5 Reporting on security

A. Purpose

1. This policy details the information entities are required to report under the Protective Security Policy Framework (PSPF) to provide assurance about their implementation of sound and responsible protective security practices and to identify security risks and vulnerabilities and the steps being taken to mitigate them. The policy describes how entities assess the maturity of their security capability, including by considering the entity's:
    a. progress in achieving the PSPF governance, information, personnel and physical security outcomes
    b. level of implementation and management of the PSPF core and supporting requirements
    c. risk environment and tolerance for security risks
    d. strategies and timeframes to manage identified and unmitigated risks, and
    e. security risks to people, information and assets.

B. Requirements

B.1 Core requirement

Each entity must report on security:

a. each financial year to its portfolio minister and the Attorney-General's Department addressing:
i. whether the entity achieved security outcomes through effectively implementing and managing requirements under the PSPF
ii. the maturity of the entity's security capability
iii. key security risks to the entity's people, information and assets, and
iv. details of measures taken to mitigate or otherwise manage identified security risks
b. to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation
c. to the Australian Signals Directorate in relation to cyber security matters.

B.2 Supporting requirements

Supporting requirements for reporting on security

#	Supporting requirements
Requirement 1. PSPF reporting model and template	Each entity **must** submit a report on security each financial year: a. through the PSPF online reporting portal for information up to PROTECTED or b. by submitting an offline reporting template for information classified higher than PROTECTED.
Requirement 2. Reporting security incidents	Each entity **must** report any significant or reportable security incidents at the time they occur to: a. the Attorney-General's Department b. the relevant lead security authority c. other affected entities. Table 3 provides detailed guidance on reporting security incidents.

#	Supporting requirements
Requirement 3. ASD cyber security survey	Each entity **must** complete the Australian Signals Directorate's annual cyber security survey.

C. Guidance

2. All non-corporate Commonwealth entities must meet the core and supporting requirements in this policy, consistent with the requirement in section 21 of the *Public Governance, Performance and Accountability Act 2013* for the Accountable Authority of a non-corporate Commonwealth entity to govern the entity in a way that is 'not inconsistent with' the PSPF.
3. The Attorney-General's Department encourages corporate Commonwealth entities and Commonwealth companies that implement the PSPF to also report on security.

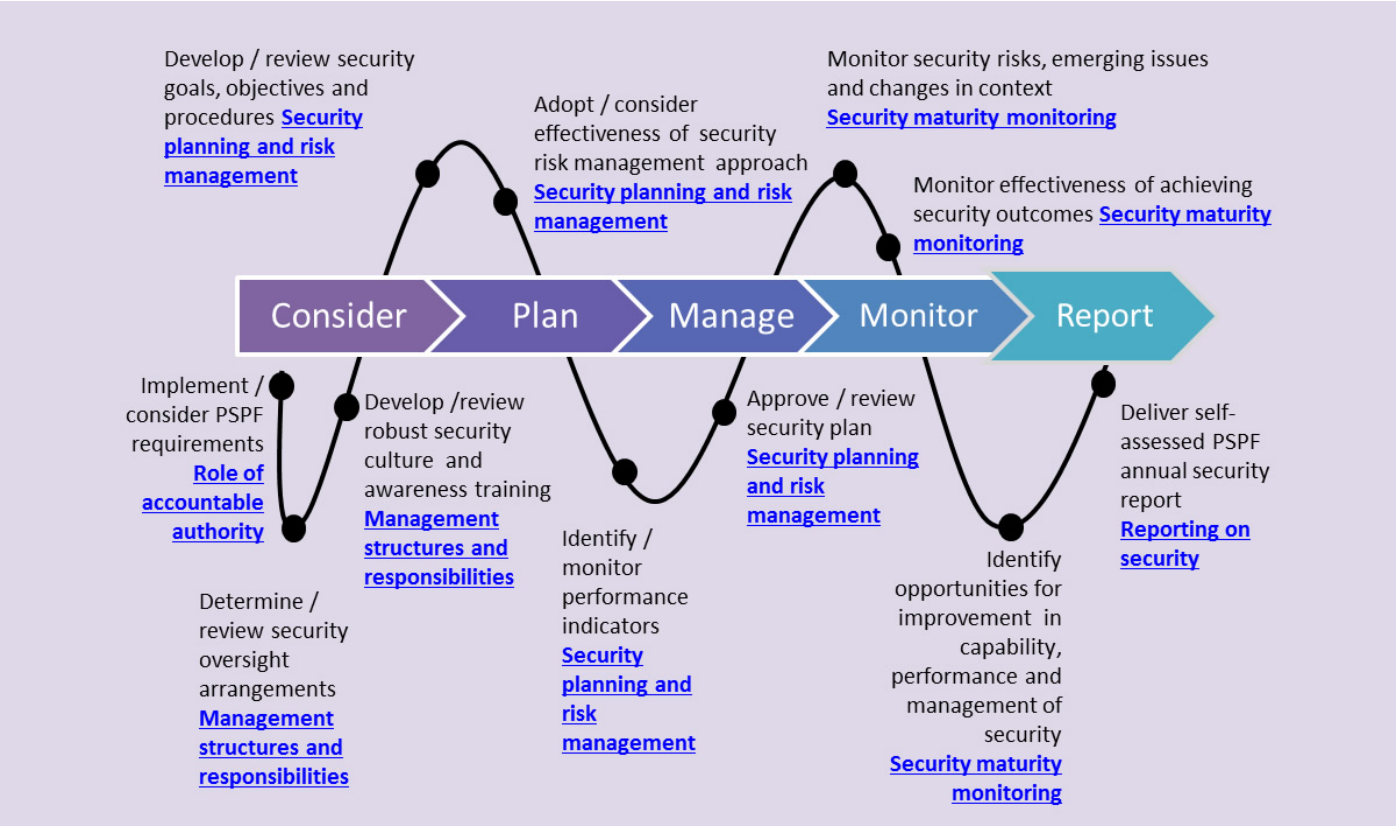
C.1 Reporting to the portfolio minister and the Attorney-General's Department

4. The core requirement mandates that an entity must report on security each financial year to its portfolio minister and to the Attorney-General's Department. An entity's annual security report summarises the maturity of its security capability and the level of implementation and management of the requirements under the PSPF.
5. The annual security report will show the extent to which an entity has:
    a. achieved the ***four protective security outcomes*** relating to security governance, information, personnel and physical security
    b. implemented the ***16 core requirements*** and the **supporting requirements** that entities **must** meet to achieve the four protective security outcomes.
    c. identified the ***key security risks*** relevant to the particular entity's people, information and assets, and
    d. implemented strategies and timeframes to **manage identified and unmitigated risks**.
6. The Attorney-General's Department provides an online reporting portal (for information classified up to PROTECTED) or a reporting template (for information classified higher than PROTECTED) to support entities to capture relevant information and meet all the elements of the core requirement. The portal and template are based on the PSPF Maturity Self-Assessment Model, which is provided at Annex A.
7. The Maturity Self-Assessment Model requires entities to assess their security capability against four levels of maturity—ad hoc, developing, managing and embedded—and provides a meaningful scale to support consideration of the entity's overall security position within its specific risk environment and risk tolerances. The Maturity Self-Assessment Model helps entities acknowledge successes and progress towards implementation; and aids decision-making by highlighting areas for improvement.
8. Under the Maturity Self-Assessment Model the maturity levels are:
    a. **ad hoc**: partial or basic implementation and management of PSPF core and supporting requirements
    b. **developing**: substantial, but not fully effective implementation and management of PSPF core and supporting requirements
    c. **managing**: complete and effective implementation and management of PSPF core and supporting requirements-this is the baseline maturity level for reporting entities
    d. **embedded**: comprehensive and effective implementation and proactive management of PSPF core and supporting requirements and excelling at implementation of better-practice guidance

C.1.1 Preparing for PSPF reporting

9. As detailed in PSPF policy: Security maturity monitoring, entities are required to regularly monitor and assess their security capability and risk culture by considering their progress against the goals and strategic objectives identified in the security plan. Information collected through security maturity monitoring can be used to inform the entity's annual security report. Figure 1 illustrates the possible information collection points that can be documented as an entity goes through the process of planning, managing and monitoring its path to security maturity.

Figure 1 Pathway to collect information on security maturity



C.1.2 Reporting on security outcomes and implementing and managing the requirements under the PSPF

10. The core requirement mandates that entities report on whether security outcomes have been achieved through effectively implementing and managing requirements under the PSPF.

11. There are four security outcomes:

    a. **Governance** – each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring: clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.

    b. **Information** (including ICT) – each entity maintains the confidentiality, integrity and availability of all official information.

    c. **Personnel** – each entity ensures its employees and contractors are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.

    d. **Physical** – each entity provides a safe and secure physical environment for their people, information and assets.

12. The outcomes are achieved by implementing the PSPF policies, each of which is comprised of core and supporting requirements. By considering the entity's effectiveness in implementing and managing the core and supporting requirements, in the context of its specific risk environment and risk tolerances, the entity can assess the maturity of its implementation of each policy. The maturity levels (ad hoc, developing, managing and embedded) for each policy are defined in the PSPF Maturity Self-Assessment Model at Annex A.

13. When reporting on the entity's effectiveness in implementing and managing requirements under the PSPF, entities are asked to evaluate the degree to which implementation achieves the minimum requirements set out in the PSPF. The degree of implementation can be described as:

    a. **Partial** – Requirement is not implemented, is partially progressed or is not well understood across the entity.

    b. **Substantial** – Requirement is largely implemented but may not be fully effective or integrated into business practices.

    c. **Full** – Requirement is fully implemented and effective and is integrated, as applicable, into business practices.

d. **Excelled** – Requirement and relevant better-practice guidance are proactively implemented in accordance with the entity's risk environment, are effective in mitigating security risk and are systematically integrated into business practices.

e. **Yes** or **No** – For a small number of requirements, it is not possible to evaluate the degree of implementation and entities can only state whether they have or have not implemented the requirement, for example, the requirement to submit the Australian Signals Directorate's annual cyber security survey.

14. For an entity to assess its implementation and management of the PSPF requirements as fully effective (managing maturity), the entity is expected to implement all of the core and supporting requirements or implement alternative protective security measures that provide the same (or exceed the level of) protection as the PSPF requirement and/or supporting requirements.

C.1.2.1 Strategies to mitigate and manage security risks

15. The core requirement mandates that entities provide details of measures taken to mitigate identified security risks. For each core requirement rated 'ad hoc' or 'developing', the PSPF reporting portal and template require entities to provide information on planned strategies and implementation activities to achieve maturity level 'managing'. Each strategy or activity requires an associated timeframe.

Table 1 Example PSPF annual reporting against PSPF policy: Safeguarding information from cyber threats

Core requirement	Safeguarding information from cyber threats
Maturity assessment	Developing
Maturity assessment rationale	Machinery of government changes temporarily affecting maturity level as the entity recalibrates ICT systems and management arrangements under the new department.
Strategies to address unmitigated risks and residual PSPF implementation	a. Identification of security advisor positions within three months of finalising machinery of government changes. b. SES security governance committee to be established to ensure appropriate security arrangements are factored into new departmental procedures. c. ICT system and management arrangements currently under review for update.
Timeframes to improve and achieve 'managing' maturity	a. December 2020 b. June 2021 c. September 2021

16. For information on risk mitigation and security risk management strategies, see the PSPF policy: Security planning and risk management.

C.1.3 Reporting on maturity of security capability

17. The core requirement mandates that the annual security report address the maturity of the entity's security capability. Assessing the maturity of the entity's security capability involves considering how holistically and effectively each entity:

    a. implements and meets the intent of the PSPF core and supporting requirements

    b. minimises harm and damage to government people, information and assets

    c. fosters a positive security culture

    d. responds to, and learns from, security incidents

    e. understands and manages their security risks

    f. achieves security outcomes while delivering business objectives.

18. While this assessment will reflect the entity's overall maturity level under the Maturity Self-Assessment Model, it allows entities to provide a more nuanced view of the entities strengths and weaknesses within that maturity level.

19. **Table 2** sets out the four maturity level indicators for security capability and the level of protection associated with each maturity level. The maturity indicators link to an entity's level of PSPF implementation and security performance within its risk environment.

Table 2 Maturity indicators for security capability and associated level of protection

Maturity level	Ad hoc 	Developing 	Managing 	Embedded 
Maturity level description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives high performance.
Maturity level indicators	Entity implementation and basic management of the PSPF core and supporting requirements is inconsistent and ad hoc.	Entity has implemented and managed the majority of the PSPF core and supporting requirements but not effectively. There is an established and documented pathway for remaining requirements to be implemented.	Entity has effectively implemented and is managing all PSPF core and supporting requirements. Security is considered part of the entity's business practices.	Entity has fully and effectively implemented all PSPF core and supporting requirements and integrated them into the entity's business. Security is proactively managed in response to the risk environment and better practice informs the entity's business and security decisions.
Maturity level protection	This category provides partial protection of the entity's people, information and assets, potentially exposing the government to unmitigated security risks.	This category provides substantial protection of the entity's people, information and assets, potentially exposing the government to security risks.	This category provides the minimum required protection of the entity's people, information and assets, consistent with policy requirements.	This category provides comprehensive protection of the entity's people, information and assets.

C.1.4 Reporting on security risk

C.1.4.1 Summary of security risk environment

20. An entity's security risk environment is the environment in which the entity operates and is determined after considering the threats, risks and vulnerabilities affecting the protection of the entity's people, information and assets including:
    a. what the entity needs to protect (via a risk assessment) being the people, information and assets assessed as critical to its ongoing operation and to the national interest
    b. what it needs to protect against (via the threat assessment and business model, for example face to face contact with the public, shared facilities)
    c. how the risk will be managed within the entity.
21. When determining their risk environment there are a number of security risk indicators an entity may consider, including:
    a. the sensitivity and security classification of information holdings, including consideration of aggregations of information and the classification of the entity's IT networks, see PSPF policy: Sensitive and classified information
    b. the type of information held and the impact level of compromise, eg aggregations of personal information
    c. the type of personnel (employees and contractors, security clearance holders or uncleared personnel) within the entity, see PSPF policy: Ongoing assessment of personnel
    d. categories of assets held by the entity, see PSPF policy: Physical security for entity resources
    e. the physical security zone levels defined in the entity's facilities, see PSPF policy: Entity facilities.

Examples of threats, vulnerabilities and risks

Threats:	Malicious action by trusted insider Malicious software attack (malware, ransomware, spyware) Cyber extortion (eg distributed denial of service attack) Abuse of privileged access control Exploited customer data through secondary targeting
Vulnerabilities:	Unpatched or uncontrolled portable devices Ineffectual security training or awareness Low resilience to natural disasters Poorly secured personal information Lack of ineffectual cyber security monitoring Ineffective service provider/third party contracts Aggregated data not managed Inadequate firewalls Poor security culture Weak security clearance management Incomplete application whitelisting
Risks:	Data breaches and spills Compromise of official/protectively marked information Incorrectly granting security clearance waiver Low resilience to natural disasters Poorly secured personal information Exploited customer data through secondary targeting

C.1.4.2 Key risks to people, information and assets

22. Identifying the key security risks affecting an entity provides an invaluable insight for entity and government decision-makers. Analysing this information may highlight:
    a. risks identified under any of the 16 PSPF policies
    b. systemic or emerging risks
    c. significant risks not sufficiently mitigated, or
    d. significant risks that have insufficient protective security policy coverage.
23. The Attorney-General's Department, as well as other lead security entities, uses information collected about key security risks to inform policy and develop strategies to mitigate security threats and vulnerabilities across government.
24. Changes in an entity's security risks may be influenced by factors including the security risk environment, operational priorities and security incidents. Entities may not have the same key security risks for consecutive years.
25. For guidance on security risk management, see PSPF policy: Security planning and risk management.

C.1.5 How to report

26. The core requirement mandates that entities submit their annual security report to the Attorney-General's Department and to the entity's portfolio minister. In accordance with supporting requirement 2, entities must use:
    a. the PSPF online reporting portal to complete and submit reports containing information classified as PROTECTED and below
    b. the PSPF offline reporting template to complete reports containing information classified higher than PROTECTED, which can be submitted by secure means appropriate for the security classification of the report.

C.1.5.1 PSPF online reporting portal

27. The PSPF reporting portal allows Commonwealth entities to complete and submit their annual security assessment online, access benchmarking reports at the conclusion of the submission period and access reports from previous reporting periods.

28. The PSPF reporting portal is accredited to process, store and communicate information up to PROTECTED.

29. At the start of the new assessment period, all CSOs will receive an email advising that the PSPF assessment for the entity is available for completion. The email will provide a link to login and indicate the due date for submission.

30. All CSOs must commence the assessment in the portal.

    a. For entities reporting information classified higher than PROTECTED, the PSPF online reporting portal will generate a downloadable offline reporting template. The offline reporting template is not saved in the PSPF reporting portal and can be transferred to an ICT system appropriate for the security classification of the report.

C.1.5.2 Completing the assessment

31. The annual security assessment is comprised of 17 modules—one for each of the 16 PSPF polices and a summary module.

Modules 1-16

The assessment contains a module for each of the 16 PSPF policies. Each of these modules has two parts:

Maturity questions

Each module consists of a set of questions drawn from the core and supporting requirements in the PSPF.

Rationale, strategies & timeframes

Based on the entity's answers to the maturity questions, the portal will suggest a maturity level for the module. This will be displayed on a chart that shows the distribution of the entities answers for the module.

The entity can confirm the suggested maturity level or select a higher or lower maturity level to reflect the entity's self-assessment.

There is a text box to enter a rationale for the selected maturity level. If the entity changed the suggested maturity level, the rationale should explain why the change is justified.

If the maturity level for the module is ad hoc or developing, there will be a set of text boxes to enter the proposed strategies and timeframes to improve the entities maturity level.

An entity may identify a core requirement as not applicable to the entity's business. Where there is an option to assess a core or supporting PSPF requirement as not applicable, the entity's security maturity will not be penalised. For example the PSPF policy: Security governance for international sharing may not be applicable where the entity is confident it does not access any information or assets governed by international agreements or arrangements to which Australia is a party. In this case marking not applicable will not affect the entity's maturity.

Summary Module

The summary module provides the entity's overall maturity rating, which is calculated based on the average of all the individual self-assessed maturity levels selected for each core requirement.

Separate to the overall maturity rating, a stand-alone entity maturity rating is calculated for each security outcome (ie governance, information, personnel and physical) based on the average of the applicable core requirements. Entities have the option of providing additional information to describe their maturity level for each outcome.

The summary module provides text boxes that must be completed:

- **Summary of risk environment**
- **Maturity of security capability**
- **Key risks to the entity's people, information and assets**

Within the summary module, the following information will be prefilled from answers provided in earlier modules or from elsewhere in the portal:

- Summary of significant security incidents during the reporting period (if applicable)—prefilled from the significant security incidents reported through the online reporting portal during the financial year. Where an entity identifies that a significant security incident has not been reported through the portal, the entity is required to add the incident to the summary module
- Exceptional circumstances (if applicable)—prefilled from Module 1 Role of the accountable authority
- Personnel security clearances and waivers—prefilled from Module 12 Eligibility and suitability of personnel and Module 13 Ongoing assessment of personnel

C.1.5.3 Approving the assessment

32. The entity's Accountable Authority is responsible for approving the report before it is submitted to the Attorney-General's Department and portfolio minister. This responsibility cannot be delegated.

33. The report cannot be approved in the portal. A copy of the final report can be downloaded for the Accountable Authority to approve offline. For entities using the offline template, instructions are included in the template.

C.1.5.4 Submitting the assessment

34. To meet the requirement to report to the entity's portfolio minister, the entity must provide the minister with the content of the summary module from the online PSPF reporting portal or offline reporting template. This content can be provided in the format of the report downloaded directly from the PSPF reporting portal or by copying and pasting the content into a format that meets the entity's standard procedures for communicating with their minister.

35. To meet the requirement to report to the Attorney-General's Department, the entity's CSO must finalise the assessment by completing the acknowledgement of reporting obligations to confirm that:

    a. the entity has reported to affected entities whose interests or security arrangements could be affected by the outcomes of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation. If not the entity has provided explanatory comments.

    b. the entity has submitted the ACSC Cyber Security Survey for Commonwealth entities. If not the entity has provided explanatory comments.

    c. the entity has reported to ASIO any significant security incidents or vulnerabilities relating to national security. If not the entity has provided explanatory comments.

    d. the assessment has been approved by the accountable authority—confirmation and date approved

    e. the assessment has been provided to the relevant portfolio minister—confirmation and date provided

36. The entity can provide additional comments at this stage, for example to advise if supplementary information needs to be provided separately because it is classified above PROTECTED.

37. The CSO is responsible for submitting the report to the Attorney-General's Department in the online portal or by secure means appropriate for the security classification of the report. This responsibility cannot be delegated.

C.2 Reporting to affected entities

38. The core requirement mandates entities report on security to all affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in the entity's PSPF implementation.

39. To fulfil this requirement, entities must report details of core and supporting requirements assessed, with ad-hoc or developing maturity that affect and expose other entities to unmitigated security risks. This includes security risks that affect national security, cyber security and shared service arrangements. Affected entities may include:

    a. lead security entities as set out in PSPF policy: Role of accountable authority, in particular:

        i. Australian Security Intelligence Organisation (ASIO) for national security risks

        ii. Australian Signals Directorate (ASD) for cyber security risks

    b. entities in shared service arrangements, for example entities such as co-tenants of premises or users of ICT infrastructure.

C.2.1 Reporting significant and reportable security incidents

40. Supporting requirement 2 mandates that entities report significant and reportable security incidents at the time they occur to:

    a. the Attorney-General's Department

    b. the relevant lead security authority

    c. other affected entities.

41. 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. A significant security incident can have wide-ranging and critical consequences for the entity and the Australian Government.

C.2.1.1 Reporting significant security incidents to the Attorney-General's Department

42. The Attorney-General's Department encourages entities to report significant security incidents to the Attorney-General's Department via the PSPF online reporting portal.

43. Information gathered on significant security incidents assists the Attorney-General's Department to:

    a. determine the adequacy of protective security policies

    b. provide an insight into entity security culture

    c. identify potential vulnerabilities in government security awareness training to inform whole-of-government security outreach activities.

C.2.1.2 Reporting security incidents to lead security authorities and other entities

44. Details of significant and reportable security incidents and the relevant authority to which entities report are provided in Table 3 and summarised below:

    a. **Significant national security-related incidents** — Australian Security Intelligence Organisation

    b. **Significant cyber security incidents** — Australian Signals Directorate

    c. **Security incidents involving Cabinet material** — Department of Prime Minister and Cabinet

    d. **Security incidents involving personnel with a security clearance** — Australian Government Security Vetting Agency (or entity CSO if the entity is an authorised vetting agency)

    e. **Contact reporting** — Australian Security Intelligence Organisation - Australian Government Contact Reporting Scheme

    f. **Correspondence of security concern** — Australian Security Intelligence Organisation

    g. **Security incidents or unmitigated security risk that affects the protection of another entity's people, information or assets** — accountable authority (or CSO) of the affected entity

    h. **Security incidents involving sensitive or classified equipment and services** — Security Construction and Equipment Committee

    i. **Security incidents involving foreign entity assets or information** — entity CSO. The incident may also need to be externally reported in line with other reportable incident categories.

45. In addition, some security incidents may be subject to other legislative or policy reporting requirements, for example:

    a. **Eligible data breaches** must be reported to the Office of the Australian Information Commissioner under the Notifiable Data Breaches Scheme

    b. **Potential criminal/serious incidents** must be reported to the Australian Federal Police (Commonwealth crimes) or local police (state and territory crimes)

    c. **Critical incidents involving public safety** must be reported to the Australian Government Crisis Coordination Centre.

46. Note: There may be other legislative requirements for reporting security incidents.

Table 3 - External security incident reporting or referral obligations (mandated under Requirement 2)

Reportable incident	Entity obligation to report	Reportable to
Significant security incidents	Advise the Attorney-General's Department of significant security incidents as they arise.	**Attorney-General's Department** PSPF Reporting Portal: https://portal.protectivesecurity.gov.au/ Email: PSPF@ag.gov.au Phone: 02 6141 3600 (PSPF Hotline)
National security incidents	Report security incidents or situations that have, or could have, an impact on national security, as defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), including suspected: a. espionage b. sabotage c. politically motivated violence d. promotion of communal violence e. attacks on Australia's defence system f. acts of foreign interference g. serious threats to Australia's territorial and border integrity. For security incidents that are reportable to ASIO, ASIO and the reporting entity will conduct an initial assessment of the potential harm. Dependent on the assessment, ASIO will either: recommend the entity continue with its own investigation and advise ASIO of the outcome, or conduct the investigation, in close consultation with the entity, and possibly in conjunction with the Australian Federal Police (AFP). Entities are encouraged to observe the need-to-know principle in relation to the details of a major security incident and its occurrence within an entity, until ASIO advises otherwise.	**Australian Security Intelligence Organisation** Email: asa@asio.gov.au Internet: http://www.asio.gov.au/ Phone: 132746 For advice on whether the incident needs to be reported, contact the National Security Hotline on **1800 123 400**.
Cyber security incidents	Report any cyber security incidents relating to: a. suspicious or seemingly targeted emails with attachments or links b. any compromise or corruption of information c. unauthorised access or intrusion into an ICT system d. any viruses e. any disruption or damage to services or equipment data spills f. theft or loss of electronic devices that have processed or stored Australian Government information g. denial of service attacks h. suspicious or unauthorised network activity. To avoid inadvertently compromising any investigation into a cyber security incident, entities are encouraged to contact the ACSC as early as possible. Refer to Australian Government Information Security Manual: a. ISM security control 0123 – Cyber security incidents are reported to an organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered. b. ISM security control 0141 – When organisations use outsourced information technology or cloud services, their service providers report all cyber security incidents to the organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered. c. ISM security control 0140 – Cyber security incidents are reported to the ACSC.	**Australian Cyber Security Centre in Australian Signals Directorate** Email: asd.assist@defence.gov.au Form to report: https://www.cyber.gov.au/report Phone: Cyber Security Hotline: **1300 CYBER 1 (1300 292 371)**

Reportable incident	Entity obligation to report	Reportable to
Cabinet material	Report security incidents (or suspected incidents) involving Cabinet material. Refer to the Cabinet Handbook for information on handling of Cabinet documents.	**Cabinet Division, Department of the Prime Minister and Cabinet** via entity Cabinet Liaison Officers.
Contact reporting	Under the **Australian Government Contact Reporting Scheme**, government personnel are required to report when a contact, either official or social, with a foreign national seems suspicious, persistent or unusual in any respect, or becomes ongoing. Such contact should be reported irrespective of whether it occurs within or outside Australia. Foreign nationals may include, but are not limited to, embassy or foreign government officials, including trade or business representatives. It is not necessary to report contact as part of official meetings provided a formal corporate record is produced detailing the topics discussed. However, employees should complete a contact report where a foreign national seeks to establish social contact outside official meetings, and/or where the contact seems suspicious, persistent or unusual. Additionally, personnel should report where a person or group, regardless of nationality, seeks to obtain information they do not need to know in order to do their job.	**Australian Security Intelligence Organisation** Email: cr@asio.gov.au
Incidents involving security clearance subjects	Report security incidents involving security clearance subjects. The entity is required to notify their vetting agency, at the appropriate time, of any security incident that may be relevant to a person's suitability to hold a security clearance. The appropriate time will depend on the significance of the incident, whether it is subject to investigation and an assessment of the related personnel security risks.	**Vetting agency** For clearances issued by the Australian Government Security Vetting Agency (AGSVA) Avenue to report: Security Officer Dashboard Phone: 1800 640 450
Correspondence of security concern	Report correspondence received that may be of a security concern, including but not limited to: a. threat to use violence to achieve a political objective b. warning of imminent threats to specific individuals, groups, property or buildings.	Entity security advisors (or CSO) to assess and determine the appropriate law enforcement or national security entity to externally report the incident.
Incident affecting another entity	Report any security incidents or unmitigated security risks that affect another entity's people, information or assets, particularly where entities are co-located or are providing services to another entity.	Advise the accountable authority of the entity whose people, information or assets may be affected. Refer to the Australian Government Directory
Classified equipment and services	Report any security incidents involving SCEC-endorsed safe hand courier services (using form). Report (via email to **SCEC@SCEC.gov.au)** any security incidents involving: a. SCEC-approved products faults or failure b. Destruction services - National Association for Information Destruction (NAID) AAA Certification with PSPF endorsement c. SCEC Security Zone Consultants and SCEC approved locksmiths.	**Security Construction and Equipment Committee** Report SCEC-endorsed safe hand courier services: https://www.scec.gov.au/scec-endorsed-courier-incidents Report other incidents types via email: scec@scec.gov.au

Reportable incident	Entity obligation to report	Reportable to
Unauthorised foreign entity access to classified Australian information or assets	Report any occurrences of Australian classified information and assets being shared with a foreign national or international entity without the protection of an appropriate agreement or arrangement. Refer to PSPF policy: Security governance for international sharing. International agreements or international arrangements may impose additional reporting and security violation handling requirements beyond those detailed in the PSPF.	Entity CSO to determine the appropriate channel to externally report the incident. CSO may also need to consider whether the incident requires reporting under another category in this table.
Compromise of foreign entity information or assets	Where a suspected security incident involves the compromise of information, or other resources, that originate from a foreign government or governments, entities must comply with the arrangements outlined in the agreement or arrangement under which the information was obtained. Where the foreign government information has been provided by another entity, inform the providing entity of the security incident as soon as possible. The providing entity may have obligations it needs to apply under an agreement or arrangement. Refer to PSPF policy: Security governance for international sharing.	Report the incident to the originating foreign government (or entity that provided the information) as soon as practicable, in accordance with the overarching agreement or arrangement.
Eligible data breaches	Report eligible data breaches, in accordance with the Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988*, to the OAIC. The scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'. The Commissioner must be notified as soon as practicable through a statement about the eligible data breach. When an entity is aware of reasonable grounds to believe an eligible data breach has occurred, it is also obligated to promptly notify any individual at likely risk of serious harm.	**Australian Information Commissioner** Form to report: https://www.oaic.gov.au/NDBform
Potential criminal/serious incidents	Report incidents that may constitute a criminal offence. See the AFP website for advice on the type of criminal incidents that are reported to the AFP (Commonwealth), or the local police (state or territory crimes), or if an incident is best handled within an entity. Examples of Commonwealth crimes (report to AFP): a. theft from the Commonwealth government b. assault on a Commonwealth official c. threats against a Commonwealth official. Examples of state and territory crimes (report to local police) a. cybercrime – including online fraud, such as eBay and internet scams b. stalking – including online stalking c. threats – including threats by phone, email, social networking sites, forums etc.	**AFP** for Commonwealth crimes Internet: https://www.afp.gov.au Phone: 02 6131 3000 **Local police** for state or territory crimes Phone: 13 14 44 **Crime Stoppers** to anonymously provide information about a crime Phone: 1800 333 000

Reportable incident	Entity obligation to report	Reportable to
Critical incidents involving public safety	**For critical incidents requiring immediate response, in particular where lives are at risk, call emergency services on triple zero (000).** Report any critical incidents that may affect public safety and require a coordinated response in support of the Australian Government and/or state and territory governments relating to: a. assault, including armed or military style assault b. arson, including suspected arson c. assassination, including suspected assassination d. bombing, including suspected use of explosive ordnance or improvised explosive devices e. chemical, biological or radiological attack, including suspected attacks f. attack on the National Information Infrastructure or critical infrastructure g. violent demonstration involving serious disruption of public order h. hijacking, including suspected hijacking i. hostage situation, including suspected hostage situation j. kidnapping, including suspected kidnapping k. mail bomb, including suspected mail bomb l. white powder incident, including real or significant hoax incidents.	**Australian Government Crisis Coordination Centre** Email: hotline@nationalsecurity.gov.au Internet: National Security Hotline Phone: 1800 123 400 The Crisis Coordination Centre will advise the AFP, ASIO, local police and/or other entities as appropriate.

47. To avoid inadvertently compromising an open security investigation entities are encouraged to contact the relevant lead security authority or affected entity as early as possible about the incident.

48. For further information on CSO's responsibilities in making decisions on investigating, responding to and reporting on security incidents, see PSPF policy: Management structures and responsibilities.

C.3 Reporting to the Australian Signals Directorate on cyber security matters

49. The core requirement mandates entities must report on cyber security matters to the Australian Signals Directorate each financial year. To meet this requirement, entities are required to complete the annual ACSC Cyber Security survey, distributed by the Australian Signals Directorate to all government entities, to assess their cyber security posture.

50. The PSPF assessment report summary module requests entities confirm submission of the annual cyber security survey to the Australian Signals Directorate**.** Where an entity has not completed the survey they are required to provide commentary.

C.4 Use of PSPF reporting data

51. The Attorney-General's Department consolidates all reporting entity's data into an aggregated annual security report for the Attorney-General and provides the report to reporting entities via the PSPF reporting portal.

52. At the conclusion of the annual PSPF reporting period the Attorney-General's Department will provide access to reporting data to the:

    a. Australian Signals Directorate

    b. Australian Security Intelligence Organisation

    c. Australian National Audit Office—in line with its responsibilities under the *Auditor-General Act 1997*.

D. Find out more

53. Additional information that may assist with reporting on security:

    a. ASIO T4 protective security guidance material (available for Australian Government entities on Govdex)

    b. *Australian Standard AS/NZS ISO 31000: Risk Management – Principles and guidelines*

    c. *Australian Standards HB 167: Security risk management*

    d. Commonwealth Risk Management Policy

    e. Australian Government *Information Security Manual*

    f. National Archives of Australia *Information Management Standard*

    g. National Archives of Australia *Digital Continuity 2020 policy*

    h. Essential Eight Maturity Model

    i. Office of the Australian Information Commissioner *Guide to Securing Personal Information*

    j. Office of the Australian Information Commissioner Data breach preparation and response – *A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*

    k. Office of the Australian Information Commissioner *Privacy (Australian Government Agencies-Governance) APP Code 2017*

D.1 Change log

Table 4 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	Apr 2020	Throughout	Updated core requirement Added three supporting requirements

	Updated guidance to reference the PSPF online reporting portal with details on the information requested and the steps required to complete the annual PSPF assessment report Added guidance on Use of the PSPF reporting data Minor changes to Annex A PSPF Maturity Self-Assessment Model in response to policy changes (Policies 5, 8, 9, 10, 11, 16)

Annex A. PSPF Maturity Self-Assessment Model

Security governance

Outcome: Each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring clear lines of accountability, sound planning, investigation and response, assurance and review processes and proportionate reporting.

Annex A. Table 1 PSPF Maturity Self-Assessment Model – Security governance

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Role of accountable authority	The accountable authority is partially aware of protective security requirements across the entity. Partial understanding, assessment and management of security risks to the entity's people, information and assets. Security is dealt with in an ad hoc manner.	The accountable authority substantially applies protective security requirements across the entity. Security risks and risk tolerances are identified and are substantially managed, monitored or reassessed on a regular basis. Security risk decisions and shared risks that affect other entities are substantially managed and communicated to affected entities.	The accountable authority consistently applies protective security policy across the entity, determines the entity's tolerance for security risks, promotes sound risk management processes and ensures appropriate governance arrangements are in place to protect the entity's people, information and assets. In medium to large entities, the management committee oversees and reviews risk profile and ensures underpinning procedures are consistent and adaptable to changes in the risk environment. Security risk decisions and shared risks that affect other entities are understood and communicated in a timely manner.	The accountable authority has an integrated, continuous-improvement approach to security management across the entity. Security risk management is a significant priority for the entity and is identified and aligned to business objectives. The entity identifies and operates within agreed and defendable risk tolerances that actively inform business decisions. Formal risk management processes and initiatives to connect security risk management and operations are in place. The entity promotes inter-entity collaboration to improve management of security risk decisions and shared risks that affect other entities. Where appropriate, the entity provides best-practice advice to other entities in its area of expertise.

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Management structures and responsibilities	Security management structures and responsibilities are partially in place. Responsibility for designated security roles, protective security planning and management of security practices are ad hoc. Incident reporting is by exception with partial staff awareness of obligations. Incident response processes are informal and not centrally managed. Security is partially prioritised by leadership with partial employee and contractor awareness.	The CSO is appointed and key security responsibilities are substantially assigned. Security risk and incident reporting is occurring across the entity and response processes are centrally managed in the majority of cases. The importance of security and developing a strong security culture is substantially recognised by the leadership. The majority of personnel attend periodic security awareness and skills development training.	The CSO is empowered to investigate, respond to and report on security incidents. Clearly defined security roles and responsibilities exist with skilled personnel appointed by the CSO and empowered to make security decisions for their entity. A governance oversight function is established (where appropriate to entity size). Entity's cycle of action, evaluation and learning is evident in response to security incidents. Personnel are knowledgeable of security incident reporting obligations with reporting processes published and accessible. Security is integral to the entity's business and informs decision-making. Leadership is actively engaged and visibly prioritises good security practices with a strong security culture evident within the entity. Personnel's attendance and understanding of regular education programs that inform and assist their understanding of security-related processes and obligations is monitored.	Role of the CSO is highly visible and central to delivering on strategic business priorities and objectives. A security governance oversight function is operational. Security is fully integrated into entity operations, actively managed, monitored and drives improvements. Security procedures and practices are robust and of proven effectiveness. The CSO ensures personnel resources are deployed to support the maintenance of effective protective security; appointing skilled personnel according to business needs. Comprehensive approach to managing security incidents including investigating to determine root causes and inform security improvements and education programs. All personnel are trained annually on security policy and procedures and take responsibility for implementation within their area of responsibility. Security culture is underpinned by continuous improvement and accountability.

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Security planning	Security planning is ad hoc. The security plan is partially developed and implemented but may not be current or comprehensive.	A security plan is endorsed, captures entity's goals and strategic objectives, key threats, risks, vulnerabilities and details of security risk tolerances and risk mitigation strategies. The plan is consistently applied across the entity in the majority of instances.	A security plan is endorsed by accountable authority and captures entity's goals and strategic objectives, key threats, risks, vulnerabilities and details of security risk tolerances and risk mitigation strategies. The plan is regularly reviewed and informs entity's decision-making. The plan is used to determine the security objectives and clearly supports the broader business goals. The security plan is communicated and accessible across the entity.	The security plan is comprehensive in identifying goals, strategic objectives, key threats, risks, vulnerabilities, risk tolerances and risk mitigations. The security plan influences executive management decision-making and planning. The entity continuously adapts the security plan in response to emerging or changing risks and threat levels.
Security maturity monitoring	The entity partially monitors security maturity performance of its security capability and risk culture against the goals and strategic objectives identified in the entity security plan.	Security capability and risk culture is addressed in the security plan. The performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly.	Consistent and defined approach to monitoring the entity's security performance, which is tailored to the entity's risk environment. The entity has clearly defined security goals and objectives in the security plan. Performance is tracked and measured to assess security capability and risk culture maturity.	The entity proactively engages in ongoing monitoring and improvement of security capability and culture through long-term planning to predict and prepare for security challenges. Performance data is captured analysed and informs change.

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Reporting on security	The entity has partially met external reporting obligations to its portfolio minister, AGD, other affected entities and ASD on cyber security matters. Reporting on the entity's achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies to manage identified risks is partial and ad hoc.	The entity substantially meets external reporting obligations to the portfolio minister, AGD, other affected entities and ASD on cyber security matters. The entity's achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies to manage identified risks is substantially captured in the annual security report.	The entity meets all external reporting obligations within required timeframes to the portfolio minister, AGD, other affected entities and ASD on cyber security matters. The entity meets these obligations through comprehensive reporting on achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies. Key findings and trends are shared within the entity.	The entity excels in meeting reporting obligations and uses annual reporting to drive improvements, strengthen security culture and inform future planning.
Security governance for contracted goods and service providers	Protective security provisions are partially included in goods and service provider contracts. The entity partially monitors service providers' adherence to contract provisions.	Appropriate security obligation clauses are included in the majority of provider contracts. The entity substantially applies processes to monitor service provider adherence to contract provisions.	Provider contracts contain explicit provisions to ensure implementation of relevant protective security requirements. The entity uses processes to monitor service providers' adherence to contract provisions and security obligations.	The entity actively monitors and audits service provider capability to fully implement contractual protective security requirements. Where appropriate, the entity supports contractors to achieve security outcomes.

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, effectively integrated and exceeding security outcomes. Entity's implementation of better-practice guidance drives achieving high performance.
Security governance for international sharing	The entity has access to foreign government information and assets and partially understands and implements handling and protection requirements agreed in international agreements and arrangements to which Australia is a party.	The entity has access to foreign government information and assets. There is substantial awareness, through training and accessibility of applicable agreements, of the level of handling protection requirements agreed in international agreements and arrangements to which Australia is a party.	The entity has access to foreign government information and assets and consistently applies handling protection requirements agreed in international agreements and arrangements to which Australia is a party. Alternatively, the entity is confident it does not access any information or assets that would be governed by international agreements or arrangements to which Australia is a party.	Where an entity has access to foreign government information and assets, it actively implements and monitors handling requirements agreed in international agreements and arrangements to which Australia is a party – and these are consistently applied. The entity proactively contributes to, and identifies, opportunities to evolve multilateral, bilateral agreements and arrangements to which Australia is a party on sharing and protection of information and assets.

Information security

Outcome: Each entity maintains the confidentiality, integrity and availability of all official information.

Annex A. Table 2 PSPF Maturity Self-Assessment Model – information security

	Ad hoc	Developing	Managing	Embedded
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Sensitive and classified information	The entity has a partial understanding of its information holdings. Procedures and operational controls to protect official government information assets proportional to their value, importance and sensitivity are ad hoc.	The entity knows the value of its information holdings and has established operational controls to ensure official government information is managed in accordance with minimum protections identified in the PSPF policy: Sensitive and classified information. The entity monitors and controls classified information holdings in the context of its risk environment.	The entity knows the value of its information holdings and operational controls are in place to ensure official government information asset holdings are consistently handled in accordance with minimum protections identified in the PSPF policy: Sensitive and classified information, proportional to their value, importance and sensitivity.	The entity culture actively supports the consistent and appropriate handling of official government information asset holdings in accordance with minimum protections identified in the PSPF policy: Sensitive and classified information. In a heightened risk environment, the entity closely monitors and controls classified information holdings.
Access to information	Information access controls and security procedures are partially in place. Supporting requirements on information sharing, access to sensitive and security classified information and controlling access to supporting ICT systems, networks, infrastructure, devices, applications and data holdings are partially applied.	Processes are substantially in place to enable appropriate sharing of information with relevant stakeholders who have a need-to-know and are appropriately security cleared. Access controls are substantially implemented to limit unauthorised access to supporting ICT systems, networks, infrastructure, devices, applications and data holdings in accordance with the information access control supporting requirements.	Information holdings are accessed and shared with appropriately security cleared personnel who have a need-to-know. Access controls support the integrity of ICT systems, networks, infrastructure, devices, applications and data holdings.	The entity proactively refines and reinforces information management processes and access controls to ensure protection of information and currency of systems to protect against emerging threats and issues. Information is shared with appropriately security cleared personnel who have a need-to-know. Systems are in place to detect, monitor and respond to irregular access to information or ICT systems, networks, infrastructure, devices and applications in real-time.

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Safeguarding from cyber threats	Partial implementation of Top 4 strategies to mitigate targeted cyber intrusions. Reactive approach to implementing the remaining Strategies to Mitigate Cyber Security Incidents to protect the entity.	The entity has implemented the majority of the Top 4 strategies to mitigate targeted cyber intrusions. The entity understands and has substantially implemented the remaining Strategies to Mitigate Cyber Security Incidents it considers necessary to protect the entity.	All Top 4 strategies to mitigate targeted cyber intrusions have been fully implemented with ongoing performance monitoring. The entity understands and has implemented the remaining Strategies to Mitigate Cyber Security Incidents it considers necessary to protect the entity.	The entity has fully implemented the Essential Eight, and other activities relevant to the entity's risk environment, to protect against harm from identified cyber threats. Processes are regularly tested to ensure real-time response to potential cyber intrusions and emerging threats.
Robust ICT systems	Partial security measures are in place for ICT system development. Management of ICT systems certification and accreditation (or assessment and authorisation) is ad hoc and partially implemented in accordance with relevant Information Security Manual technical standards when operationalised.	Security measures are substantially in place for ICT system development. Certification and accreditation (or assessment and authorisation) of ICT systems is in accordance with ISM technical standards in the majority of cases managed when operationalised.	Security measures are applied during all stages of ICT system development. ICT systems are certified and accredited (or assessed and authorised) in accordance with ISM technical standards when operationalised.	ICT security measures, including ICT systems certification and accreditation (or assessment and authorisation) are in accordance with the ISM technical standards. The entity excels in proactively exploring opportunities to further improve ICT security protections in response to ICT security threats.

Personnel security

Outcome: Each entity ensures its employees (and contractors) are suitable to access Australian Government resources and meet an appropriate standard of integrity and honesty.

Table 3 PSPF Maturity Self-Assessment Model

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Eligibility and suitability	The entity partially has procedures and systems in place to ensure personnel are eligible and suitable to access Australian Government resources. Pre-employment screening is ad hoc and security vetting requirements (where relevant) are partially followed. Some risks associated with eligibility and suitability of personnel are managed.	The entity has developed the majority of the entity's procedures and systems to ensure that personnel are eligible and suitable to access Australian Government resources. Pre-employment screening practices are substantially in place and security vetting requirements (where relevant) mostly followed. The entity manages the majority of risks associated with eligibility and suitability of personnel.	Procedures and systems are in place to ensure that all personnel are eligible and suitable to access Australian Government resources. All pre-employment screening and security vetting (where relevant) requirements are followed. These procedures and systems mitigate risks identified in the entity's personnel security risk assessment.	The entity excels in implementing efficient and timely processes to ensure the eligibility and suitability of personnel to access Australian Government resources. All requirements are followed and the entity has comprehensive practices in place to proactively manage risks identified in its personnel security risk assessment.
Ongoing assessment of personnel	The entity partially assesses and manages ongoing suitability of its personnel. Information of security concern for ongoing suitability of personnel is assessed and shared on an ad hoc basis with relevant stakeholders. Some security clearance maintenance requirements (where relevant) are met.	The entity has substantially developed its procedures and systems to assess and manage ongoing suitability of its personnel. In the majority of cases, information of security concern for ongoing suitability of personnel is assessed and shared by the entity with relevant stakeholders. Procedures are mostly in place to ensure compliance with security clearance maintenance requirements (where relevant).	Procedures and systems are in place to ensure that the ongoing suitability of personnel is assessed and managed in accordance with the entity's personnel security risk assessment. The entity has established lines of communication and processes to ensure information of security concern is shared with stakeholders as appropriate. The entity has procedures in place to ensure compliance with all security clearance maintenance requirements (where relevant).	The entity is proactive in assessing and managing the suitability of personnel, including security clearance maintenance requirements (where relevant), to ensure integrity of the entity's core business. The entity has well established lines of communication and robust processes to ensure information of security concern for ongoing suitability of personnel is shared with stakeholders in a timely manner.

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Separating personnel	Partial ad hoc processes are in place to ensure that separating personnel have their access to Australian Government resources withdrawn and are informed of their ongoing security obligations.	Separating personnel, in the majority of cases, understand their ongoing security obligations and have their access to Australian Government resources withdrawn. Systems and processes are substantially developed to verify consistency of separating personnel practices across the entity.	The entity has in place systems and processes to ensure that all separating personnel understand their ongoing security obligations, particularly where they have had access to sensitive and security classified information and resources during their employment. Separating personnel have their access to Australian Government resources withdrawn within an appropriate timeframe.	The entity has proactively implemented systems and processes that are reviewed regularly for separating personnel. Access to Australian Government resources is withdrawn from personnel on separation. The entity ensures separating personnel are debriefed and provided a comprehensive understanding of their ongoing security obligations. Information of security concern about separating personnel is shared with relevant stakeholders, including internally, where appropriate. Risk assessments are undertaken, where appropriate.

Physical security

Outcome: Each entity provides a safe and secure physical environment for people, information and assets.

Annex A. Table 4 PSPF Maturity Self-Assessment Model – Physical security

	Ad hoc 	Developing 	Managing 	Embedded 
Description	**Partial:** Some PSPF core and supporting requirements are implemented although are not well understood across the entity. Security outcomes are not being achieved in some areas.	**Substantial:** The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. Entity is largely meeting security outcomes.	**Full:** All PSPF core and supporting requirements are implemented, integrated into business practices and effectively disseminated across the entity. Entity meets security outcomes.	**Excelled:** All PSPF core and supporting requirements are implemented, are effectively integrated and exceeding security outcomes with better-practice guidance achieving high performance.
Physical security for entity resources	The entity partially applies physical security requirements. This increases the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation.	The entity substantially has in place physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation. The majority of physical security measures are implemented according to the requirements.	The entity applies physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation in accordance with requirements. Risks to the compromise of resources are mitigated to a level consistent with entity risk tolerance levels, in accordance with the entity's security plan.	The entity applies physical security measures and better-practice guidance that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation, which improves the delivery of business. These measures are proportionate to the level of risk and are scalable to changes in the threat environment.
Entity facilities	The entity partially considers physical security in the early stages of planning, selecting, designing and modifying facilities. Facility certification, accreditation, documentation and review are partially in accordance with the PSPF and the applicable ASIO Technical Notes.	In the majority of cases the entity considers physical security when planning, selecting, designing and modifying facilities, substantially integrating physical security requirements into all facilities. Certification, accreditation, documentation and periodic review of the majority of facilities are in accordance with the PSPF and applicable ASIO Technical Notes.	Physical security requirements are integrated into all stages of planning and modifying facilities. Entity facilities are certified and accredited systematically, with appropriate documentation, and in accordance with the PSPF and applicable ASIO Technical Notes.	Physical security requirements are a key driver for selection, design or modification of entity facilities. The entity actively ensures systematic certification and accreditation, with appropriate documentation, of its facilities in accordance with the PSPF and applicable ASIO Technical Notes. Required physical security upgrades of facilities are implemented as a priority.