Australian Government

PROTECTIVE SECURITY GUIDE

FOR CHIEF SECURITY OFFICERS

Contents

Foreword

The role of the Chief Security Officer (CSO) is the key to ensuring the secure delivery of Government business.

As a CSO, you are tasked with providing strategic oversight of protective security arrangements across your entity. You are responsible for fostering a culture where personnel have a high-degree of security awareness, reinforced through practices that embed security into entity operations.

This guide provides an overview of the CSO role and how to successfully implement the Protective Security Policy Framework (PSPF). Each section includes questions, and suggested reading, to help you consider how the desired protective security outcomes can be achieved in your entity.

The information provided complements, and should be read in conjunction with, the PSPF Securing government business: Protective security guidance for executives.

Understand the Protective Security Policy Framework

Effective protective security is fundamental to the continuous and secure delivery of government business.

The PSPF assists Australian Government entities to protect their people, information and assets, at home and overseas. It:

- outlines the fundamental security principles that apply to every area of security and guide decision-making
- details the four security outcomes, the desired end-state results the government aims to achieve
- specifies 16 policies with core requirements and a number of supporting requirements that describe the minimum level of security acceptable to Government, and
- requires entities to take a risk-based approach to protective security and apply proportionate security controls to manage security risks.

The PSPF allows entities to apply the requirements in a way that best suits their individual security objectives, threat environment, risk tolerance and security capability.

Security principles

1. Security is everyone's responsibility. Developing and fostering a positive security culture is critical to security outcomes.
2. Security enables the business of government. It supports the efficient and effective delivery of services.
3. Security measures applied proportionately protect entities' people, information and assets in line with their assessed risks.
4. Accountable authorities own the security risks of their entity and the entity's impact on shared risks.
5. A cycle of action, evaluation and learning is evident in response to security incidents.

Achieving security outcomes

As CSO, you must decide how your entity will achieve the PSPF's four security outcomes:

- **Security 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.
- **Information Security:** Each entity maintains the confidentiality, integrity and availability of all official information.
- **Personnel Security:** Each entity ensures its employees and contractors are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.
- **Physical Security:** Each entity provides a safe and secure physical environment for their people, information and assets.

Consideration must also be given to what, if any, additional controls are required to manage your entity's risks and ensure your entity's people, information and assets are safeguarded from harm or compromise.

The current PSPF requirements have been in place since October 2018, so many may have already been implemented in your entity.

Maintaining a mature security posture is a continuous undertaking for entities. As CSO, your role is to ensure that arrangements are in place to support ongoing review and monitoring of security capability and effective PSPF implementation so that your entity is best placed to meet and maintain a mature position.

Annual reporting on security maturity obligates you to reflect critically on how your security implementation is progressing.

policies

Role of accountable authority	9	Access to information
Management structures and responsibilities	10	Safeguarding information from cyber threats
Security planning and risk management	11	Robust ICT systems
Security maturity monitoring	12	Eligibility and suitability of personnel
Reporting on security	13	Ongoing assessment of personnel
Security governance for contracted goods and service providers	14	Separating personnel
Security governance for international sharing	15	Physical security for entity resources
Sensitive and classified information	16	Entity facilities

PSPF Snapshot

PURPOSE OF EACH OF THE 16 PSPF POLICIES

		PSPF POLICY	PURPOSE
GOVERNANCE	1	Role of accountable authority	Accountability for security and establishes consistent, efficient and effective protective security measures across government.
	2	Management structures and responsibilities	Appropriate management structures and responsibilities in determining how security decisions are made in accordance with security practices.
	3	Security planning and risk management	Effective security planning and embedding security into risk management practices.
	4	Security maturity monitoring	Monitoring and assessing the maturity of your entity's security capability and risk culture.
	5	Reporting on security	Annual reporting under the PSPF, including assessing the maturity of your entity's security capability.
	6	Security governance for contracted goods and service providers	Assessing and managing security risks that arise from procuring goods and services.
	7	Security governance for international sharing	Protections for valuable information and assets under international sharing agreements or arrangements to which Australia is a party.

PURPOSE OF EACH OF THE 16 PSPF POLICIES

	PSPF POLICY		PURPOSE
INFORMATION	8	Sensitive and classified information	Assessing the sensitivity or security classification of information and adopting marking, handling, storage and disposal arrangements that guard against information compromise.
	9	Access to information	Security protections that support your entity's provision of timely, reliable and appropriate access to official information.
	10	Safeguarding information from cyber threats	Strategies to mitigate common and emerging cyber threats.
	11	Robust ICT systems	Safeguarding information and communication technology systems to support the secure and continuous delivery of government business.
PERSONNEL	12	Eligibility and suitability of personnel	Pre-employment screening processes and standardised vetting practices to be undertaken when employing personnel and contractors.
	13	Ongoing assessment of personnel	Maintaining confidence in the ongoing suitability of your entity's personnel to access Australian Government resources, and manage the risk of malicious or unwitting insiders.
	14	Separating personnel	Processes to protect Australian Government people, information and assets when personnel permanently or temporarily leave their employment with your entity.
PHYSICAL	15	Physical security for entity resources	Physical protections required to safeguard people, information and assets (including ICT equipment) to minimise or remove security risk.
	16	Entity facilities	Applying a consistent and structured approach to building construction, security zoning and physical security control measures of your entity's facilities.

When can an entity deviate from a PSPF policy?

The PSPF recognises that there may be circumstances where an entity may need to deviate from implementing the PSPF requirements. Decisions to deviate from the PSPF should be made by either the Accountable Authority or CSO, and reasons recorded.

The Accountable Authority is the person or group of persons responsible for, and with control over, your entity's operations. This is set out in Section 12 of the Public Governance, Performance and Accountability Act 2013.

Implementing alternative mitigations

You can decide to implement an alternative mitigation from the PSPF requirement, providing it meets or exceeds the level of protection afforded by the PSPF requirement.

Exceptional circumstances

Where exceptional circumstances prevent or affect your entity's capability to implement or maintain a PSPF requirement, and an alternative mitigation is not available, you may apply, for a limited time, the 'exceptional circumstances' provision.

The decision to apply this provision requires a documented risk assessment, including details of the proposed variation, which is approved by your entity's Accountable Authority.

Using the 'exceptional circumstances' provision may affect your entity's reportable maturity level for the corresponding PSPF requirement for the assessment period.

Note: Decisions to use either of these deviations must be in your entity's annual security report.

Questions to consider

- Has your Accountable Authority determined your entity's tolerance for security risks?
- How mature is your entity in implementing all the PSPF core and supporting requirements?
- Do you have visibility of how these requirements (and any additional controls) are being implemented across the four PSPF security outcomes?
- Is there an established way of monitoring your entity's performance and implementation of strategies to manage identified and unmitigated risks?
- Is your entity currently employing an alternative mitigation or experiencing exceptional circumstances?
- Is it documented and being managed in accordance with PSPF policy?

Suggested reading:

www.protectivesecurity.gov.au

Securing government business: Protective security guidance for executives

PSPF on a page

PSPF policy 1: Role of accountable authority

PSPF policy 5: Reporting on security

Know your role and responsibilities

Chief Security Officers are the Australian Government's security custodians.

The CSO role is mandated by the PSPF and its overarching purpose is to:

- support the Accountable Authority by providing strategic oversight of protective security arrangements for your entity, and
- bring security together at a senior level, break down the silos that traditionally existed in security, and leverage the opportunities brought about by having a single person with a holistic view of security for your entity.

As a CSO, you are vital to embedding and fostering a positive security culture where all personnel working in your entity understand the value of good security principles and are able to put them into practice.

Your remit covers all four security outcomes: governance, information, personnel and physical.

The PSPF requires that you report directly to the Accountable Authority on security matters.

Your key responsibilities include:

- Implementing PSPF requirements and delivering security outcomes
- Setting the strategic direction for protective security planning and risk management
- Integrating security into your entity's risk and business processes
- Championing a positive security culture and implanting effective security awareness training
- Embedding efficient and effective security practices and procedures
- Prioritising appropriate staffing levels and resources to support delivery of security outcomes
- Managing security-related incidents and emergencies and establishing monitoring mechanisms within your entity
- Monitoring security performance to achieve required protections and maturity, and
- Overseeing preparation of your entity's annual security report.

Suggested reading:

www.protectivesecurity.gov.au

PSPF fact sheet—Role of the Chief Security Officer

PSPF policy 2: Management structures and responsibilities

Establish security governance arrangements

Implementing effective security governance arrangements will help you achieve the full scope of your CSO responsibilities and ensure the protection of your entity's people, information and assets.

Success is ultimately tied to the work of the collective—it cannot be achieved in isolation. You do not need to be an expert in each of the four security outcomes; rather, you need to employ oversight and sound judgement in making security-related decisions for your entity, drawing on the expertise of those within your entity (or other entities) to implement measures or strategies for each of the protective security policies. You will need to tailor your security arrangements to the scale and complexity of your entity and its risk environment.

Security oversight

Where it is not possible for you to directly oversee all areas of security due to the size, complexity or high-risk nature of your entity—particularly where other senior officers who are not in your direct line of reporting are performing security-related functions—you will need to determine governance arrangements.

Establishing and chairing a security governance committee is one way of achieving and maintaining the required level of protective security oversight and accountability for your entity. It is recommended that such committees meet on a regular basis to keep across arrangements, and promote regular communication on issues of protective security.

Regardless of the structure you implement, you still retain overarching responsibility.

Security advisors

You may wish to consider appointing security advisors to support the day-to-day delivery of protective security outputs and to perform specialist services.

If your entity is large, complex or carries high-risk, multiple advisors may be required to manage security-related functions.

Security advisors should be appropriately skilled, empowered and resourced to perform their designated functions. They should also have access to training and networking opportunities across government to maintain and upskill on new and emerging security issues.

What should your governance arrangements look like?

Your security governance arrangements should be commensurate with your entity's size, complexity and risk environment.

They should include establishing:

- appropriate arrangements to monitor security across your entity, and these are reviewed and updated regularly
- clear lines of reporting and accountability for all personnel performing security-related functions (including those who do not directly report to you), and
- where relevant, a security governance committee with you as the Chair, to achieve effective security oversight.

Your protective security governance arrangements should be approved by your Accountable Authority.

Questions to consider

Based on your entity's size, complexity and risk environment, consider:

- Can you achieve oversight of all four security outcomes directly or do you need support?
- How many security advisors do you need to support your role? Do they need to be specialists in particular fields?
- Does your entity need to establish a security governance committee to enable you to achieve overarching oversight of protective security?
- Are there clear reporting lines and accountability?
- Are you performing other functions for your entity?
- If so, do these conflict with achieving your security responsibilities?
- If your entity performs a security-related function for another entity, have you factored these into your entity's governance arrangements?

Suggested reading:

www.protectivesecurity.gov.au

PSPF policy 1: Role of accountable authority

PSPF policy 2: Management structures and responsibilities, including information on establishing a security governance committee.

Ensure effective security practices and procedures

Protective security practices and procedures underpin your entity's maturity in implementing the 16 PSPF policies and achieving all four security outcomes.

These are more likely to be effective when they are demonstrated by senior management, embedded into day-to-day operations, and are well understood by all personnel.

As detailed in PSPF policy: Management structures and responsibilities, you must have procedures to cover all elements of protective security consistent with relevant PSPF policies.

You need to consider your entity's security procedures to determine whether these are sufficient to ensure all personnel can apply protective security practices in a consistent and effective way—do personnel know how to access them, what they mean, and what their responsibilities are?

Your security procedures must ensure:

- all elements of the entity's security plan are achieved (see Manage security risks through planning section)
- security incidents are investigated, responded to, and reported, and
- relevant security policy or legislative obligations are met.

We suggest that you:

- develop these procedures in conjunction with your entity's other security and risk planning documents
- update them when significant changes in the risk environment occur
- put in place measures to monitor the effectiveness of procedures and security performance, and
- update your entity's annual security awareness training with relevant messaging about current procedures.

Security incidents

The procedures you put in place to manage security incidents and investigations in your entity will depend on your entity's scale, complexity and risk environment.

You may be able to oversee and manage security incidents with support from one or more security advisors. If your entity is large, complex or carries high-risk, you may need to establish arrangements whereby security incidents are triaged and escalated to you as they reach business impact level thresholds or key decision points.

When to investigate a security incident

Not all security incidents warrant investigation. You are required to determine when a security incident is serious or significant enough to commence an investigation. Investigating actual or suspected security incidents may be necessary to remediate an existing breach or vulnerability and mitigate the impact.

An investigation may provide you with valuable information for future risk reviews and assessments and assist with evaluating current security practices and procedures.

Who else needs to know about an incident?

You are obligated under the PSPF to report significant security incidents to the relevant authority, external entity or an affected entity.

We suggest you take particular note of incidents that are reportable to the Attorney-General's Department (AGD), Australian Federal Police, Australian Signals Directorate, Australian Security Intelligence Organisation, Office of the Australian Information Commissioner, and Department of the Prime Minister and Cabinet.

Significant security incidents, reportable to AGD, are also provided to Secretaries' Board—ensuring learnings from these incidents, and how risks are managed during these situations, are shared across government.

Keep in mind, if a suspected security incident involves the major compromise of official information or other resources that originate from, or are the responsibility of another entity, it is important to seek advice from the originating entity prior to instigating any investigation. The originating entity may have operational security requirements that need to be applied to remediation activities or an investigation. In some cases, it may be more appropriate that the originating or responsible entity carries out remediation work or an investigation.

Questions to consider

- Have you reviewed your entity's existing security practices and procedures? Are they effective in achieving the four security outcomes along with a mature protective security performance? Do you need to develop additional procedures?
- Are your security procedures accessible to all personnel? Can they be easily understood?
- Do your security procedures align with the security culture you aim to cultivate?
- Are your entity's security procedures consistent and complementary across the four security outcomes? For example, are your IT/cyber policies consistent with and complement your physical security procedures or your security awareness training materials?
- Do your security practices and procedures unnecessarily hinder your entity's business or productivity? Consider what changes might be made to improve efficiency without compromising security planning.
- Do you have procedures in place to manage information of security concern about your personnel, including information provided by your vetting agency?

- Do you have procedures in place to manage, and where necessary triage and escalate, security incidents and investigations? Do all your security-related personnel understand these procedures and know how to respond to incidents?
- Do you have escalation and reporting processes in place to manage significant security incidents and investigations?
- Have you considered how a security incident in your entity may affect another entity or more broadly, the Australian Government? Do your procedures address communicating with and jointly managing incidents that affect other entities?
- Do you know where to seek assistance with responding to specific types of risks? For example, contacting the Australian Cyber Security Centre for assistance with a denial of service attack.
- Are your security incidents mapped to a business impact level?

Suggested reading:

www.protectivesecurity.gov.au

PSPF fact sheet—Significant security incidents

PSPF policy 2: Management structures and responsibilities

PSPF policy 5: Reporting on security

Manage security risks through planning

Security planning is designing, implementing, monitoring, reviewing and continually improving practices for security risk management. Maintaining an accurate, tailored and up-to-date security plan is integral to your role as CSO.

The basic principles of a security risk-management approach are to:

- identify the risks
- apply relevant controls
- assess the residual risk, and
- accept the residual risk or determine that additional controls are necessary to bring the residual risk within the organisation's risk tolerance.

What is a security risk?

A security risk is something that could result in the compromise, loss, unavailability or damage to information or assets, or cause harm to people. Security risk is the effect of uncertainty on objectives and is often measured in terms of its likelihood and consequences.

The causes of a security risk may be inadvertent and generated by people, systems, processes, procedures; or could be the result of deliberate malicious and/or criminal activity (eg cyber-attack) or a natural disaster (eg destruction of property).

What is a shared security risk?

A shared security risk is one that extends beyond your entity to another entity, the community, industry, international partners, or other jurisdictions. These type of risks require high levels of cooperation between stakeholders to effectively understand and manage, particularly where there is no apparent owner for the shared risk, where shared risk is complex, or where the parties involved have differing risk tolerances. Even though your entity may need to share some security risks with another entity or party, you cannot transfer the responsibility for these risks entirely—your entity remains responsible for your security risks.

Where shared risks are identified, it is important to:

- develop clear roles and responsibilities for managing the shared risk

- set channels for sharing information
- agree arrangements for differing appetites for the same risk
- establish government arrangements for managing complex shared risk
- capture details of any shared risk in your entity's security plan.

The Commonwealth Risk Management Policy provides further information on understanding and managing shared risks.

Develop a security plan

The PSPF mandates that you have a security plan to manage your entity's security risks.

Developing the security plan allows you to review the degree of security risk that exists in different areas of your entity's operations and to take appropriate action to mitigate identified risks.

It must be reviewed at least every two years to determine the adequacy of existing measures and mitigation controls, and to respond to and manage significant shifts in your entity's risk, threat and operating environment.

The security plan (and subsequent revisions) must be approved by your Accountable Authority.

What if a single plan is not practicable?

Where a single security plan is not practicable for your entity due to its size or complexity, your Accountable Authority may approve a strategic-level overarching security plan that addresses the core requirements, supported by more detailed supporting security plans.

If you have more than one plan, you should make sure consideration is given to ensure relevant staff are aware of all security plans and that consideration is given to how the totality of plans contribute to managing your entity's security. This includes mechanisms to ensure any updates to security plans are considered holistically.

What should a security plan include?

Your entity's security plan is recommended to address:

- security goals and strategic objectives, including how security risk management intersects with and supports broader business objectives and priorities
- threats, risks and vulnerabilities that impact the protection of your entity's people, information and assets
- your entity's tolerance to security risks
- maturity of your entity's capability to manage security risks, and
- strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

Questions to consider

- Does your entity have an existing security plan? If so, have you reviewed it to confirm it is fit for purpose and details the security goals and strategic objectives of your entity, including the intersection of security with broader business objectives and priorities?
- Do you know when your security plan is due to be updated, noting it must be reviewed at least every two years?
- How regularly do you test your security plan with desktop and/or live exercises? How do you ensure learnings from these exercises are circulated and acted upon?
- Consider how your current maturity rates against the goals and strategic objectives outlined in your security plan. How can you ensure your maturity aligns with those objectives?
- Is your security plan scalable and adaptable to change?
- Does your entity share any security risks with another entity or party? If so, are the current arrangements effective in managing these risks and detailed in your security plan?

Suggested reading:

www.protectivesecurity.gov.au

PSPF policy 3: Security planning and risk management, including Table 2 which provides suggested coverage for a security plan

Commonwealth Risk Management Policy (also available on www.finance.gov.au)

Australian Standards (also available on https://www.standards.org.au/)

Cultivate a strong and positive security culture

Having a strong and positive security culture is a fundamental enabler of good government business.

Good security culture relies on visible endorsement and engagement from the top, along with support and re-enforcement at all levels of your entity's workforce.

By following the guidance within the PSPF, you will be working towards a security culture in which your security practices and procedures are embedded and well-understood throughout your entity.

Culture is difficult to precisely define—it is often easier to observe the absence of a positive security culture. Broadly, a culture consists of the values, behaviours and other characteristics common to the members of a particular group.

What does a positive security culture look like?

A strong and positive security culture is where all personnel are aware, capable, supported and active in managing security risks around them. It requires security to be fully embedded into your entity's prevailing culture.

You, supported by your security advisors, are responsible for providing security leadership and promoting a culture where personnel value, protect and use your entity's information and assets appropriately.

In addition to keeping your entity and its personnel safe, a strong and healthy security culture helps to increase internal and external trust, embed consistent positive behaviour and support personnel to engage productively with risk.

Who else is thinking about security culture?

We encourage you to talk with other entities, particularly those in your portfolio or entities that are similar in size or function, and share ideas, materials and lessons learnt.

For example, you could reach out to other CSOs to see what they have implemented to date. The CSO network has regular forums, and a number of CSOs have shared their experiences and security awareness materials.

Security awareness training

Security awareness training is an important element of fostering a positive security culture. It also supports the implementation of protective security across physical, information and personnel security policies, practices and procedures.

The PSPF requires that entities provide all personnel, including contractors, with security awareness training at engagement and annually thereafter. It further requires that personnel in specialist or high-risk positions receive additional training targeted to the scope and nature of the position.

The Protective Security Policy GovTEAMS community provides access to training materials, including security training awareness materials that entities have shared for Government use. To access this GovTEAMS community, email PSPF@ag.gov.au.

We also encourage you to talk with other entities, particularly those in your portfolio or entities that are similar in size or function, and share ideas, materials and lessons learnt.

Questions to consider

- How will you ensure you are fostering a positive security culture?
- How can security culture be visibly endorsed, promoted and supported throughout your entity?
- How can your security awareness training be reinforced with other initiatives, such as a security awareness week or collaborating with another entity?
- Do you need to cater for diverse learning styles to ensure your entity's personnel understand and are able to apply the training?
- Could you share your security training materials with other entities, especially those who may not have the resources to develop the same quality of materials?

Suggested reading:

Protective Security Policy GovTEAMS
https://users.govteams.gov.au/Community/1155

AGD's Cultural Transformation Strategy

Shared security resources and materials

Embed monitoring and review arrangements

Monitor security performance to achieve required protections, identify emerging risks, build security capability, mitigate unacceptable security risks, and improve security maturity.

Effective protective security is not a ‘set and forget’ proposition. You are required to monitor and assess the maturity of your entity’s security capability and risk culture. This includes your entity’s capability to actively respond to emerging threats and changes in its security environment, while maintaining the protection of your people, information and assets.

Security capability maturity

Security capability maturity refers to your entity’s security position in relation to its specific risk environment and risk tolerances. This includes considering your entity’s effectiveness in implementing the PSPF, as well as acknowledging areas for improvement. Effective protective security is a long term goal, and recognising the need for change and improvement is critical to the success of your entity’s arrangements for protective security.

Monitoring security maturity

Monitoring security maturity is an ongoing process and involves routine assessment of your entity’s security capability and risk culture against a set of indicators. It is recommended that you develop a security maturity monitoring plan as part of your overarching security plan.

Questions to consider

- Do you have a process for monitoring your entity's security maturity and performance throughout the year?
- Are you comfortable with the level of information you receive on your entity's security performance and maturity?
- How often is your entity's security performance and maturity reviewed to ensure the appropriate strategies and timeframes to achieve the goals and objectives are in your security plan?
- Do you have a clear vision of the security improvements your entity will achieve ahead of the next reporting period? Are the timeframes for areas of improvement being monitored?
- Have you agreed how often security monitoring advice will be provided to your Accountable Authority?

Suggested reading:

www.protectivesecurity.gov.au

PSPF policy 4: Security maturity monitoring – for detailed guidance on what a monitoring plan could include and the stages of an effective monitoring cycle.

Deliver mature security performance

The annual report on security reflects your entity's security maturity posture and details how it is addressing areas of vulnerability.

Each entity is required to report annually on security. You must oversee the preparation of your entity's annual security report.

Preparing accurate and transparent reporting enables you to develop a full picture of your entity's security maturity, while identifying opportunities for future development and improvement. Your report also contributes to informing government about protective security settings across all entities, including ongoing or emerging issues that are affecting protective security arrangements.

PSPF maturity self-assessment model

The PSPF maturity self-assessment model enables you to consider the elements of your entity's security capability, based on the overall security position within your specific risk environment and risk tolerances.

These elements include:

- achieving the four security outcomes
- implementing and managing the 16 PSPF policies
- considering security risks to people, information and assets
- assessing your risk environment and identifying key security risks, and
- implementing strategies and timeframes to manage security risks.

PSPF maturity levels

Ad hoc—partial or basic implementation and management of requirement. Requirement is not implemented, is partially progressed or is not well understood across the entity.

Developing—substantial but not fully effective implementation and management of requirement. Requirement is largely implemented but may not be fully effective or integrated into business practices.

Managing—complete and effective implementation and management of requirement. Requirement is fully implemented and is integrated, as applicable, into business practices. This is the baseline maturity level for each entity.

Embedded—comprehensive and effective implementation and proactive management of requirement. Entity is excelling at implementation of better-practice guidance to mitigate security risk and the requirement is systematically integrated into business practices.

Preparing for PSPF reporting

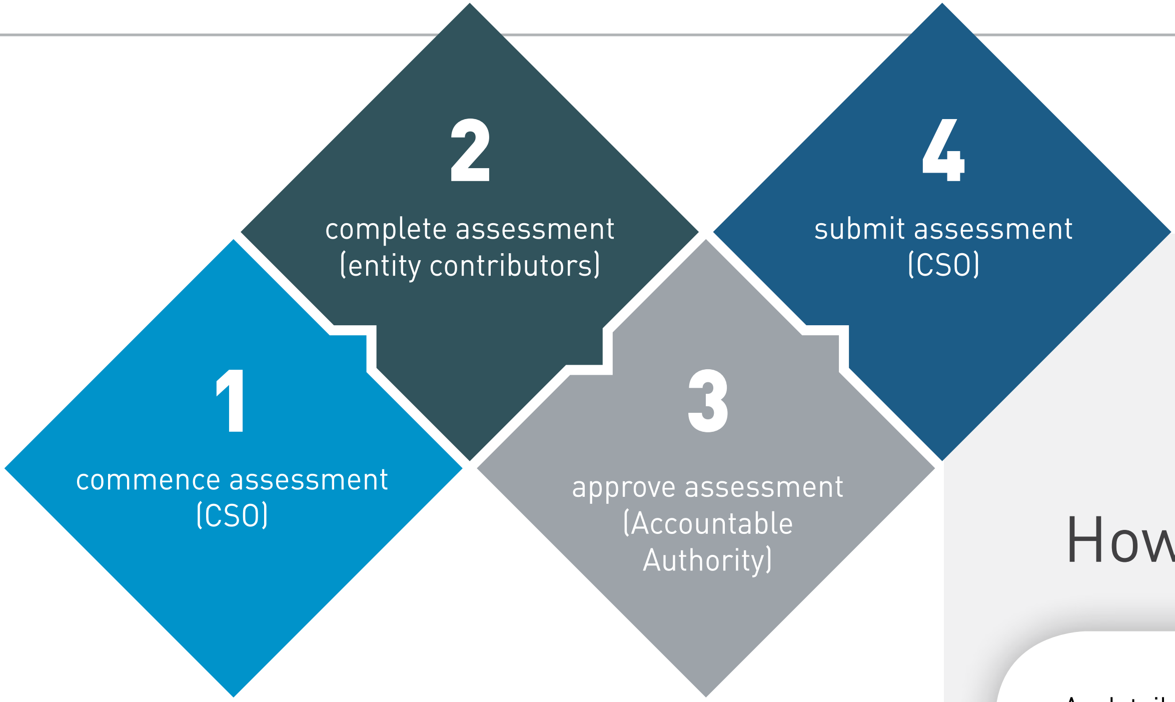
As detailed in PSPF policy: Security maturity monitoring, you are required to regularly monitor and assess your entity's security capability and risk culture by considering progress against the goals and strategic objectives identified in your security plan.

Information collected through security maturity monitoring can be used to inform your entity's annual security report.

Assessing the maturity of your entity's security capability involves considering how holistically and effectively your entity:

- implements and meets the intent of the PSPF core and supporting requirements
- minimises harm and damage to government people, information and assets
- fosters a positive security culture
- responds to, and learns from, security incidents
- understands and manages their security risks, and
- achieves security outcomes while delivering business objectives.

Reporting self-assessment steps



1 commence assessment (CSO)

2 complete assessment (entity contributors)

3 approve assessment (Accountable Authority)

4 submit assessment (CSO)

You can either assign step two—complete the assessment, to other users, such as your security advisors, or retain responsibility and complete it yourself.

The Accountable Authority must undertake step three—approve final assessment.

Suggested reading:

www.protectivesecurity.gov.au

PSPF policy 4: Security maturity monitoring

PSPF policy 5: Reporting on security

How to report

As detailed in PSPF policy: Reporting on security, you complete and submit your entity's annual security report via AGD's online PSPF reporting portal for reports classified up to PROTECTED or offline reporting template for reports classified SECRET or above.

Contact the PSPF team to gain access to the PSPF reporting portal.

Glossary

TERM	DEFINITION
Accountable Authority	As set out in Section 12 of the Public Governance, Performance and Accountability Act 2013 (Cth), each Commonwealth entity has an Accountable Authority. The person, or group of persons, prescribed by an Act or the rules of a listed Commonwealth entity is that entity's Accountable Authority.
Alternative mitigation	Adopting a different protective security measure or control that provides the same (or exceeds the level of) protection as the PSPF requirement.
Chief Security Officer (CSO)	A member of the Senior Executive Service (SES), appointed by the Accountable Authority to provide strategic oversight of protective security for the entity and empowered to make security decisions. Where an entity has fewer than 100 employees, the Accountable Authority may appoint their CSO at the Executive Level 2 (EL2), providing the EL2: • reports directly to the Accountable Authority on security matters, and • has the sufficient authority and capability to perform the responsibilities of the CSO role.
Core requirements	The sixteen core requirements articulate what entities must do to achieve the four security outcomes. These core requirements have a number of mandatory supporting requirements that help facilitate a standardised approach to implementing security across government.

TERM	DEFINITION
Exceptional circumstances	This provision allows the Accountable Authority to adapt to arising circumstances that affect the entity's implementation or maintenance of a particular requirement. Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement, the Accountable Authority may vary application (for a limited period of time) consistent with the entity's risk tolerance. Examples of exceptional circumstances include natural disasters and emergency situations; exceptional circumstances are not routine in nature or enduring.
PSPF maturity self-assessment model	This model requires entities to make an assessment of the maturity of their security capability based on the entity's overall security position within its specific risk environment and risk tolerances. The maturity self-assessment model supports each entity to consider the elements of its security capability. This includes: • implementation and management of each PSPF core and supporting requirement • achievement of security outcomes for governance, information, personnel and physical security • security risks to people, information and assets • risk environments and tolerance for security risks, and • strategies and timeframes to manage identified and unmitigated risks.

TERM	DEFINITION
PSPF reporting portal	The PSPF reporting portal allows Commonwealth entities to: • complete and submit their annual security maturity self-assessment online • access benchmarking reports at the conclusion of the submission period, and • access assessments and reports from previous reporting periods.
Risk-based approach	The PSPF requires entities to take a risk-based approach to protective security and apply proportionate security controls to manage security risks. The basic principles of a security risk-management approach are that you need to identify the risks, apply relevant controls, assess the residual risk and then the relevant person with the appropriate level of authority within the entity accepts the residual risk or decides that additional controls are necessary to bring the residual risk within the entity's risk tolerance. However, there is no discretion to accept risks relating to not fully implementing the PSPF core and supporting requirements, without also accepting a lower level of security maturity ('developing' or 'ad hoc') for your entity in its annual security report.
Risk tolerance	Risk tolerance is an informed decision to accept a risk. It is the level of acceptable risk after risk treatment to achieve an objective or manage a category of risk. The Accountable Authority must determine their entity's tolerance for security risks, supported by a transparent and justifiable process.
Security advisor	Person appointed by the CSO to support them in the day-to-day delivery of protective security and to perform specialist services. While there is no obligation to appoint security advisors, the number you may need will depend on the size, complexity and make-up of your entity.

TERM	DEFINITION
Security capability maturity	Security capability maturity refers to your entity's security position in relation to its specific risk environment and risk tolerances. This includes considering your entity's security capability and effectiveness in implementing the PSPF, as well as acknowledging areas for improvement.
Security culture	Broadly, a culture consists of the values, behaviours and other characteristics common to the members of a particular group. A strong and positive security culture is where all personnel are aware, capable, supported and active in managing security risks around them. It requires security to be fully embedded into your entity's prevailing culture.
Security governance committee	Committee, chaired by the CSO with members from across areas of protective security (covering governance, information, personnel and physical security) to achieve and maintain the required level of protective security oversight and accountability for the entity.
Security incident	A security incident is any irregular or adverse activities or events, threats and behaviours. 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.
Security outcomes	The four desired security outcomes relating to security governance, information, personnel and physical security, outlining the end-state results the government aims to achieve.
Security plan	Articulates how the entity's security risks will be managed and how security aligns with the entity's priorities and objectives.
Security principles	Five fundamental principles that apply to every area of security and guide decision-making.
Security risk	Any event that could result in the compromise, loss of integrity or unavailability of official information or resources, or deliberate harm to people measured in terms of its likelihood and consequences.

Further information

The Protective Security Policy Team in the Attorney-General's Department delivers programs and policies to assist Australian Government entities to protect their people, information and assets, at home and overseas.

Contact the PSPF Team

PSPF Hotline: (02) 6141 3600

PSPF mailbox: PSPF@ag.gov.au

Access PSPF policy

Protective Security Policy Framework
www.protectivesecurity.gov.au

Protective Security Policy GovTEAMS community https://users.govteams.gov.au/Community/1155

PSPF online reporting portal
https://portal.protectivesecurity.gov.au/

Connect with other CSOs

The Chief Security Officer Forum was established to support CSOs in their role as the Australian Government's security custodians. AGD facilities biannual forums to support networking, information sharing and targeted discussions. Email: CSO_Forum@ag.gov.au

Other Australian Government resources on protective security

Australian Security Intelligence Organisation ASIO Outreach
www.outreach.asio.gov.au

Australian Cyber Security Centre
www.cyber.gov.au

Australian Government Information Security Manual
www.cyber.gov.au

Commonwealth Risk Management Policy
www.finance.gov.au/government/comcover/commonwealth-risk-management-policy

For more Australian Government resources visit: www.protectivesecurity.gov.au

Australian and international standards

www.protectivesecurity.gov.au

ISBN: 978-1-921091-28-5 (Print)
ISBN: 978-1-921091-29-2 (Online)

Use of the Coat of Arms

www.protectivesecurity.gov.au