel, including contractors, the entity's protective security practices and procedures.

88. Entities are encouraged to strengthen security awareness through:

a. campaigns that address the ongoing needs of the entity and the specific needs of sensitive areas, activities or periods of time

b. security instructions and reminders via publications, electronic bulletins and visual displays such as posters

c. protective security-related questions in personnel selection interviews

d. drills and exercises

e. inclusion of security awareness and attitudes in the entity performance management program.

C.10.1 Delivery of security awareness training

89. The Department of Home Affairs recommends that the CSO decide on the most appropriate delivery method to ensure consistent delivery of training within their entity or those entities they provide training to as part of a lead security arrangement.

90. The Department of Home Affairs recommends that in meeting **Requirement 3** to provide security awareness training upon engagement and annually thereafter, entities also provide:

    a. advice to personnel on entity-specific asset management and loss reporting procedures prior to them taking custody of assets, including entity fraud measures

    b. a safety handbook for all personnel that includes emergency response guidelines and contacts, as well as entity-specific safety requirements and procedures

    c. regular safety exercises and drills for personnel

    d. personnel with specific emergency safety or security roles with regular training, as well as assessment of their ongoing competency

    e. specialist training to meet entity-specific risks

    f. targeted security awareness training where the entity has identified a need based on their risk profile, or when the entity has an increased or changed threat environment.

91. If an entity elects to use an outsourced training provider to deliver the security awareness training, the Department of Home Affairs recommends they have sufficient knowledge of the PSPF and expertise in delivering adult education.

C.10.2 Content of security awareness training

92. The Department of Home Affairs recommends that security awareness training programs or briefings for all personnel include:

    a. an overview of protective security requirements, procedures and security culture in the entity

    b. personal safety and security measures in entity facilities and in the field

    c. individual and line manager security responsibilities

    d. confidentiality, integrity and availability requirements for information and assets, including intellectual property

    e. understanding entity-specific security risks and threats:

        i. the protective security policies and procedures for their area

        ii. the risks the policies and procedures are designed to mitigate against

        iii. the roles and responsibilities of personnel in relation to the policies and procedures.

    f. information control measures (need-to-know principle)

    g. overseas travel safety and security

    h. unusual and suspicious behaviour

    i. asset protection

    j. reporting requirements, including but not limited to:

        i. reporting security incidents (including compromise of information, breach of entity procedures, data spills etc)

        ii. contact reporting, including the Contact Reporting Scheme

        iii. reporting concerns about other personnel, including their suitability to access Australian Government resources

        iv. any other entity-specific reporting requirements including public interest disclosure (whistleblowing) under the *Public Interest Disclosure Act 2013*.

93. Previously reported or investigated security incidents can be used in security awareness training as examples demonstrating what could happen, how to respond to incidents, and how to minimise them in the future. The Department of Home Affairs recommends that information be redacted to maintain appropriate confidentiality.

C.10.2.1 Additional content for security-cleared personnel

94. The Department of Home Affairs recommends that, as a minimum, security awareness training programs or briefings for security-cleared personnel:
    a. ensure that people who have access to security classified resources, understand and accept their day-to-day security responsibilities and reporting obligations (eg changes of circumstances, and suspicious, ongoing, unusual or persistent contacts)
    b. provide clearance holders with briefing and training reminding them of their clearance responsibilities at regular internals
    c. include training and briefings from or in consultation with compartment owners, for personnel with access to Sensitive Compartmented Information.

C.10.2.2 Content for high-risk positions

95. **Requirement 4** mandates that entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training to address the risks related to the nature and scope of their work or specialisations. Specialist or high-risk positions could include:
    a. sensitive or priority negotiations or policy work
    b. responsibility for or access to valuable or attractive assets
    c. working remotely or in dangerous conditions
    d. being required to liaise with foreign officials, or regularly share information with foreign officials.

C.10.3 Security awareness refresher training

96. Under **Requirement 3**, entities are required to provide personnel with security awareness training annually. The CSO determines the form (eg in person, online), scope of coverage and content required for the annual training requirement to maintain sufficient awareness of security requirements and obligations to protect the entity's people, information and assets.

97. The Department of Home Affairs recommends that the CSO consider:
    a. the entity's risk and current threat environment
    b. goals and objectives of the entity's security plan
    c. any identified inadequacies in previous methods of training or consistent failure to understand content, particularly when systemic or reoccurring security incidents indicate potential vulnerabilities in awareness training.

C.10.4 Security email address

98. The siloing of security information in an entity can inhibit effective security management. Silos may be the result of a number of behavioural or system problems, including something as simple as email management. To address this, **Requirement 5** mandates a monitored email address for security-related matters to protect against changes in security personnel and facilitate the flow of security-related information.

99. The Department of Home Affairs recommends that the email address:
    a. be generic in nature
    b. take the form of security@[entityname].gov.au or cso@[entityname].gov.au

c. is monitored to ensure the flow of security-related information to the CSO, security advisors, committees and other areas in the entity as appropriate

d. is provided to the Department of Home Affairs (at PSPF@homeaffairs.gov.au) and other relevant entities to maintain contact with the entity and keep informed of changes in security personnel.

100. Where the entity is unable to provide a generic email address for security-related matters and relies on an individual's email address, entities are encouraged to ensure the flow of security information is maintained during periods of absence, or if the person leaves the position. For example, the individual's email nominated for security-related matters is monitored by another officer, or is accessible to other officers who perform security functions.

101. This requirement does not preclude entities from maintaining other security-related mailboxes (eg to limit information based on the need-to-know or for sensitive matters). However, the main monitored email address will be used for all PSPF related correspondence unless otherwise advised.

D. Find out more

102. Other legislation and policies include:

a. Commonwealth Fraud Control Framework

b. Australian Government Investigations Standards

c. Public Governance, Performance and Accountability Rule 2014

d. Information Security Manual – Guidelines for cyber incidents

e. Information Security Manual – Guidelines for cyber security roles

f. ISO/IEC 27035: Information technology — Security techniques — Information security incident management

g. ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls information security incident management section

h. Office of the Australian Information Commissioner, Privacy Act 1988, Guides and APP guidelines.

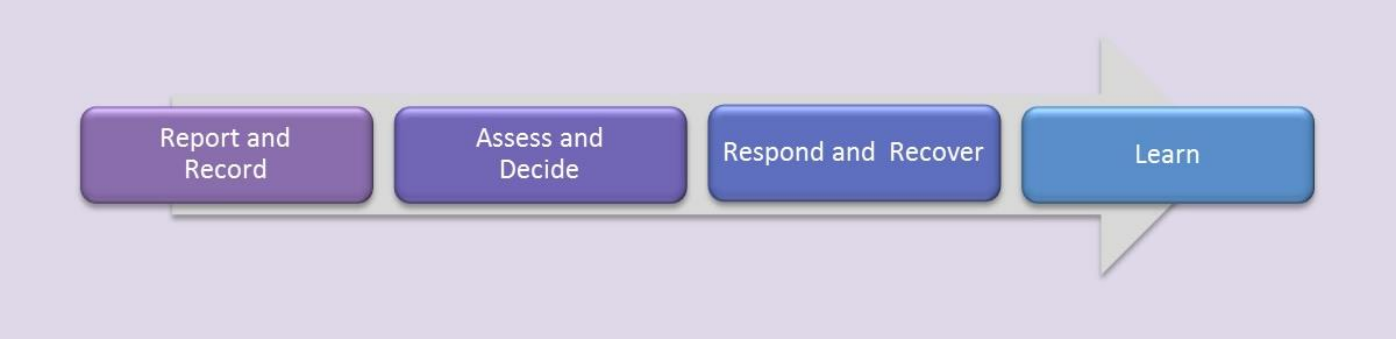
D.1 Change log

Table 1 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy
v2018.2	Jul 2019	Throughout	Remove GovDex references
v2018.3	Apr 2020	Supporting requirements, throughout	Moved Requirement to report Significant security incidents to PSPF Policy 5: Reporting on security and updated links
V2018.4	Mar 2023	Throughout	Updated AGIS hyperlinks
V2018.5	Aug 2023	Core and throughout	Mandate CSO hold an NV1 security clearance and mandate the CISO role.

Annex A. Managing security incidents

Annex A Figure 1 Managing security incidents process



Step 1: Report and record

1. Establishing simple channels for personnel to report security incidents or suspected incidents is an effective way to ensure timely reporting. The Department of Home Affairs recommends that entity security procedures:

a. require personnel, including contractors, to report security incidents to a centralised point in the entity (for example to CSO or security advisor)

b. specify the roles and responsibilities of personnel involved in the administration of security incidents and the conduct of investigations

c. establish formal procedures and mechanisms to make it easy to report security incidents

d. require the security advisors to maintain records of any reported incidents and any other security incidents

e. have suitable feedback processes to ensure that personnel reporting information security events are notified of results after the issue has been dealt with and closed.

2. The Department of Home Affairs recommends entities record the details of each reported security incident, including:

a. time, date and location of security incident, including how the incident was detected

b. type of official resources involved

c. description of the circumstances of the incident, including any personnel or locations involved

d. nature or intent of the incident, eg deliberate or accidental

e. assessment of the degree of compromise or harm

f. whether it is an isolated incident or part of a broader reoccurring issue

g. summary of immediate action (including containment or eradication) and any long-term action taken (including post-incident activities).

Step 2: Assess and decide

3. Once a security incident is recorded, the Department of Home Affairs recommends it is assessed by the CSO or appointed security advisor to:

a. confirm it is a genuine security incident rather than a false alarm or vexatious complaint

b. determine the type of incident and scale of harm resulting from the incident

c. decide what action is required to address the incident (by whom and when), for example:

i. no further action

ii. amendments to entity procedures, systems or training

iii. containment, recovery or eradication action required

iv. training or performance management activities with the individual/s involved in the incident

v. security investigation

vi. escalation to CSO, accountable authority or responsible minister, or

vii. external reporting or referral to appropriate authority (refer to Table 3 in Error! Reference source not found.).

Step 3: Respond and recover

4. It is appropriate that procedures for responding to serious security violations are formal. This reflects the significance these deliberate or reckless actions may have on security.

5. After an incident has been contained, it may be necessary for eradication or recovery action to be taken to restore information or systems. For details on managing cyber incidents, refer to the Guidelines for Cyber Incidents.

Step 4: Learn

6. Embedding post-incident learning into incident reports or updated procedures can provide useful insights into opportunities for improvements and emerging issues, vulnerabilities in processes and training, or personnel's understanding of how to apply security obligations. The Department of Home Affairs recommends that a process of continual improvement be applied to monitoring, evaluating, responding to and managing security incidents.

7. The Department of Home Affairs recommends that entities identify, document and share learnings internally (ie with and between the accountable authority, security advisors and security governance committee) and externally, where appropriate (ie with co-located entities, entities with similar risk profiles or through whole-of-Government arrangements).

8. Possible questions to consider once the incident is resolved:

   a. Were the procedures adequate to deal with the incident and were all stages of incident management followed?

   b. Were the right people involved and were escalation points and timeframes sufficient and useful?

   c. Did the incident highlight areas of vulnerability and if so, what action is being taken to address these vulnerabilities?

   d. Could the incident have been prevented? If so, how?

   e. Could the incident have been detected earlier, or damage reduced if detected earlier?

   f. What were the triggers and is there a way to prevent future occurrences?

   g. Is it a recurring incident or becoming systemic, if so, what additional protection or action is required to prevent further incidents?

Annex B. Conducting security investigations

1. Although not mandatory for security investigations, the Australian Government Investigations Standards provides an investigations practice framework that entities are encouraged to adopt.

Determining the nature of an investigation

2. Once the CSO, CISO (for cyber incidents) or appointed security advisor has established the need for an investigation, they are encouraged to assess from the outset:

a. the seriousness or complexity of the incident

b. the type of investigation based on likely outcome (administrative, administrative security, civil or criminal)

c. if the incident is criminal in nature and needs to be referred to an external entity

d. the resources needed to conduct the investigation

e. who is the best placed or qualified person to complete the investigation and what support do they need

f. timeframes for the investigation

g. the authorisation needed to undertake the investigation

h. the nature of the possible outcome of the investigation.

Criminal investigations

3. A Commonwealth criminal offence refers to an act that will generally be an offence under the *Crimes Act 1914* or the Criminal Code or other Commonwealth legislation.

4. The purpose of a criminal investigation is gathering admissible evidence which may lead to placing the offender/s before the court.

5. As outlined in the Australian Government Investigations Standards, if a security matter is considered by the entity to be a serious crime or complex criminal investigation, it must be referred to the AFP in accordance with the AFP referral process (see www.afp.gov.au), except where:

a. the entity has the capacity and appropriate skills and resources needed to investigate serious crime or conduct complex criminal investigations and meet the requirements of the Commonwealth Director of Public Prosecutions in gathering evidence and preparing briefs of evidence, or

b. where the issue involves alleged breaches of the *Commonwealth Electoral Act 1918*.

6. Where another entity has legislative investigative powers (eg Comcare and ASIO), that entity may have primacy in determining which type of investigation takes precedence.

7. Where a suspected Commonwealth criminal offence is not or cannot be referred to the AFP for investigation (see AFP website), or requires initial investigation prior to establishing a need to refer to the AFP, entities may need to conduct an investigation for matters such as suspected fraud, theft and unauthorised disclosure of official information. To the extent possible when investigating a suspected Commonwealth criminal or a matter that may result in a criminal investigation, entities are encouraged to consider the rules of evidence.

8. The rules of evidence cover:

a. admissibility of evidence: whether or not the evidence can be used in court

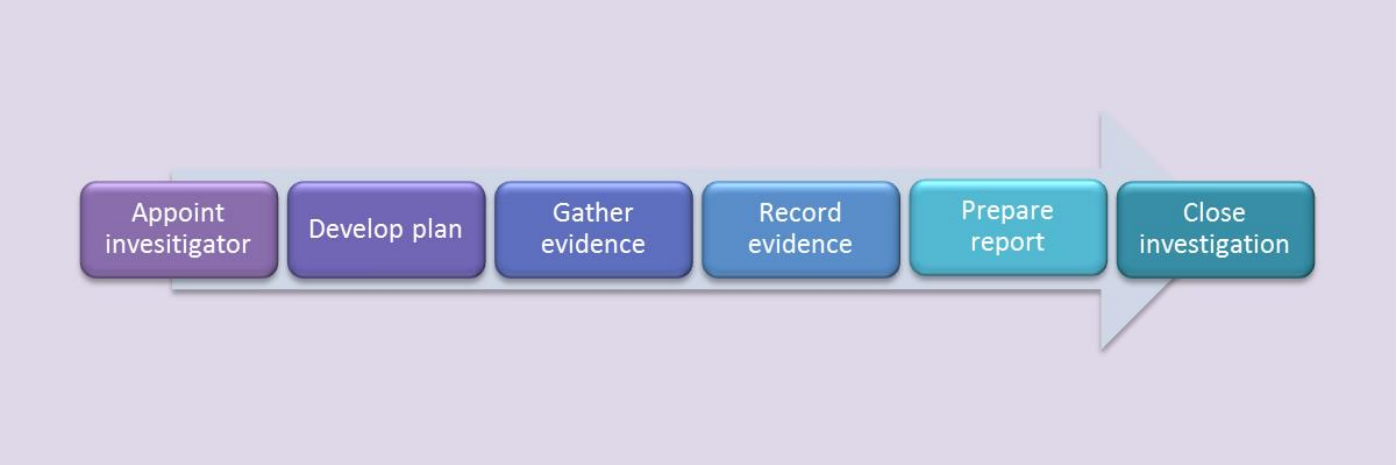
b. weight of evidence: the quality and completeness of the evidence.

9. For guidance on obtaining, recording and storing evidence in accordance with the rules of evidence, refer to the Australian Government Investigations Standards (AGIS).

10. For further guidance on integrity of evidence for cyber investigations, refer to the ISM's Guidelines for cyber incidents.

11. The Commonwealth Fraud Control Framework sets out procedures for investigating actual or suspected fraud against the Commonwealth.

Annex B Figure 1 Security investigation process



12. A security investigation establishes the facts:

a. who, what, why, when, where and how

b. the nature of the incident and how it occurred

c. the circumstances that led to the incident occurring

d. the person/s involved

e. the degree of damage to security interests, government people, information or assets

f. procedural or system improvements needed to prevent or reduce the likelihood of recurrence.

Step 1: Appoint investigator

13. In the interests of procedural fairness, it is important that the investigator be impartial and not have an actual or apparent conflict of interest in the matter being investigated.

14. Entities are strongly encouraged to provide relevant and appropriate training for investigators, as determined by the entity. The AGIS provides guidance on recommended training or qualifications for investigators. Where insufficient power to collect available or required evidence is identified, or if a conflict of interest is identified, the investigator is encouraged to refer the investigation to another person or entity with the necessary powers.

15. An investigator's key responsibilities include:

a. understanding the incident being investigated and the terms of reference

b. identifying the relevant law, policy or procedures that apply

c. making sufficient inquiries to ascertain all relevant facts

d. ascertaining whether an offence or incident has occurred based on the relevant facts

e. reporting the findings, identifying the reasons for the findings

f. making relevant recommendations.

16. Investigators assess:

a. applicable legislation that may determine the nature of and set the framework for the investigation

b. the nature of the incident

c. how serious the incident is and therefore the possible level of harm it has for the entity, or more widely, for government

d. whether the incident indicates the existence of a systemic problem

e. whether it is part of a pattern of conduct

f. whether it may breach any Australian law, especially any criminal provision.

Step 2: Develop an investigation plan

17. The investigation plan identifies:

a. the issues to be investigated

b. any relevant legislation, particular provisions of a code of conduct, entity policy and procedures, particular standards and guidelines

c. required evidence

d. methods and avenues to collect the evidence

e. legal requirements and procedures to be followed in collecting evidence

f. the allocation of tasks, resources and timings

g. arrangements in case the terms of reference or investigation plan need to be modified during the investigation.

Terms of reference for security investigations

18. The Department of Home Affairs recommends that the CSO approve the terms of reference, objectives and limits for all security investigations, and is encouraged to seek regular reports on investigation progress. The terms of reference could include:

a. the background

b. resources allocated (people, finances etc)

c. timeframes

d. types of inquiries to be conducted

e. extent and limit of powers of the investigating officer (consistent with relevant Commonwealth and jurisdictional legislation) during the investigation to collect evidence by:

f. obtaining information from people about policies, procedures and practices

g. accessing relevant records and other material

h. interviewing witnesses and suspects

i. search and surveillance

j. the format of progress reporting and the final report

k. any special requirements or factors specific to the investigation.

Step 3: Gather evidence

19. The 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:

a. physical

b. documentary (records)

c. verbal (recollections)

d. expert (technical advice).

20. Evidence gathered in a security investigation may not comply with the rules of evidence and therefore may not be satisfactory in a criminal investigation, or where legal proceedings might arise in relation to the incident. For guidance on obtaining, recording and storing evidence, refer to the AGIS.

Step 4: Record and store evidence

21. The Department of Home Affairs recommends investigators maintain a separate file for each investigation. This 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. Investigators are encouraged to store this file and any physical evidence securely to prevent unauthorised access, damage or alteration. This is to maintain confidentiality and ensure continuity of evidence. It is important that the record includes the handling of physical evidence and any tampering with the file or physical evidence.

Step 5: Prepare the investigation report

22. At the conclusion of the investigation, the investigator produces a findings report to the CSO, CISO, commissioning body (eg security governance committee) or the decision-maker. The report includes reasons for the findings according to the terms of reference using supporting material, and recommendations that could include:

a. disciplinary action

b. dismissal of a disciplinary charge following a constituted hearing

c. referral of a matter to an external entity for further investigation or prosecution, and

d. changes to administrative or security policies, procedures or practices.

Standard of proof

23. In drawing conclusions regarding 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’.

Step 6: Close the investigation

24. The investigation is considered 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.