Australian Government
Attorney-General's Department

Protective Security Policy Framework

Summary of key changes

The new Protective Security Policy Framework (PSPF) commenced on 1 October 2018.

Then (2014 PSPF)	Now (2018 PSPF)
Architecture	
• Complex—unclear what is mandatory • 29 policy documents • 36 core security requirements • 2,200 supporting controls	• Simplified—more logical, principles-based, clarity of mandatory requirements • 16 core requirements explained 16 policy documents—achieved by removing duplication within the PSPF and with other government legislation or policy • 143 supporting requirements
Security governance	
• Compliance encourages tick box approach to security	• Adopts a life cycle approach to security management (planning, monitoring and reporting) • Greater focus on risk management approach • Clearer accountability for security and embedding security culture.
Information security	
• Complex classification system, leading to over classification and inaccurate handling of sensitive and security classified information • Insufficient focus on ICT and cyber security matters • Insufficient link to ISM	• Simplified classification of information. • Increased focus on cyber security matters. • Addresses inconsistency (and duplication) between the PSPF and ISM
Personnel security	
• Compliance approach that encourages passive and reactive approach to personnel security	• Strengthened provisions to mitigate against the insider threat • Highlights the importance of information sharing.

New PSPF policy and guidance documents

POLICY DOCUMENT	KEY CHANGES
1. Role of accountable authority	• Clearer articulation of the role of the accountable authority (entity heads) and of entities with a lead role in security policy or services such as the Attorney-General's Department • Greater focus on shared risks and impact of entity risks on others
2. Management structures and responsibilities	• Introduces a new Chief Security Officer role that expands on the Security Executive role in the previous PSPF. The CSO: o provides for more holistic oversight of entity security o aligns with recommendations of the Smith review • Provides greater flexibility in appointing security roles by removing mandatory security titles • Gives greater prominence to security culture
3. Security planning and risk management	• Enhances guidance on security risk management • Embeds a maturity focus throughout the planning, monitoring and reporting cycle
4. Security maturity monitoring	• Introduces a requirement for ongoing consideration and oversight of security; this supports the enhanced executive oversight in policies 1 and 2

POLICY DOCUMENT	KEY CHANGES
5. Reporting on security	• Replaces previous compliance reporting with reporting on security maturity • Provides greater nuance of reporting levels (Ad Hoc, Developing, Managing, Embedded) vs compliant/noncompliant • Allows entities to consider and report on what they are doing well and identify areas for improvement • Provides government with a better understanding of its whole-of-government protective security posture
6. Security governance for contracted goods and service providers	• No significant policy change • Enhanced guidance to support implementation, noting this is an ongoing area of security concern across government
7. Security governance for international sharing	• No significant policy change • More explicit guidance to support upcoming reforms to the Criminal Code related to espionage and international sharing of information
8. Sensitive and classified information	• Simplifies the existing classification system with a focus on: o Reflecting the value of all government information in line with the Archives Act by replacing the UNCLASSIFIED security classification with 'OFFICIAL' o Simplifying the confusing suite of dissemination limiting markers by consolidating previous markers (For Official Use Only - FOUO, Sensitive, Sensitive: Legal, and Sensitive: Personal) with a single marking of 'OFFICIAL: Sensitive' o Retaining the ability to categorise certain types of information and describe a right to access o Better reflecting the unique nature of cabinet material by establishing a special handling Cabinet caveat to replace the previous Sensitive: Cabinet DLM o Discontinuing the CONFIDENTIAL classification to align with international partners. This reform recognises the limited use of the classification across government • Given the scale of these reforms, there is extended implementation to 2020 and grandfathering of existing holdings of classified and DLM material information to avoid having to reclassify
9. Access to information	• No significant policy change • The policy more clearly articulates the link between personnel and information security
10. Safeguarding information from cyber threats	• Increases the prominence of cyber security matters in the PSPF. • Provides authority for ASD's Strategies to mitigate cyber security incidents by explicitly requiring entities to implement four of ASD's 'Essential eight' strategies: o application whitelisting o application patching o operating system patching o restricting administrative privileges
11. Robust ICT systems	• Provides policy authority for the ICT system accreditation process detailed in the ISM; this aligns with previous PSPF practice for accreditation of physical spaces and reflects the increased prominence of cyber security matters in the PSPF
12. Eligibility and suitability of personnel	• Consolidates previous employment screening and security clearance-related requirements, and policy guidance from various sources and streamlines guidance • Introduces a requirement for entities to verify a person's identification documents with the issuing authority by using the Document Verification Service • Clarifies roles and responsibilities in the supporting requirements • Improves guidance on informed consent • Provides definitions of key terms
13. Ongoing assessment of personnel	• Raises the importance of conducting annual security check • Strengthens provisions for assessing the ongoing suitability of security-cleared personnel
14. Separating personnel	• No significant policy change
15. Physical security for entity resources	• No significant policy change • Better integration between PSPF and ASIO technical notes
16. Entity facilities	• Retains existing 'zones' approach to physical security for entity facilities • Better integration between PSPF and ASIO technical notes