5 Reporting on security

A. Purpose

1. This policy details the information entities are required to report annually under the Protective Security Policy Framework (PSPF) which is assessment of the maturity of the entity's security capability. It includes 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.
2. Reporting provides assurance that sound and responsible protective security practices are occurring. It also identifies security risks and vulnerabilities and the steps being taken to mitigate them.

B. Requirements

B.1 Core requirement

Each entity must report on security each financial year to:

- ***a. its portfolio minister and the Attorney-General's Department on:***
  - ***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 risks to the entity's people, information and assets, and***
  - ***iv. details of measures taken to mitigate or otherwise manage identified security risks***
- ***b. 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. the Australian Signals Directorate in relation to cyber security matters.***

B.2 Supporting requirements

3. The Attorney-General's Department provides a reporting template that sets out the PSPF Maturity Self-Assessment Model as well as the specific data to be provided under this policy.
4. There are no supporting requirements for reporting on security.

C. Guidance

C.1 Annual security report

5. The core requirement mandates that each entity must report on security. Under the *Public Governance, Performance and Accountability Act 2013* this requirement applies to non-corporate Commonwealth

entities. The Attorney-General's Department encourages corporate Commonwealth entities that implement the PSPF to also report on security.

6. An entity's annual security report summarises the maturity level of its security capability and performance. The report also compiles data on how effective the entity is in managing protective security within the entity.
7. The Attorney-General's Department consolidates entity data into an aggregated annual security report for the Attorney-General and provides the report together with benchmarking information to entities.
8. As detailed in the PSPF policy: Security maturity monitoring, entities are required to regularly monitor the security capability and internal procedures and mechanisms within their risk environments.

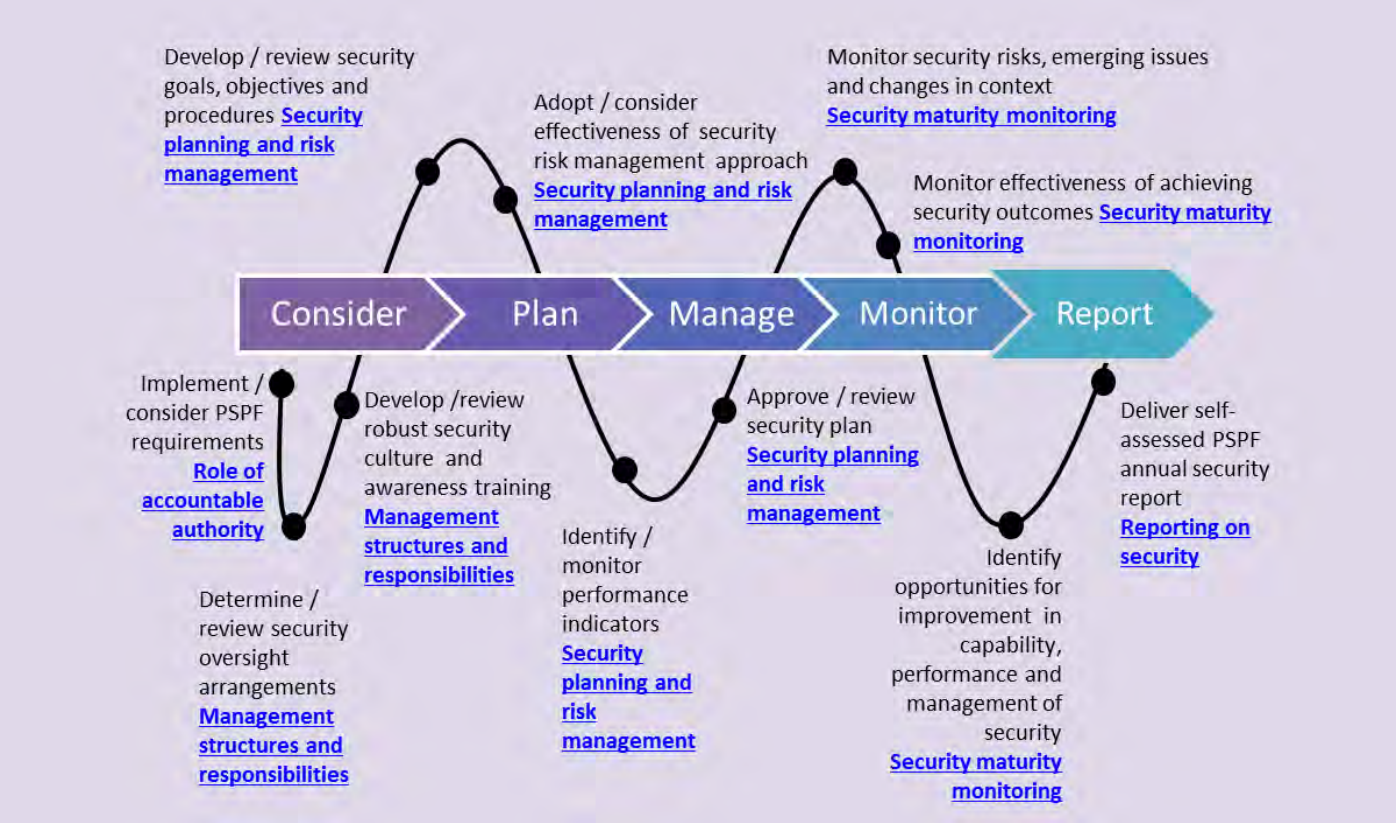
C.1.1 Reporting on security outcomes

9. As mandated in the core requirement, entities must report on whether security outcomes have been achieved through effectively implementing and managing requirements under the PSPF.
10. The four key security outcomes are:
    a. **Governance** – the entity manages security risks and promotes a positive security culture through clear lines of accountability, sound planning, security incident management, assurance and review processes and proportionate reporting.
    b. **Information** (including ICT) – the entity maintains the confidentiality, integrity and availability of official information.
    c. **Personnel** – the entity ensures its employees and contractors are suitable to access Australian Government resources and meet an appropriate standard of integrity.
    d. **Physical** – the entity provides a safe and secure physical environment for people, information and assets.
11. When reporting on the entity's effectiveness in implementing and managing requirements under the PSPF, entities are encouraged to evaluate the degree to which implementation successfully achieves the intent of the PSPF.

C.1.2 Reporting on maturity of security capability

12. Maturity provides a meaningful scale to assess an entity's overall security position within its specific risk environment and risk tolerances. Maturity acknowledges successes and progress towards implementation; and aids decision-making by highlighting areas for improvement.
13. Maturity of security capability considers 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.
14. Figure 1 illustrates the possible path an entity might take in achieving security maturity.

Figure 1 Possible path to security maturity



15. **Table 1** sets out the four maturity level indicators and protections for reporting entities to assess their PSPF maturity. The maturity level indicators link to an entity's level of PSPF implementation and security performance within its risk environment.

16. Under the PSPF Maturity Self-Assessment Model (see Annex A) the maturity levels equate to:

    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.

Table 1 PSPF Maturity Self-Assessment Model indicators and 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.1.3 Reporting on risks to people, information and assets

17. Identifying the security risks affecting an entity provides invaluable insight for entity and government decision-makers into risks that are:

    a. systemic or emerging

    b. not sufficiently mitigated, or

    c. that have insufficient protective security policy coverage.

    This evidence informs strategies to mitigate security threats and vulnerabilities across government.

Table 2 Examples of threats, vulnerabilities and risks

Threats	Vulnerabilities	Risks
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	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	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

18. 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.

19. For guidance on security risk management, see the PSPF policy: Security planning and risk management.

C.1.4 Reporting on mitigating and managing security risks

20. The core requirement mandates entities provide details of measures taken to mitigate identified security risks. The PSPF annual security report template seeks information on implementation activities for each core requirement rated 'ad hoc' or 'developing' to achieve maturity level 'managing'.

Table 3 Example PSPF annual reporting against PSPF policy: Safeguarding information from cyber threats

Core requirement	Maturity rating	Maturity rating rationale	Strategies and timeframes to address unmitigated risks and residual PSPF implementation
Safeguarding information from cyber threats	Developing	Maturity level reduced to 'developing' (from 'managing'). Machinery of government changes temporarily affecting maturity level as the entity recalibrates ICT systems and management arrangements under new department.	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 expected to be resolved by next financial year.

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

C.2 How to report – reporting template

22. The PSPF annual security report template guides entities through annual security reporting obligations. The template seeks:

    a. self-assessed maturity ratings for each core requirement and a rationale for the rating

    b. proposed future activities and timeframes to improve maturity and address identified risks (required for 'ad hoc' or 'developing' ratings)

    c. a summary of entity risk environments and security capability

    d. details of an entity's key security risks, including those identified for each security outcome (governance, information (including ICT), personnel and physical) as well as the mitigations used to address identified risks

    e. details of exceptional circumstances affecting implementation of the PSPF (see the PSPF policy: Role of accountable authority and remedial action taken to reduce the risk)

    f. security clearance level, type and number of each type of active security clearances waivers (see the PSPF policy: Eligibility and suitability of personnel)

    g. a summary of significant security incidents during the reporting period (see the PSPF policy: Management structures and responsibilities)

    h. confirmation that an entity has submitted the Australian Signals Directorate (ASD) annual survey.

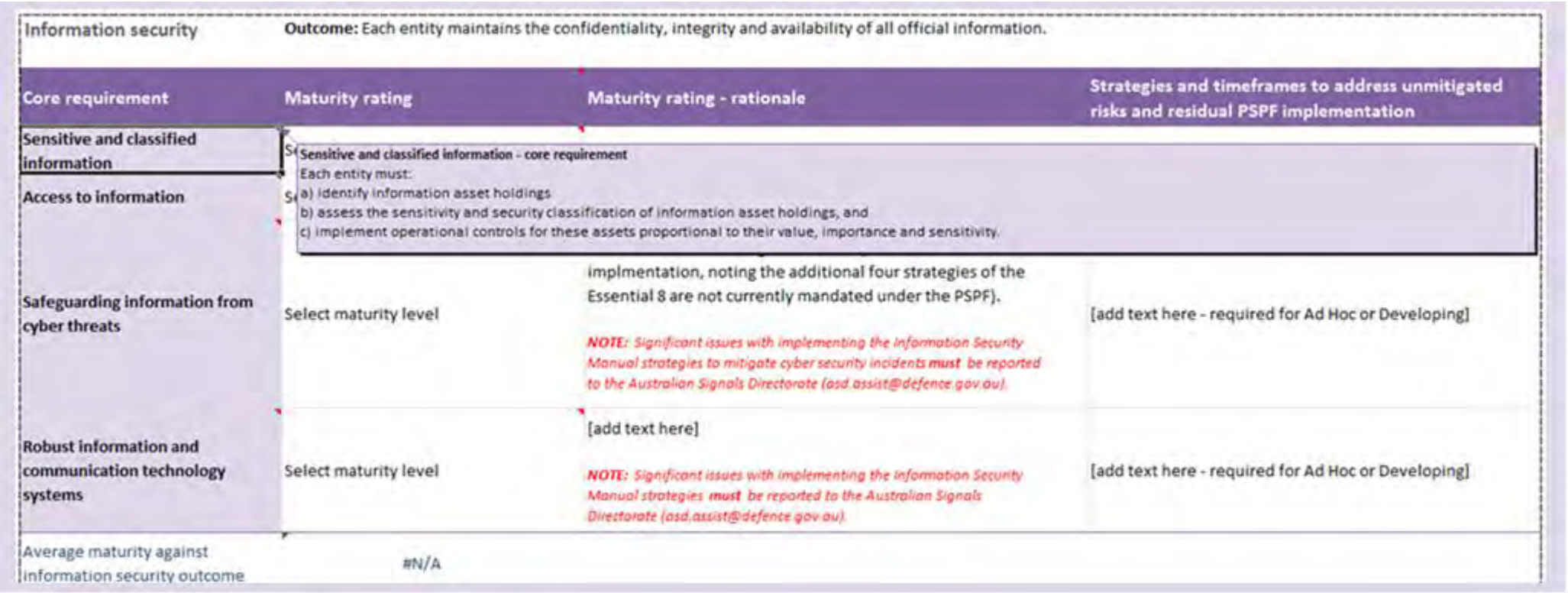
23. An entity may identify a core requirement as not applicable to the entity's business. Where a core PSPF requirement is not applicable, the entity may maintain a managing maturity level for that requirement and their overall security maturity will not be penalised. For example the PSPF policy: Security 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 the entity is to report a managing maturity level.

24. An entity's overall maturity rating is automated, 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.

25. Guidance and information is provided in the template and is accessed by moving the cursor over any cell with a red triangle in the top right-hand corner. See examples below.

Figure 2 Example reporting on PSPF policy: Sensitive and classified information



Information security	**Outcome:** Each entity maintains the confidentiality, integrity and availability of all official information.		
Core requirement	**Maturity rating**	**Maturity rating - rationale**	**Strategies and timeframes to address unmitigated risks and residual PSPF implementation**
Sensitive and classified information	S	**Sensitive and classified information - core requirement** Each entity must: a) identify information asset holdings b) assess the sensitivity and security classification of information asset holdings, and c) implement operational controls for these assets proportional to their value, importance and sensitivity.	
Access to information	S		
Safeguarding information from cyber threats	Select maturity level	implmentation, noting the additional four strategies of the Essential 8 are not currently mandated under the PSPF). ***NOTE:*** *Significant issues with implementing the Information Security Manual strategies to mitigate cyber security incidents* ***must*** *be reported to the Australian Signals Directorate (asd.assist@defence.gov.au).*	[add text here - required for Ad Hoc or Developing]
Robust information and communication technology systems	Select maturity level	[add text here] ***NOTE:*** *Significant issues with implementing the Information Security Manual strategies* ***must*** *be reported to the Australian Signals Directorate (asd.assist@defence.gov.au).*	[add text here - required for Ad Hoc or Developing]
Average maturity against information security outcome	#N/A		

Figure 3 Example indicators for each of the four maturity levels – PSPF policy: Sensitive and classified information

26. Once the report is complete, the entity determines the appropriate classification of the report (see the PSPF policy: Sensitive and classified information) and lodges it with their portfolio minister and the Attorney-General's Department by 31 August annually and according to the requirements of Table 4.

Table 4 Lodgement requirements for annual security report

Report sensitivity or classification	Lodgement details	Lodgement contacts
OFFICIAL, OFFICIAL: Sensitive or PROTECTED	Email: PSPF@ag.gov.au Phone 02 6141 3600	**Applicable portfolio minister** **Secretary, Attorney-General's Department** 3-5 National Circuit Barton ACT 2600 PSPF@ag.gov.au **Affected entities** and reporting requirements– refer C.5 **Australian Signals Directorate** asd.assist@defence.gov.au **Australian Security Intelligence Organisation** asa@asio.gov.au **Other entities** as required.
SECRET	Email: nationalsecuritypolicy@ag.gov.au For safe hand procedures refer to PSPF policy: Sensitive and classified information	

C.3 Reporting to the minister

27. The core requirement mandates that an entity must report on security each financial year to their portfolio minister. To fulfil this requirement, entities provide Section1: *Entity details* and Section 2: *Entity self-assessed security maturity* of the PSPF annual security report to their portfolio minister.

C.4 Reporting to the Secretary, Attorney-General's Department

28. The core requirement mandates entities must report on security each financial year to the Secretary, Attorney-General's Department. To fulfil this requirement entities complete all sections of the PSPF annual security report to the Secretary, Attorney-General's Department

C.5 Reporting to affected entities

29. The core requirement mandates entities must report on security to affected entities whose interests or security arrangements may be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in any entity's PSPF implementation. To fulfil this requirement, entities must report details of core and supporting requirements assessed with ad-hoc and developing maturity that affect and expose other entities to unmitigated security risks. This includes security risks that affect national security and cyber security. Affected entities may include:

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

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

        ii. the Australian Signals Directorate (ASD) – cyber security risks

        iii. other entities in shared-services arrangements

    b. entities such as co-tenants of premises or users of ICT infrastructure.

30. Table 5 provides examples of reportable issues and the affected entity for reporting purposes.

Table 5 Specific reportable issues

Reportable issue	Affected entity
Significant issues with implementing the Information Security Manual strategies to mitigate cyber incidents or suspected cyber security incidents relating to: a. suspicious or seemingly targeted emails with attachments or links b. any compromise or corruption of information c. unauthorised hacking d. any viruses e. any disruption or damage to services or equipment f. data spills.	Director, Australian Signals Directorate[i] asd.assist@defence.gov.au
Security incidents or situations that: a. involve suspected: i. espionage ii. sabotage iii. acts of foreign interference iv. attacks on Australia's defence system v. politically motivated violence vi. promotion of communal violence vii. serious threats to Australia's territorial and border integrity b. may compromise security classified information: i. contact reporting ii. malicious insider activity.	Director-General, Australian Security Intelligence Organisation asa@asio.gov.au
Security incidents or unmitigated security risks that affect another entity's people, information or assets, particularly where entities are co-located or providing services to another entity.	Accountable authority of the entity whose people, information or assets may be affected (refer to the Australian Government Directory).

Table 5 notes:

[i] To avoid inadvertently compromising an investigation into a cyber security incident, entities are encouraged to contact ASD as early as possible.

31. For information on security incident reporting, see the PSPF policy: Management structures and responsibilities.

C.6 Reporting to the Australian Signals Directorate on cyber security matters

32. The core requirement mandates entities must report on cyber security matters to ASD each financial year. To meet this requirement, entities complete the annual survey distributed by ASD to all government entities to ascertain their cyber security posture.

33. The PSPF annual security report template requests entities confirm submission of the annual survey to ASD.

D. Find out more

34. 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 6 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy

Annex A. PSPF Maturity Self-Assessment Model

Security governance

1. **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 and other affected entities. 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 is partial and ad hoc.	The entity substantially meets external reporting obligations to the portfolio minister, AGD and other affected entities. 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 is substantially captured in the annual security report.	The entity meets all external reporting obligations within required timeframes to the portfolio minister, AGD and other affected entities 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

2. **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 asset 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 asset 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 asset 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 asset holdings.
Access to information	Information access controls and security procedures are partially in place. Standards on information sharing, access to sensitive and security classified information and controlling access to supporting ICT systems 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 and data holdings in accordance with the information access controls standards.	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 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 systems 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 emerging cyber intrusions and threats.	The entity has implemented the majority of the Top 4 strategies to mitigate targeted cyber intrusions and has developed a substantial understanding of emerging cyber intrusions and threats.	All Top 4 strategies to mitigate targeted cyber intrusions have been fully implemented with ongoing monitoring of performance. The entity's procedures and systems are sufficient to mitigate known cyber intrusions and emerging threats.	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 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 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 in accordance with ISM technical standards when operationalised.	ICT security measures, including ICT systems certification and accreditation 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

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

Annex A.Table 3 PSPF Maturity Self-Assessment Model – Personnel 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.
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 assesses and partially manages ongoing suitability of all personnel affecting. 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 all 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.

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

4. **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 ASIO Technical Notes.	The entity considers physical security when planning, selecting, designing and modifying facilities, in the majority of cases, with physical security requirements substantially integrated into all facilities. Certification, accreditation, documentation and periodic review of the majority of facilities are in accordance with ASIO Technical Notes.	Physical security requirements are integrated into all stages of planning and modifying facilities. Entity facilities are certified and accredited systematically and in accordance with ASIO Technical Notes with appropriate documentation.	Physical security requirements are a key driver for selection, design or modification of entity facilities. The entity actively ensures certification and accreditation of its facilities in accordance with ASIO Technical Notes is systematic with upgrades implemented as a priority.