Australian Government
Department of Home Affairs
Protective Security Policy Framework

Protective Security Policy Framework

Assessment Report 2023–24

Table of Contents

List of Figures

Introduction

The Protective Security Policy Framework (PSPF) prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally. It sets out the mandatory requirements for Non-Corporate Commonwealth Entities (NCEs) to achieve the protective security outcomes.

Responsibility for protective security policy transferred to the Department of Home Affairs (the Department) in August 2023 as part of a Machinery of Government change. As reflected in the Minister for Home Affairs, Minister for Immigration and Multicultural Affairs and Minister for Cyber Security's *Directive on the Security of Government Business*, the policy intent of the PSPF is to ensure the secure delivery of government business. Further information about the PSPF is available at Annex A and at www.protectivesecurity.gov.au.

Achieving a robust, positive security culture across entities is fundamental to ensuring reliable and efficient delivery of government business. Managing protective security risks proportionately and effectively enables entities to build trust and confidence between the different levels of government, the Australian public, and international partners.

On 1 November 2024, the Department issued PSPF Release 2024. PSPF Release 2024 demonstrates the Australian Government's commitment to ensuring the policy settings are appropriate for the contemporary threat environment to protect, deter and respond to the security threats and challenges facing the Australian Government. PSPF Release 2024 represents the first in an annual series of releases.

Since its inception, the PSPF has enabled the secure delivery of government business. Building on this legacy, PSPF Release 2024 provides the Australian Government with a world-leading annual process to focus on addressing contemporary protective security threats.

Australian Government entities will be required to report against PSPF Release 2024 requirements in the 2024-25 reporting period.

This is therefore the final report where NCEs were required to report against the previous PSPF's four security outcomes:

1. 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.
2. Information Security: Each entity maintains the confidentiality, integrity and availability of all official information.
3. 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.
4. Physical Security: Each entity provides a safe and secure physical environment for their people, information and assets.

The PSPF requires Accountable Authorities[1] of NCEs to complete an annual self-assessment and report to their relevant portfolio minister and the Department of Home Affairs. This report was prepared using the self-assessment reports submitted by the 100 NCEs that were required to report in 2023-24. Each self-assessment report is approved by the entity's Accountable Authority. To understand the full scale of work by entities to improve security across government, this report should be considered alongside other threat-specific assessments provided by the Australian Security Intelligence Organisation (ASIO) and the Australian Signals Directorate (ASD).

Assessing Continuous Improvement

This is the sixth and final assessment report using the previous PSPF's 4-scale maturity model, detailed in Diagram 1.

[1] The accountable authority of a Commonwealth entity is the person or group of persons responsible for, and with control over, the entity's operations. This is set out in Section 12 of the *Public Governance, Performance and Accountability Act 2013*.

The PSPF maturity model is designed to encourage entities to engage with their unique security risk profile and develop tailored plans and strategies for continuous improvement.

The scaled maturity model recognises that individual entities' threats, vulnerabilities and risks differ and their security posture does not remain static over time. The model allows entities to identify the level of maturity that most accurately reflects the maturity of their security capability over the 12-month reporting period (1 July to 30 June).

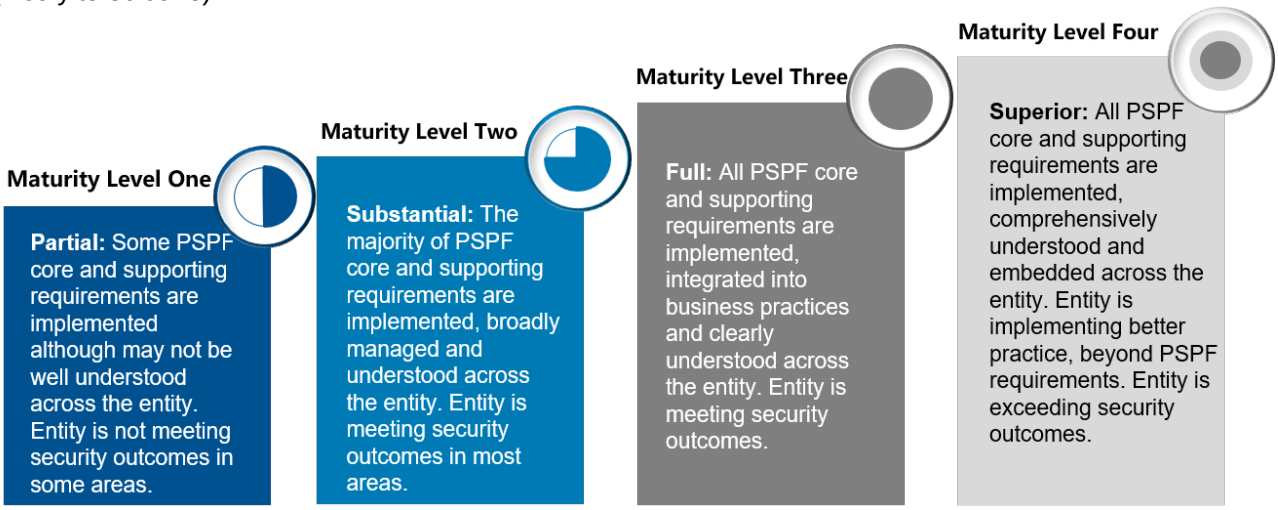

Diagram 1. PSPF Self-Assessment Maturity Model

Maturity Level Four exceeds what entities are expected to implement and requires the highest degree of implementation. Entities need to make their own judgments about whether striving for this maturity level is desirable, based on their risk environment and the efficient and effective use of their resources. It is expected that the majority of entities will fluctuate between Maturity Level Two and Maturity Level Three depending on their risk profile, threat environment, and resources.

PSPF Release 2024 introduces a compliance-based reporting model with a risk management element to replace the self-assessment maturity model. Further information on the new reporting arrangements is available at www.protectivesecurity.gov.au.

Threat Environment

The Australian Government's operating environment remains characterised by a complex geopolitical landscape and accelerated shifts in advancement of technologies. Australians continue to be targeted for espionage and foreign interference. The Director-General of Security's 2024 Annual Threat Assessment noted that Australia's security environment is challenging and changing and that in 2024, threats to our way of life have surpassed terrorism as Australia's principal security concern.

The Australian Government continues to be the target of malicious cyber state and non-state actors that show the intent and capability to compromise Australia's networks. ASD's Annual Cyber Threat Report 2023-2024 notes that while advancements in critical and emerging technologies offer significant social and economic benefits, they also improve the capabilities of malicious cyber actors who continue to target Australia's networks. Critical infrastructure networks are regularly targeted, rendering a significant potential impact to Australia's security and prosperity. Improving the cyber security of Australia's public, private and civil sectors is a priority of the Australian Government. The implementation of preventative cyber security measures is the best way to help secure Australian networks.

PSPF Directions are one such mechanism to address specific security threats that present an unacceptable protective security risk to the Commonwealth. On 8 July 2024, the Secretary of the Department of Home Affairs issued three mandatory PSPF Directions to manage cyber security risks to the Australian Government:

- PSPF Direction 01/2024 requires NCEs to manage Foreign Ownership, Control or Influence (FOCI) Risk in Technology Assets. Entities must identify indicators of FOCI risk as they relate to procurement and maintenance of technology assets, and appropriately manage and report those risks.
- PSPF Direction 02/2024 requires NCEs to undertake a Technology Asset Stocktake of all internet connected technology assets and services and develop a Technology Security Risk Management Plan to manage their technology holdings.

- PSPF Direction 03/2024 requires NCEs to engage with the Australian Signals Directorate (ASD) on cyber security threats, including participating in the Cyber Security Partnership Program, advising ASD of the deployment of threat hunting capabilities and connecting to ASD's Cyber Threat Intelligence Sharing (CTIS) platform.

The past twelve months have reinforced the need for the Australian Government to have a clearer picture of risks to its technology assets and to ensure entities are working with technical authorities, in particular ASD, to address those risks. These PSPF Directions directly address the risk to the Australia Government's existing environments, new procurement and our communications channels.

PSPF Release 2024 and future annual releases will allow protective security policy to adapt and keep pace with new and emerging threats.

Overall Results

The Australian Government's overall protective security maturity remains at Maturity Level 2 (67% of entities), which indicates substantial implementation of protective security requirements.

Overall results for 2023-24 are similar to 2022-23, with only a slight decline in maturity levels reported.

For the first time, all entities reported overall Maturity Level 2 or higher, this represents a 1% improvement from 2022-23 where one entity reported at Maturity Level 1.

Entities self-assessing their overall maturity at Maturity Level 3, which indicates full implementation of the PSPF requirements, reduced slightly in 2023-24 to 33%, down from 35% in 2022-23. Entities reporting at Maturity Level 2 increased by 3% reflecting the movement of one entity previously at Maturity Level 1 to Maturity Level 2, and two entities decreasing from Maturity Level 3 to Maturity Level 2. No entities reported Maturity Level 4 in either 2023-24 or 2022-23.

Figure 1 provides a year-on-year comparison of the overall security maturity at each of the four maturity levels.

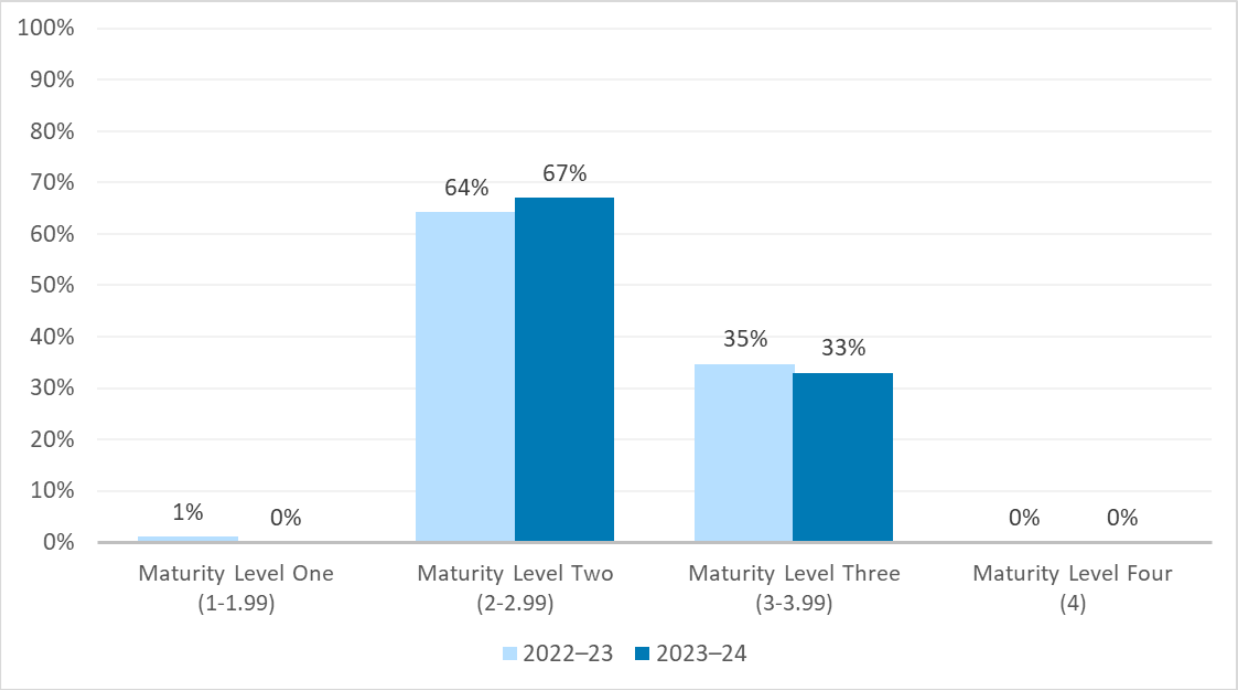

Figure 1. Overall PSPF Security Maturity

Security Outcomes

Maturity decreased across three of the four security outcomes, with Governance Security remaining the same as in 2022-23. Across the four Security Outcomes, fewer entities reported at Maturity Level 3 or higher 2023-24 than in 2022-23. The Information Security and Personnel Security Outcomes decreased by 2% and 4% respectively. There was no change to the Governance Security and Physical Security Outcomes.

As in previous reporting periods, the Information Security Outcome continues to be the most challenging for entities to achieve maturity. 23% of entities reported at Maturity Level 3 or higher for Information Security, down from 27% in 2022-23. There was a corresponding increase in the number of entities reporting at Maturity Level 2 and Maturity Level 1; 69% and 8% respectively, up from 66% and 7% in 2022-23.

Figure 2 provides a year-on-year comparison of the proportion of entities reporting at each of the four maturity levels for the four Security Outcomes.

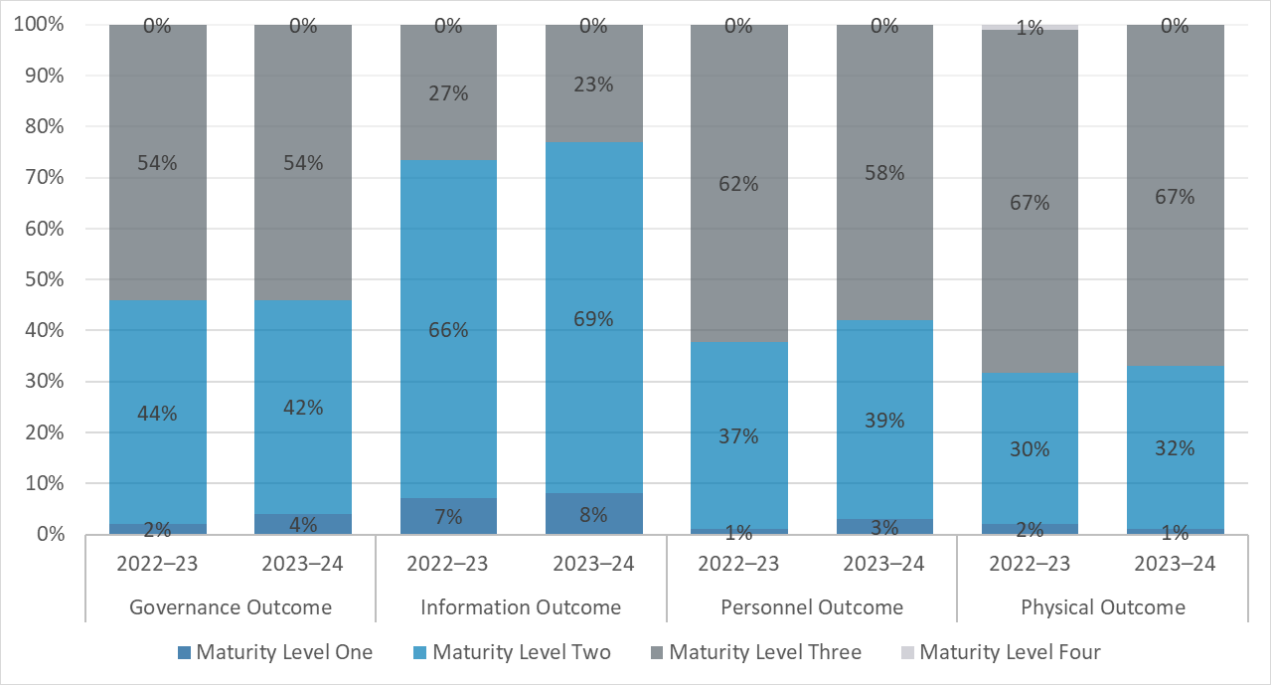

Figure 2. Overall Maturity of Security Outcomes

Entities that reported Maturity Level 1 for any of the 16 policies were referred to Technical Authority Entities for support, for example, ASIO for Physical Security and ASD for Information Security. The Department also shared reporting data with ASIO and ASD to inform uplift programs and guidance to entities on areas for targeted improvement.

Security Governance

The Security Governance Outcome requires entities to manage security risks and support a positive security culture. Entities must have effective arrangements in place, including clear lines of accountability, sound planning, investigation and response, assurance and review processes, and proportionate reporting.

The number of entities that reported Maturity Level 3 for Security Governance in 2023–24 remained at 54%, the same as in 2022-23. 96% of entities reported Maturity Level 2 or higher for Security Governance, down from 98% in 2022-23. There was a 2% increase in the number of entities reporting at Maturity Level 1.

Figure 3 details maturity levels for each of the seven policies in the Security Governance Outcome.

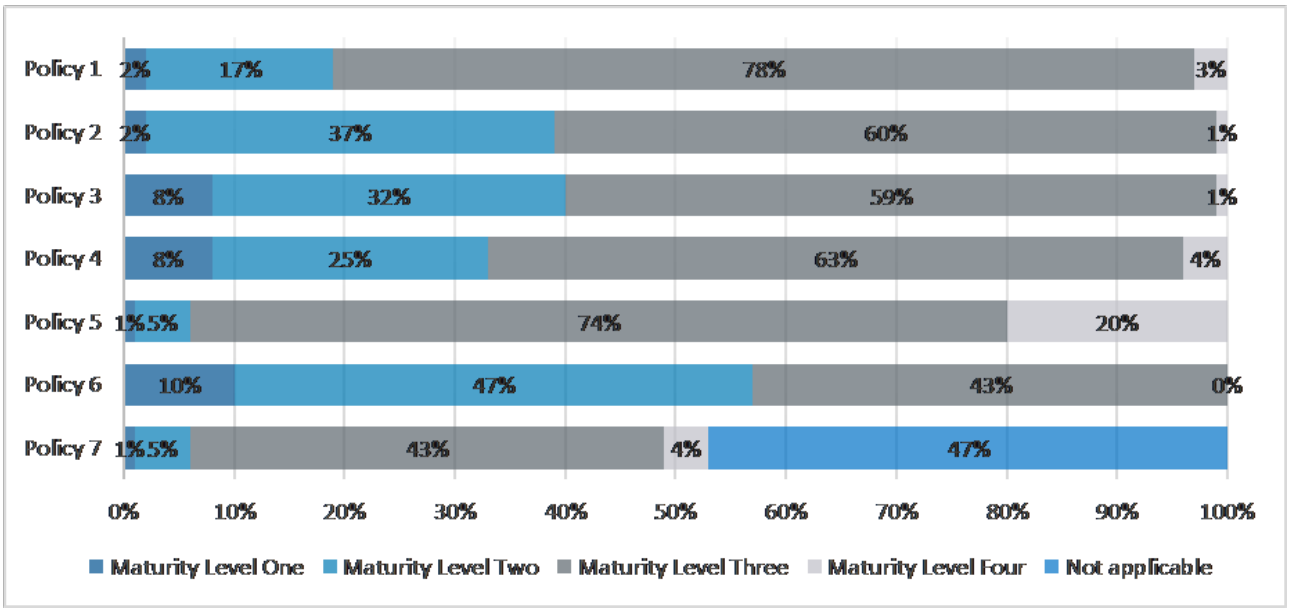

Figure 3. Maturity Levels for Security Governance Outcome

Of seven Security Governance polices, only one, PSPF Policy 7: *Security Governance for International Sharing*, recorded an increase of entities reporting at Maturity Level 3; 47%, up from 46% in 2022-23. All other policies registered an overall decrease in maturity.

PSPF Policy 4: *Security Maturity Monitoring* experienced the greatest decrease in entities reporting at Maturity Level 3 or higher; 67%, down from 78% in 2022-23 where it was the most improved policy in 2022-23 across all 16 polices.

PSPF Policy 1: *Role of Accountable Authority* also registered a decrease in entities reporting at Maturity Level 3 or higher; 81%, down from 89% in 2022-23.

A change to the maturity calculation methodology in 2022-23 had resulted in some unintended consequences leading to a greater proportion of entities represented at the Maturity Level 4 in 2022-23. This was resolved in the 2023-24 reporting period.

PSPF Direction 001–2023

PSPF Policy 1: *Role of Accountable Authority* enables the Secretary of the department with responsibility for the PSPF to issue mandatory PSPF Directions to accountable authorities. A PSPF Direction is a binding requirement to Government entities to manage an unacceptable protective security risk and is informed by advice from intelligence and security agencies.

PSPF Direction 001-2023 was issued on 4 April 2023 to restrict the access and installation of the *TikTok* application on government devices, with exceptions for legitimate business reasons. The Direction focused on addressing the emerging security risks associated with this application.

Entities were asked in both the 2022-23 and 2023-24 PSPF reporting cycles whether they had complied with this Direction. As the Direction was issued part-way through the 2022-23 reporting period, the question was not scored and did not count towards entities' maturity in 2022-23. In 2023-24, the question was scored and counted towards the overall score for PSPF Policy 1: *Role of Accountable Authority*.

In 2023-24, 89% of entities reported that they had prevented the installation and removed existing instances of the TikTok application on Government devices, down from 91% in 2022-23. A total of 4 entities that reported they had prevented the installation and removed existing instances of the TikTok application on Government devices in 2022-23, changed their response in 2023-24, indicating they were not compliant with the requirements of the Direction.

Entities reported the following impediments to adhering to the Direction:

- lack of technical ability to block or prevent users from installing the TikTok app on work issued devices or personal devices used for work purposes (BYOD) and,
- in some instances, the legacy configuration of relevant systems preventing the entity from being able to enforce application control.

Policy Updates – Security Governance

During 2023-24:

- PSPF Policy 2: *Management Structures and Responsibilities* was amended to:
  - require Chief Security Officers hold a minimum Negative Vetting Level 1 security clearance, and
  - mandate the appointment of a Chief Information Security Officer to be responsible for cyber security leadership in the entity.
- PSPF Policy 5: *Reporting on Security* was amended to improve reporting of significant security incidents and introduce guidance to support decision-making.

Information Security

The Information Security Outcome requires entities to maintain the confidentiality, integrity and availability of all official information and assets owned by the Australian Government, or those entrusted to the Australian Government by third parties, or through international agreements with Australia.

Information Security continues to be the most challenging outcome for entities to reach and maintain full implementation. The number of entities reporting at Maturity Level 1 for Policy 8: *Classification System* reduced to 0% in 2023-24, down from 6% in 2022–23. The number of entities reporting at Maturity Level 3 for PSPF Policy 9: *Access to Information* increased to 75%, up from 69% in 2022-23.

Entities reported the following impediments to achieving higher levels of maturity for Information Security:

- introduction of additional controls to the Essential Eight Maturity Model
- uplift projects currently underway
- limited resources
- size of the entity
- constraints caused by shared service providers for outsourced systems and services
- minimum handling requirements and continuous uplift in the cyber security space, and
- continued reliance on legacy information technology (IT).

Figure 4 details maturity levels for each of the four policies in the Information Security Outcome.

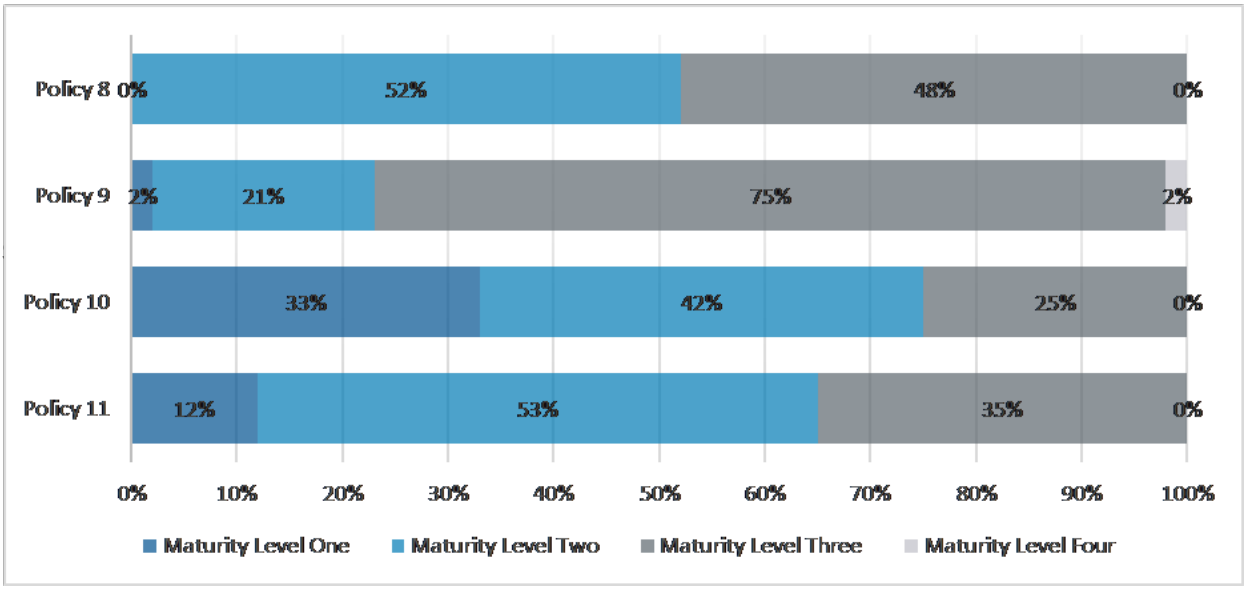

Figure 4. Maturity Levels for Information Security Outcome

Safeguarding data from cyber threats

From 1 July 2022, entities were required to implement all eight strategies of ASD's Essential Eight Mitigation Strategies and the 2023-24 reporting period was the second time that reported maturity for all eight counted towards an entity's maturity rating. In earlier reporting periods, only the subset of strategies known as the 'Top 4' counted towards maturity.

PSPF Policy 10: *Safeguarding Data from Cyber Threats* remains the policy with the highest number of entities reporting Maturity Level 1 across all 16 policies: 33% in 2023-24, up from 22% in 2022-23. This is reflected in a decrease in the number of entities reporting at Maturity Level 3 at 25%, down from 36% in 2022-23. The number of entities reporting Maturity Level 2 remained at 42% in 2023-24, unchanged from 2022-23.

Entities that reported Maturity Levels 1 and 2 noted:

- November 2023 changes to the Essential Eight Maturity Model had a significant impact on entities' capacity to improve maturity against these additional controls within the time available
- implementation of cyber uplift projects, some of which are multi-year in focus, complicated compliance, resulting in a reduction of maturity levels
- external entities responsible for management of some IT aspects led to reduced capacity for control
- unique nature of a complex IT environment, legacy IT, and limitations on resources contributed to the challenges in meeting existing PSPF requirements, and
- challenges to ensure the consistent application and regular review of PSPF requirements.

Legacy IT

Entities have consistently reported that a continued reliance on legacy IT inhibits their ability to completely implement ASD's Essential Eight Mitigation Strategies. 76% of entities reported having one or more legacy system, up from 70% in 2022-23. The increases is partly attributable to the introduction of a standard definition for 'legacy IT' in PSPF Policy 11: *Robust ICT Systems* and entities having a greater understanding of what constitutes a legacy system.

In April 2024, ASD published Managing the Risks of Legacy IT: Practitioner Guidance which provides which provides low-cost mitigations for legacy IT that entities can draw upon, in addition to their own strategies until such time as it can be replaced. PSPF Release 2024 introduced a new requirement for entities to implement ASD's temporary mitigations for legacy IT to manage IT that cannot yet be replaced.

While most entities noted uplift work was underway, they reported various challenges to transitioning away from and retiring legacy IT systems, including:

- entity capacity and capability
- complexity of change
- dependency on whole-of-Government systems that are not compliant
- prioritisation of limited resources, project funding, and required work against other demands within the entity
- resource constraints, including insufficient funding and workforce limitations, and
- risk of disrupting operations where there is a capability shortfall or impacts to business continuity are anticipated.

Policy Updates – Information Security

During 2023-24:

- PSPF Policy 8: *Classification Systems* was amended to change the OFFICIAL: Sensitive Dissemination Limiting Marker (DLM) to a security classification. The change to OFFICIAL: Sensitive did not trigger the necessity for on-flow changes to:
    - Email Protective Marking System (EPMS) – OFFICIAL: Sensitive is already treated as a security classification within the EPMS
    - access to information security clearance requirements for OFFICIAL: Sensitive – employment screening for entity personnel remains sufficient
    - minimum protections and handling requirements for OFFICIAL: Sensitive – these remain unchanged, and
    - Australian Government Security Caveat Standard – caveats that allow use with OFFICIAL: Sensitive are already indicated.

Personnel Security

Entities are required to ensure their personnel (including contractors) meet an appropriate standard of integrity and honesty, and are suitable to access Australian Government resources. Effective Personnel Security facilitates the trusted sharing of Australian Government resources and mitigates the threat posed by trusted insiders.

The number of entities reporting at Maturity Level 3 and above decreased to 58% in 2023-24, down from 62% in 2022-23. The number of entities reporting at Maturity Level 1 increased to 3%, up from 1% in 2022-23. The number of entities reporting at Maturity Level 2 increased to 39%, from 37% in 2022-23.

A total of 76% of entities reported Maturity Level 3 or higher for PSPF Policy 12: *Eligibility and Suitability of Personnel*, up from 71% in 2022-23. Conversely, entities reporting at Maturity Level 3 or higher for PSPF Policy 13: *Ongoing Assessment of Personnel* decreased to 64%, down from 68% in 2022-23. Maturity Level 3 or higher for PSPF Policy 14: *Separating Personnel* reminded stable at 71%, as in 2022-23.

Entities reported the following impediments to achieving higher levels of maturity for Personnel Security:

- lack of policy frameworks for managing the ongoing suitability of personnel after initial on-boarding
- lack of established reporting mechanisms to confirm mangers have undertaken annual security checks and assessments of ongoing suitability of security cleared staff
- yet to be established Trusted Insider Threat mechanisms
- yet to be implemented TOP SECRET-Privilege Access Standard,
- not using the Document Verification System, and
- insufficient separation procedures.

Figure 5 details maturity levels for each of the three policies in the Personnel Security Outcome.

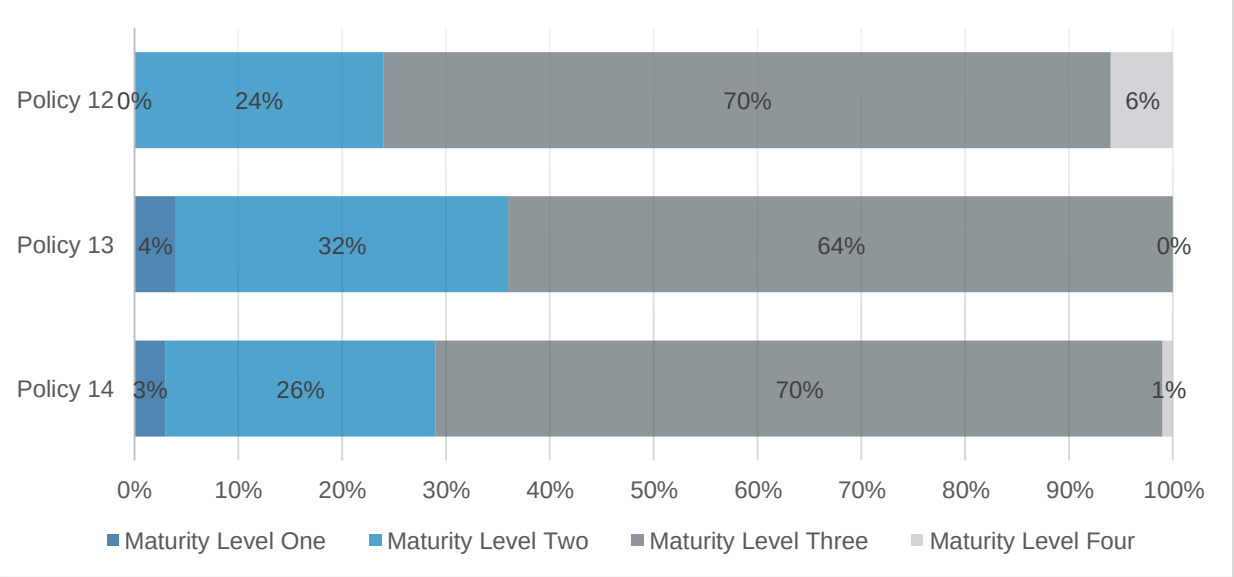

Figure 5. Maturity Levels for Personnel Security Outcome

Policy Updates – Personnel Security

During 2023–24:

- PSPF Policy 12: *Eligibility and Suitability of Personnel* and PSPF policy 13: *Ongoing Assessment of Personnel* were updated to reflect a terminology change for ASIO security assessments to 'ASIO security clearance suitability assessment'. This aligns more closely with changes to the *Australian Security Intelligence Organisation Act 1979*.
- PSPF Policy 12: *Eligibility and suitability of personnel* was amended to clarify that the TOP SECRET-Privileged Access Authority is a vetting authority and updated references to relevant Australian Standards.

Physical Security

Entities are required to provide a safe and secure physical environment for their people, information and resources.

Reported maturity for the Physical Security Outcome in 2023-24 was similar to 2022-23.

The number of entities reporting at Maturity Level 3 and above only slightly decreased to 67%, from 68% in 2022-23. There was an improvement in Maturity Level 1 results with only 1% of entities reporting at that level, down from 2% in 2022-23.

A total of 83% of entities reported Maturity Level 3 or higher for Policy 15: *Physical Security for Entity Resources*, down from 86% in 2022-23.

Entities reported the following impediments to achieving higher levels of maturity for Physical Security:

- compliance at the enterprise level with departmental physical security policies and procedures is not consistently understood, and
- IT asset control and disposal of communication assets without factory default.

Information is available to support Physical Security implementation through ASIO Outreach and ASIO's Technical Notes.

Figure 6 details maturity levels for each of the two policies in the Physical Security Outcome.

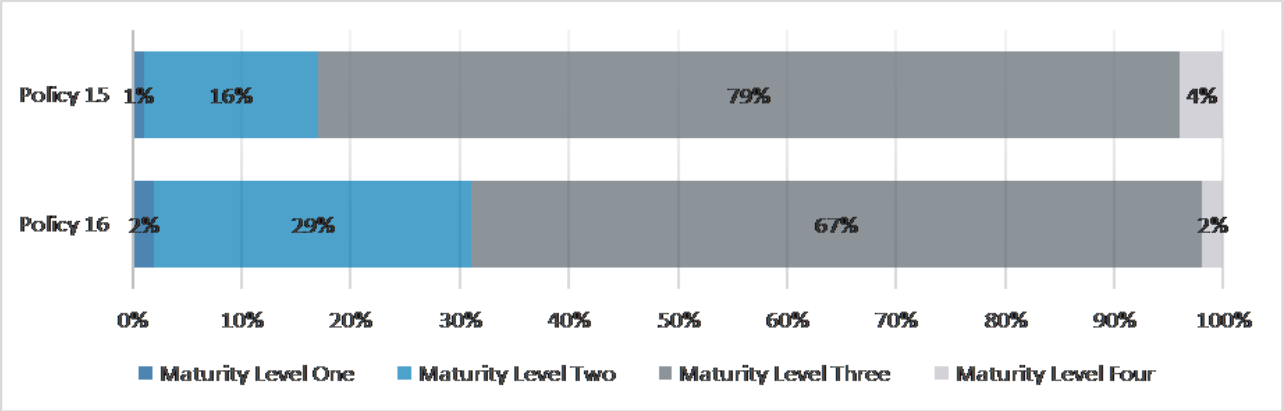

Figure 6. Maturity Levels for Physical Security Outcome

Entities Posing a Heightened Security Risk

Entities are assessed as posing a heightened security risk if they:

- Do not submit an annual assessment report
- Report an overall level of Maturity Level 1, and/or
- Report a substantial decline in their maturity in successive years in three or more core requirements.

Of the 100 NCEs required to report, 100% submitted an assessment for 2023-24.

For the first time, no entities reported overall maturity at Maturity Level 1. This represents a consistent improvement over the past three reporting periods where one entity reported overall maturity of Maturity Level 1 in 2022-23 and two in 2021-22.

Corporate Commonwealth Entities

Corporate Commonwealth Entities (CCEs) and wholly-owned Commonwealth Companies (CCs) are not required to comply with the PSPF, but are encouraged to implement the PSPF as best practice.

In 2023-24, eight CCEs voluntarily submitted an annual assessment report, of which seven reported an overall maturity at Maturity Level 2. One reported overall maturity at Maturity Level 3.

Six of the CCEs that reported in 2022-23 reported again this year, along with two new entities that elected to report for the first time.

Conclusion

The threat environment in Australia remains complex, challenging and changing. Protective security standard set by the Government are adjusted throughout the year in order to address emerging threats in a timely manner and to keep pace with this rate of change.

This is the sixth assessment report using the PSPF's maturity model and results demonstrate a slight decrease in the overall level of maturity of entities compared to 2022-23, as well as a slight decline across each of the four security outcomes. In 2023-24, the cyber security components of the Information Security Outcome remained the most challenging for entities to implement and it is expected this trend will continue into the future.

Entities will continue to fluctuate between Maturity Level 2 and Maturity Level 3, depending on their risk profile, threat environment, and available resources. Movement between maturity levels is also expected when requirements are amended or new requirements are imposed part way through a reporting cycle. Nevertheless, entities are falling below the standard set by the PSPF and there is more work to do to shift the Australian Government's overall protective security above Maturity Level 2.

Every entity has an important role to play in the security of Australian Government business. The Australian Government will continue to support entities and invest in measures to uplift and transform our collective protective security.

For further information and support, please contact PSPF@homeaffairs.gov.au or visit the Protective Security Policy Framework website.

Annex A: Structure of the Protective Security Policy Framework

It is mandatory for NCEs to apply the PSPF as it relates to their risk environment. For other Commonwealth entities (Corporate Commonwealth Entities and wholly owned Commonwealth Companies), the PSPF is best practice.

Prior to the introduction of PSPF Release 2024, the PSPF comprised:

- Five security principles
- Four security outcomes, and
- 16 policy requirements.

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.

Security Outcomes

The four security outcomes outline the desired end-state the Government aims to achieve.

- 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.

PSPF Policies

The 16 policies in the previous PSPF articulated the requirements entities must implement to deliver the Government's desired protective security outcomes.

These policies, now replaced by PSPF Release 2024, are available to Government personnel on the Protective Security Policy GovTEAMS community.

OUTCOME	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.
INFORMATION	8. Classification System	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 Data 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 consistent and structured approach to building construction, security zoning and Physical Security control measures of your entity's facilities.