agilient
Security Risk & Resilience

INFORM · ASSESS · PROTECT

PSPF RELEASE 2026

Protective Security Policy Framework: what changed in Release 2026

PSPF Release 2026 took effect on 1 July 2026. It updates the Australian Government's mandatory protective security requirements across the six security domains, and the obligations reach the suppliers and contractors that serve government through contracts, deeds and panel agreements.

THE SIX SECURITY DOMAINS — WHAT RELEASE 2026 CHANGES

Governance and Risk

- A new mandatory requirement obliges entities to hold a policy prohibiting personnel from publicising their security clearance online.
- Expanded reporting of foreign ownership, control or influence, and more frequent CISO reporting, carried forward.
- The directions mechanism lets the Home Affairs Secretary act on a present risk at any time, not only at the annual release.

Information and Technology

- The Commonwealth Technology Standard applies when authorising systems to operate up to SECRET.
- Entities must develop a post-quantum cryptography transition plan and share risk assessments to a centralised capability.
- Hosting and gateway requirements are aligned to the updated standards; the standalone TikTok controls are retired.

Personnel and Physical

- Security awareness training must now cover foreign interference, espionage and the cultivation of personnel.
- Eligibility-waiver provisions for citizenship and checkable background are refined.
- A security risk assessment is required where personnel work in another entity's facilities; SCIF accreditation aligns to the National SCIF Accreditation Program.

WHO THIS APPLIES TO

Non-corporate Commonwealth entities
Compliance is mandatory under the PGPA Act 2013.

Corporate entities and companies
Apply the framework as better practice.

State and territory agencies
Apply it when holding Commonwealth classified material.

Suppliers and contractors
Bound where a contract, deed or panel agreement passes controls down.

Cleared individuals
Must not publicise a clearance or classified access online.

BY THE NUMBERS

6
Security domains: governance, risk, information, technology, personnel and physical.

01/07/2026
Date PSPF Release 2026 took effect.

Annual
The PSPF is reviewed and re-released each year against the current threat environment.

New
Mandatory requirement: a policy prohibiting online disclosure of security clearances.

WHAT TO DO NOW

- ✓ **Run a gap analysis.** Assess against all six domains, not only technology, and sequence remediation by risk.
- ✓ **Review contracts.** Confirm which PSPF controls flow down through contracts, deeds and panel agreements.
- ✓ **Plan the technology uplift.** Address the Commonwealth Technology Standard and a post-quantum cryptography transition plan.
- ✓ **Set the clearance policy.** Audit websites, biographies and social profiles, and remove statements naming individual clearances.
- ✓ **Update awareness training.** Cover foreign interference, espionage and the cultivation of personnel.
- ✓ **Ready your reporting.** Prepare evidence for the annual maturity self-assessment.

PSPF Release 2026 is a live obligation, not a document filed once. **Conformance increasingly shapes tender success and contract continuity** for suppliers to government.

agilient.com.au
PROTECTIVE SECURITY · PSPF · SECURITY RISK

Sources: Department of Home Affairs, PSPF Release 2026 — Summary of Changes and List of Requirements, protectivesecurity.gov.au. Figures point-in-time; verify before formal use. © 2026 Agilient Security Consulting.