



Australian Government
Attorney-General's Department

Protective Security Policy Framework

2018-19 Assessment Report

Contents

- Protective Security Policy Framework.....1
 - 2018-19 Assessment Report.....1
 - Introduction.....3
 - Revised framework.....3
 - Evolving maturity model.....3
 - Assessing continuous improvement.....4
 - Key observations5
 - Overall security assessment results6
 - Security Governance.....7
 - Information security8
 - Personnel security9
 - Physical security10
 - Entities posing a heightened security risk11
 - Conclusion11
- Annex A: Structure of the reformed Protective Security Policy Framework from 1 October 2018.....12
- PSPF – Security outcomes and PSPF policies.....13

Introduction

The Protective Security Policy Framework (PSPF) assists Australian Government entities to protect their people, information and assets, both here and overseas.

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 our international partners.

Security is everyone's business, and these annual assessment reports are one way Australian Government entities can better develop a comprehensive understanding of emerging security risks, and work to continuously improve their security practices.

Revised framework

On 1 October 2018, the Attorney-General issued the revised Protective Security Policy Framework (PSPF).

The reforms address findings from the *2015 Independent Review of Whole-of-Government Internal Regulation*, and ensure the PSPF keeps pace with international best practice by:

- building and maintaining a strong security culture that effectively engages with risk
- addressing the malicious insider threat through improved personnel security, and
- increasing the cyber security of government networks and information.

The revised PSPF implements reforms that seek to improve clarity, reduce unnecessary 'red tape' and foster a strengthened security culture across government.

The PSPF applies to non-corporate Commonwealth entities (NCCE) and must be applied as it relates to their respective risk profile. It represents better practice for corporate Commonwealth entities (CCE) and wholly-owned Commonwealth companies (CC). Further information about the PSPF, including an overview of the security principles, is available at **Annex A**.

Evolving maturity model

The PSPF is a living document and is regularly updated to reflect new and emerging issues, developments in protective security best practice and changes to Government policy. It recognises that entities operate within a complex and dynamic threat environment. Terrorism, espionage, foreign interference, malicious insiders, and cyber intrusion are examples of threats that impact on the 4 protective security outcomes of security governance, information security, personnel security and physical security. The PSPF requires entities to continuously update their security posture to reflect their changing risk profile.

This annual assessment report is the first using the new four-scale maturity model and replaces the former binary compliance-based model. The new maturity model adopts international best practice and is designed to encourage entities to better engage with their unique security risk profile, as well as develop tailored plans and strategies for continuous self-improvement. The maturity model recognises that entities' security posture does not remain static over time.

As a result of the different reporting methodology, it is not possible to make a direct comparison between the results in this, and previous reports. However, the results are able to be broadly compared to understand both enduring vulnerabilities, and efforts to reach a more mature and resilient security posture.

While the new model allows for year-on-year comparison moving forward, it is not intended to provide a baseline comparison. Results should be considered in the context of the threat environment at the time of the report. It is expected that entities may fluctuate across the maturity scale as they identify, detect and respond to new and emerging threats.

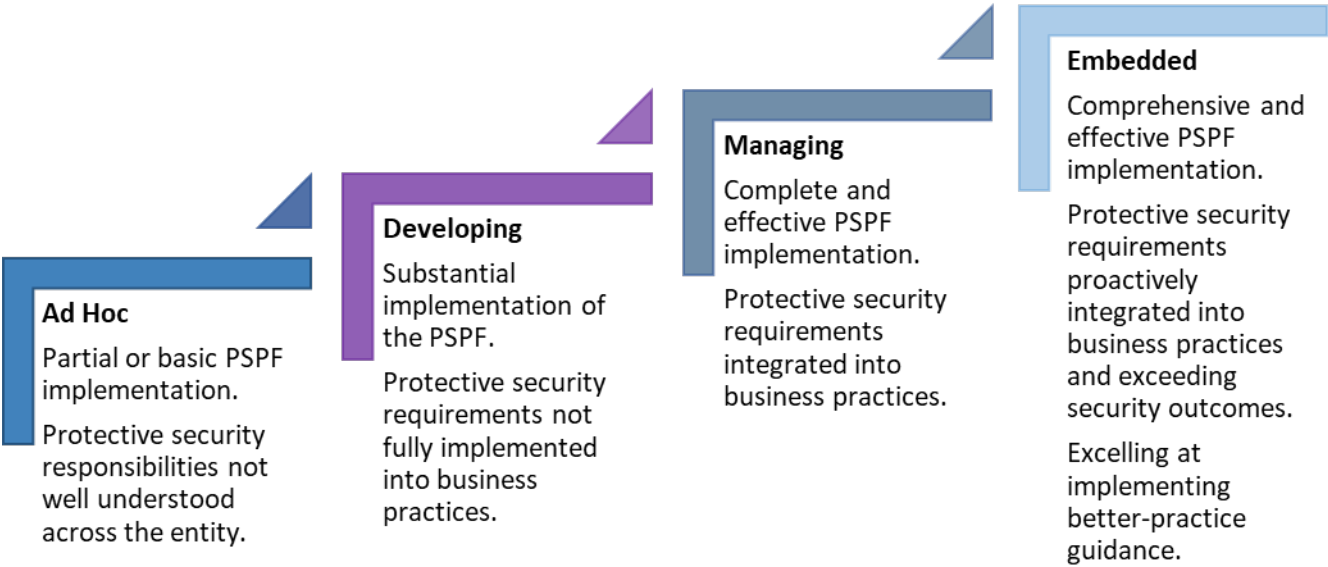
This report should be considered alongside other threat-specific assessments, for example the Commonwealth Cyber Security Posture report, to understand the full scale of work being undertaken by entities to improve security across government.

Assessing continuous improvement

Under the new four-scale maturity model, entities are required to make an assessment of their security maturity against each of the 16 core policies¹ set out in the PSPF. The new model includes 4 maturity levels, which are set out at **Diagram 1**.

The scaled assessment model recognises that individual entities’ threats, vulnerabilities and risks differ. This enables entities to better understand their unique risk profile, better identify the level of maturity of their security capability, and tailor strategies for improvement.

Diagram 1. PSPF maturity assessment model

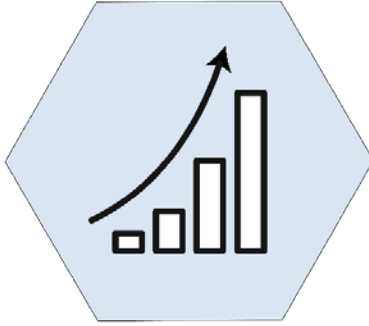


An entity’s overall maturity level is calculated by averaging their assessed maturity level for each of the 16 PSPF policies. This approach provides a holistic picture of the entity’s overall security posture. Recording ‘ad hoc’ or ‘developing’ maturity in any policy reduces the likelihood of achieving a ‘managing’ maturity level overall.

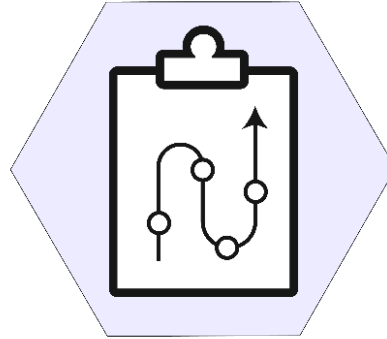
The ‘embedded’ level is above what entities are expected to implement and striving for this maturity level will depend on the individual entity. Not all entities are expected to aim for the ‘embedded’ maturity level. This recognises that it requires the highest degree of implementation and entities need to make an individual judgment about whether striving for this maturity level is required based on their risk environment and available resources. It is expected that the majority of entities will fluctuate between ‘developing’ and ‘managing’ maturity depending on their risk profile, threat environment, and available resources.

¹ See Annex A for more details.

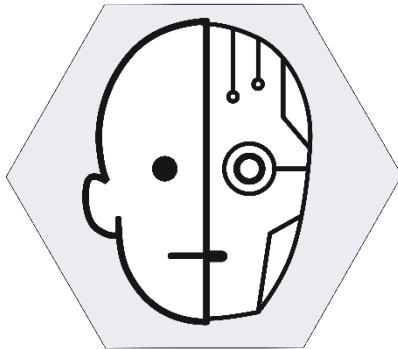
Key observations



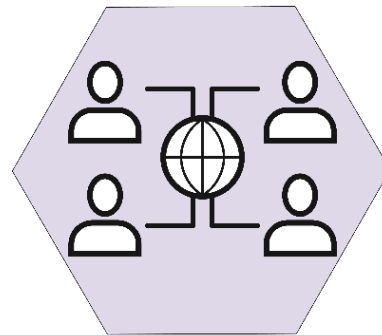
89% of entities reported substantial or higher implementation



The majority of entities have plans and timeframes in place for continuous improvement



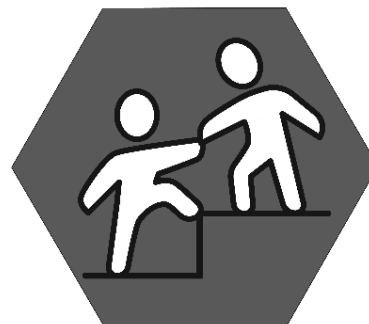
Cyber remains the most significant threat to entities



The Government has introduced a range of initiatives to improve cyber security and increase the overall cyber security capability of entities



Entities reported progress against implementation of the PSPF reforms



Entities with the lowest levels of maturity have been referred to relevant entities to support uplift efforts

Overall security assessment results

In the 2018-19 reporting period, all 98 NCCEs submitted their annual assessment report. There is substantial implementation overall of the PSPF policies, with 89% of entities reporting a ‘developing’ or higher level of maturity. While some entities require additional supports, these results demonstrate that entities are working to continually improve their security posture, and demonstrate a sound understanding of the threat environment in which they operate.

Figure 1 provides a snapshot of the distribution of the consolidated overall maturity levels reported by all NCCEs. These percentages are not average figures.

Figure 1. Overall PSPF security maturation

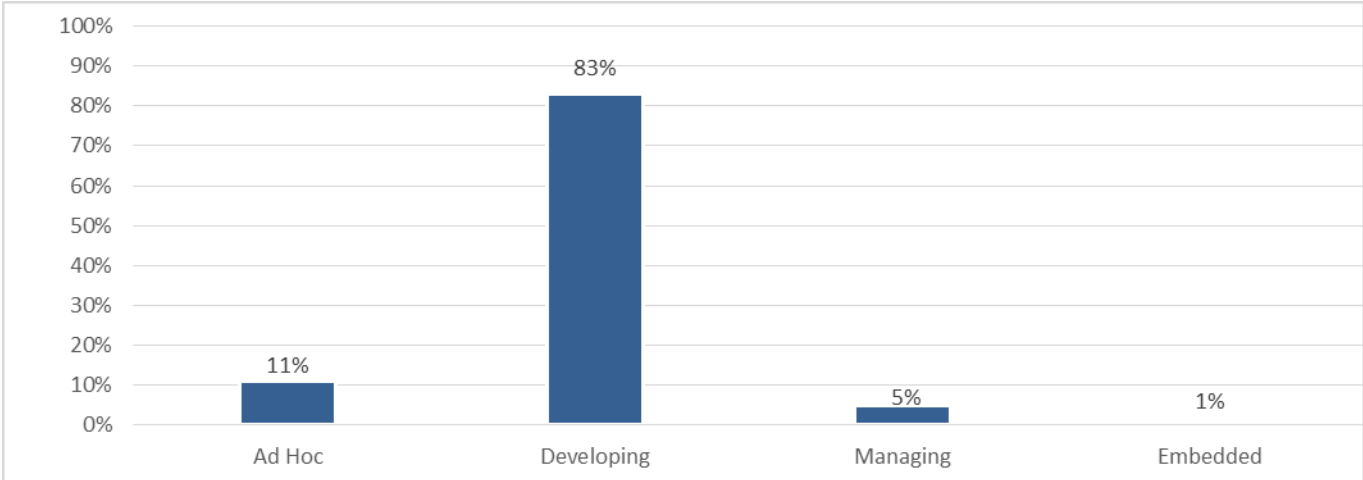
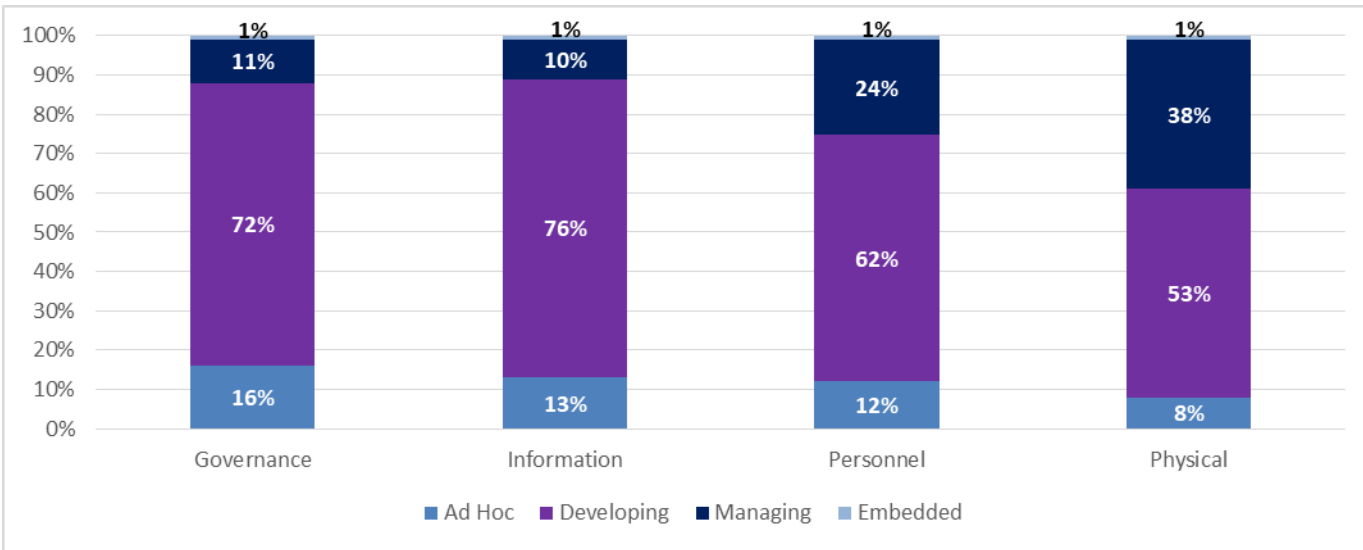


Figure 2 details the maturity of the 4 security outcomes, calculated by consolidating the maturity levels reported by each NCE for the 4 outcome maturity levels. These percentages are not averaged figures, instead demonstrating the percentage distribution of the consolidated maturity levels of the individual performances of the 98 NCCEs against the security outcomes.

Figure 2. Overall maturity of 4 security outcomes



The security governance outcome had the lowest level of maturity across all entities – 16% reported at the ‘ad hoc’ level. This outcome requires entities to manage security risks and support a positive security culture

by ensuring clear lines of accountability, sound planning, investigation and response, assurance and review processes, and proportionate reporting. This result is not unexpected and can be attributed, in part, to the reforms to the PSPF which were introduced in October 2018. Implementation of some of the new requirements was not required until the 2019-20 reporting period. The majority of entities that reported as 'ad hoc' have plans and timeframes in place to improve their maturity in the 2019-20 reporting period.

Entities that reported as 'ad hoc' for the security governance outcome were more likely to have also reported as 'ad hoc' for their overall maturity. This highlights the importance of proper governance coupled with development of a sound security culture as being fundamental to good protective security.

Information security remains an ongoing issue for NCCs with 13% reporting at the 'ad hoc' level. Nevertheless, it is encouraging that 87% of entities reported at the 'developing' or higher level in the first year of using the new model. Entities indicated they were most concerned about malicious cyber activities. Some entities may have reported a lower level of maturity due to new or emerging threats, while others reported that the practices they had in place enabled them to adequately respond to their risk profile.

Entities identified low information security capability, and financial and staffing constraints as barriers to full and effective implementation across the 16 core requirements. Those with 'ad hoc' maturity have been referred to relevant entities, such as the Australian Cyber Security Centre (ACSC), for support to uplift their security capability.

The Attorney-General's Department's (AGD) protective security policy Communities of Practice also provide entities with an opportunity to increase their maturity level by discussing issues, engaging on common risk concerns, identifying new and emerging threats, and accessing and sharing products that may assist to address particular security concerns.

Entities operating in environments with higher risk² provided more detailed articulation of their operational risks and mitigations. Entities where there are likely to be significant consequences as a result of security breaches demonstrated a lower threshold for risk in their reporting. These entities were more cautious in their security maturity assessments than counterparts who operate in an environment with fewer threats, contributing to a greater number of overall maturity assessments at the substantial implementation ('developing') level compared to the complete implementation ('managing') level.

Security Governance

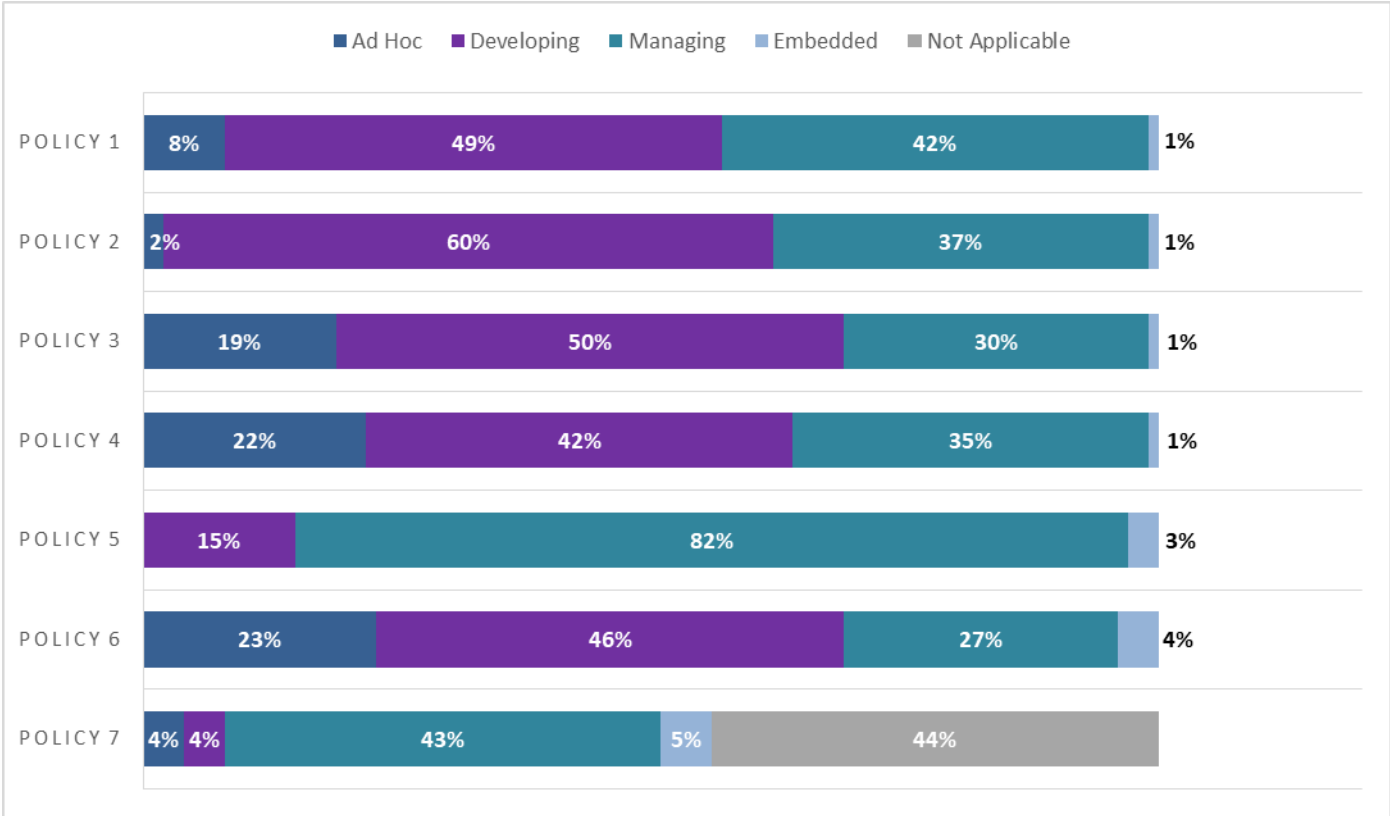
Entities are required to have effective arrangements in place which include clear lines of accountability, sound planning, investigation and response, assurance and review processes, and proportionate reporting for an entity's protective security arrangements.

Across the security governance outcomes, 84% of entities reported 'developing' or higher maturity, which equates to substantial implementation.³ Figure 3 details how entities reported in relation to each of the seven policies that comprise this outcome.

² Entities holding large volumes of classified information and/or working in areas vulnerable to attack by malicious actors are considered operating in environments with higher risk

³ See Figure 2

Figure 3. Maturity for security governance policies⁴



Entities were still implementing some of the new requirements of the reformed PSPF during this reporting period. Entities indicated they have plans and timeframes in place to achieve implementation, and therefore improve their maturity level, during the 2019-20 reporting period.

Entities also have access to a range of education and security awareness materials to support implementation of security governance through the protective security policy Communities of Practice delivered by AGD.

Information security

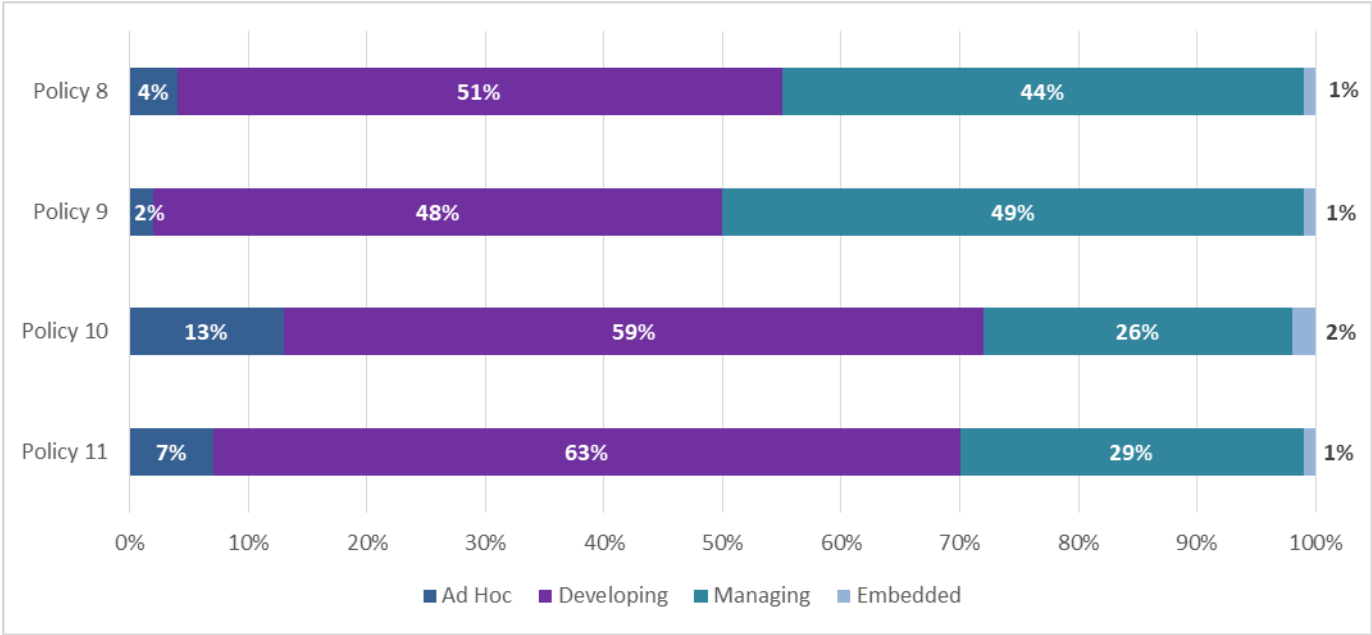
Entities are required to maintain the confidentiality, integrity and availability of all official information and information assets owned by the Australian Government, or those entrusted to the Australian Government by third parties, within Australia. Safeguarding from cyber threats and ensuring robust ICT systems are critical and entities must meet the Australian Signals Directorate’s (ASD) Top 4 strategies to mitigate cyber security risks.

A maturity level of ‘developing’ or higher was reported by 87% of entities, which equates to substantial implementation.⁵ This is a promising result and recognises that more entities are taking steps to apply the baseline strategies to increase their maturity.

Figure 4 details how entities reported in relation to each of the four policies that comprise this outcome.

⁴ Policy 7 relates to security governance for international sharing. Where agencies do not have international arrangements in place, they are not required to report.
⁵ See Figure 2

Figure 4. Maturity for information security policies



The PSPF Assessment Report data is shared with the ACSC. This enables the ACSC to provide technical expertise and deliver entity-specific assistance to improve capability. The PSPF and the Australian Government Information Security Manual are aligned and set clear and consistent cyber security requirements from both the policy and technical perspective.

The PSPF is also complemented by the ACSC’s *Cyber Uplift Program* and Home Affairs’ *Cyber Security Strategy 2020* which are designed to enhance understanding of cyber security expectations and improve capability. Additionally, the obligation for entities to complete the annual ASD cyber security survey was included in the 2018-19 reporting, with 94% of entities acknowledging that they had completed the survey.

Personnel security

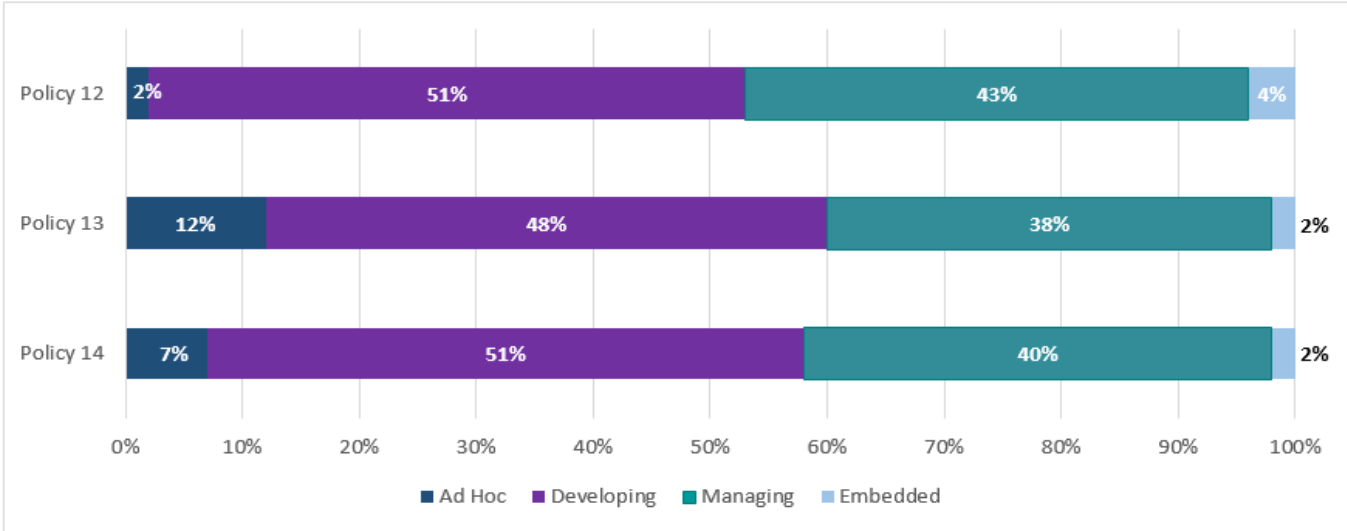
Entities are required to ensure their employees and contractors meet an appropriate standard of integrity and honesty, and are suitable to access Australian Government resources. Effective personnel security facilitates the trusted sharing of Australian Government resources, and mitigates the insider threat.

‘Developing’ or higher maturity was reported by 88% of entities which equates to substantial implementation.⁶

Figure 5 details how entities reported in relation to each of the three policies that comprise this outcome.

⁶ See Figure 2

Figure 5. Maturity for personnel security policies



Access to classified resources is subject to personnel successfully undergoing a vetting process and holding a valid security clearance. The PSPF provides a waiver process entities can employ, where exceptional business requirements exist, to enable personnel who are not able to obtain a security clearance to still access classified resources. These waivers relate to the Australian citizenship requirement and the checkable background requirement (where a person has lived outside of Australia for longer than 12 months, and that time cannot be validated by an Australian citizen).

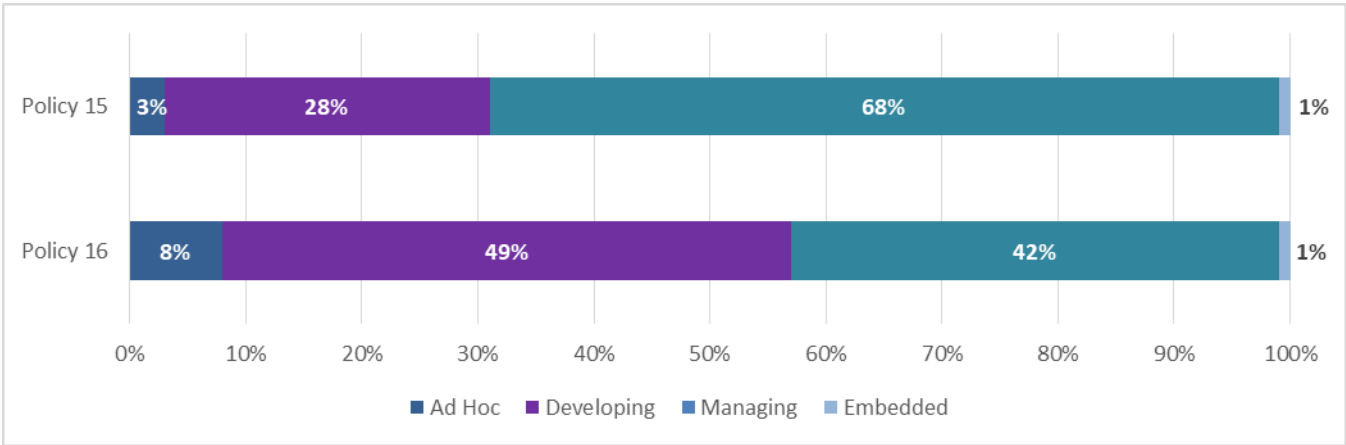
Waivers are role-specific, non-transferable, finite and subject to an annual review. Given waivers raise their risk profile, entities are required to report on the number of active citizenship and checkable background waivers. In the 2017-18 reporting period, 264 active waivers (186 citizenship and 78 checkable background) were reported as compared to 280 active waivers (215 citizenship and 65 checkable background) in the 2018-19 period.

Physical security

Entities are required to provide a safe and secure physical environment for their people, information and assets. There is substantial implementation of physical security outcomes with 92% of entities reporting a maturity level of ‘developing’ or higher.

Figure 6 details how entities reported in relation to each of the two policies that comprise this outcome.

Figure 6. Maturity for physical security policies



The results demonstrate that entities are implementing appropriate protections, however, improvements can be made by considering physical security requirements during building construction or modifications. Information is available to support these efforts through the Chief Security Officer Forum delivered by AGD.

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 'ad hoc', and/or
- report a substantial decline in their maturity in successive years by three or more core requirements.

All 98 NCCEs submitted their annual assessment report, with 11 entities reporting an overall maturity level of 'ad hoc'. Of these, five assessed their security environment as low-risk and three assessed theirs as medium risk. The remaining three did not provide sufficient information to confirm their risk profile. All 11 entities indicated they have plans in place to improve their security plans and processes, and demonstrated a commitment to strengthening governance processes within 12-18 months.

Conclusion

This is the first report using the new maturity model and reflects the importance of entities actively engaging with risk, developing a robust understanding of their threat environment, and committing to improving the security of their information, people and assets in order to maintain high levels of security maturation.

Proper governance coupled with the development of a sound security culture is fundamental to strong and enduring protective security. AGD, in cooperation with other lead security entities such as ASD, will continue to work with entities to improve their security posture.

For more information and support, please contact PSPF@ag.gov.au or visit the [Protective Security Policy Framework](#) website.

Annex A: Structure of the reformed Protective Security Policy Framework from 1 October 2018

The revised PSPF comprises:

- 5 principles
- 4 outcomes, and
- 16 core requirements.

This structure replaces the former 36 mandatory requirements. Entities' responsibilities to protect their people, information and assets remain.

Key policy changes include:

Security governance

- Clearer articulation of the role of the accountable authority and the new Chief Security Officer role.
- Greater prominence to embedding security culture within the entity.
- Greater focus on a risk management approach to security.
- Introduced the security maturation monitoring requirement for ongoing consideration and oversight of the maturity of the entity's security capability and risk culture.

Information security

- Simplified security classification of information system, with an extended implementation period until 1 October 2020.
- Increased focus on cyber security matters through better articulation of the cyber requirements, consistent with the Information Security Manual.

Personnel security

- Introduced the requirement for entities to verify a person's identification by using the Document Verification Service (DVS).
- Increased importance of conducting annual security checks.
- Highlighted the importance of personnel security information risk sharing.

PSPF – Security outcomes and PSPF policies

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. Sensitive and security 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 consistent and structured approach to building construction, security zoning and physical security control measures of your entity's facilities.