info

The Administrative Arrangements Order (https://www.pmc.gov.au/sites/default/files/resource/download/aao-amendments-3-august-2023.pdf) of 3 August 2023 transferred responsibility for protective security policy, including the Protective Security Policy Framework, to the Department of Home Affairs from the Attorney-General's Department. These Machinery of Government (MOG) changes commenced on 4 August 2023.

Australian Government and international resources

There are a small number of Australian Government entities that provide information, services and advice that will help entities to implement the PSPF.

These include:

- Australian Security Intelligence Organisation
- Australian Cyber Security Centre
- Commonwealth Fraud Prevention Centre
- Australian Public Service Commission
- Department of Finance.

Australian Government protective security resources

GovTEAMS

The Protective Security Policy team in the Attorney-General's Department manages the protective security policy community on GovTEAMS. This online community provides a forum for Australian Government protective security practitioners and policy makers to share information and best practice. The site has an extensive publications library with information, designated for limited distribution, to facilitate implementing the PSPF.

Access to the GovTEAMS community is only available to government personnel. To request access, complete the website's 'Contact us (/node/496)' form.

ASIO Outreach

ASIO Outreach (https://www.blu.asio.gov.au/) is the principal interface between the Australian Security Intelligence Organisation (ASIO) and government and industry stakeholders. It provides information in a variety of ways, including:

- a subscriber-controlled website
- ASIO-hosted briefings
- face-to-face engagement
- joint government and industry forums.

These mechanisms aim to provide risk management government and industry decision-makers with the most current security intelligence and protective security advice.

This assists them to:

- recognise and respond to national security threats
- develop appropriate risk mitigation strategies
- provide informed briefings to executives and staff.

The ASIO Outreach (https://www.blu.asio.gov.au/user/register) website contains intelligence-backed reporting on the domestic and international security environment, drawn from ASIO's information holdings and expertise (including the multi-agency National Threat Assessment Centre, ASIO's protective security area (T4) and the Counter-Espionage and Interference Division) and some foreign intelligence partner agency reports.

Access to the website is free. To subscribe, visit the ASIO Outreach (https://www.blu.asio.gov.au/user/register) website.

Australian Cyber Security Centre (ACSC)

The Australian Cyber Security Centre (https://www.cyber.gov.au/) ACSC) is the Australian Government's lead on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and support the economic and social prosperity of Australia in the digital age.

It is responsible for policy guidance, specialised information security training and professional forums supporting government information security. Visit the ACSC website for information security resources, including the Strategies to Mitigate Cyber Security Incidents (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents-mitigation-details) and the Australian Government Information Security Manual (https://www.cyber.gov.au/acsc/view-all-content/ism).

Through the Australian Cyber Security Centre, the Australian Signals Directorate provides cyber security advice and assistance to Australian governments, businesses and individuals. The *Intelligence Services Act 2001 (https://www.legislation.gov.au/Latest/C2019C00018)* establishes the Australian Signals Directorate as the Commonwealth authority on the security of information.

Security Construction and Equipment Committee (SCEC)

The Security Construction and Equipment Committee (https://www.scec.gov.au/) is a standing inter-departmental committee responsible for the evaluation of security equipment for use by Australian Government departments and agencies. SCEC is also responsible for the SCEC Security Zone Consultant scheme, SCEC Approved Locksmith scheme, and SCEC endorsed Courier scheme. SCEC's equipment evaluation program and consultant, locksmith and courier schemes are managed by ASIO's T4 Protective Security (https://www.asio.gov.au/asio-t4-protective-security.html).

The Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner's (https://www.oaic.gov.au/) 3 primary functions – privacy, freedom of information and government information policy – are all relevant to implementing the PSPF. Their website includes information about the Australian Privacy Principles (https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles) and the Notifiable Data Breaches (https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme) scheme.

Australian Public Service Commission

The Australian Public Service Commission (https://www.apsc.gov.au/working-aps/integrity/integrity-resources/aps-values-code-conduct-and-employment-principles) provides advice and resources on a range of matters relating to the Australian Public Service and public sector workforce management. Its purpose is to position the APS workforce for the future, by shaping the APS workforce, modernising the employment framework, building workforce capability, and promoting integrity. The APSC has published *Handling Misconduct: a human resource manager's guide (https://www.apsc.gov.au/news-and-events/latest-news/handling-misconduct-human-resource-managers-guide)* to help APS agencies and employees understand misconduct processes in the Australian Public Service.

Commonwealth Fraud Control Framework

The Commonwealth Fraud Prevention Centre (https://www.counterfraud.gov.au/) is part of the Attorney-General's Department. It is responsible for coordinating fraud control policy. Fraud against the Commonwealth is a serious matter for all Australian Government departments and agencies, and the community. It prevents taxpayer dollars from reaching intended targets and affects the government's ability to deliver key services.

The Commonwealth Fraud Control Framework (https://www.counterfraud.gov.au/library/commonwealth-fraud-control-framework) outlines the Australian Government's requirements for fraud control. One of these is that government entities must put in place a comprehensive fraud control program that covers prevention, detection, investigation and reporting strategies.

Reports, audits and inquiries

The Australian National Audit Office), as well as some parliamentary committees and Australian Government entities, conduct audits and inquiries, and produce reports with findings relevant to protective security.

ANAO audit reports

The ANAO's annual work program often includes performance audits on the implementation of protective security policy in selected government agencies. Reports of past audits are available on the ANAO (https://www.anao.gov.au/pubs/performance-audit) website, which can be searched by key words, sector or year. Recent performance audit reports that are relevant to the implementation of the PSPF include:

- Cyber Security Strategies of Non-Corporate Commonwealth Entities (https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities#:~:text=The%20objective%20of%20the%20audit,cyber%20policy%20and%20operational%20entities.) (ANAO Report No. 32 of 2020-21) – Published 19 March 2021
- Cyber Resilience (https://www.anao.gov.au/work/performance-audit/cyber-resilience-2017-18) (ANAO Report No. 53 of 2017–2018) – Published 28 June 2018
- Mitigating Insider Threats through Personnel Security (https://www.anao.gov.au/work/performance-audit/mitigating-insider-threats-through-personnel-security) (ANAO Report No. 38 of 2017-2018) – Published 11 May 2018

Check the ANAO's annual work program (https://www.anao.gov.au/work-program) for information on upcoming performance audits.

Joint Committee of Public Accounts and Audit

The Joint Committee of Public Accounts and Audit (JCPAA) examines all Auditor-General reports that are tabled in each House of the Parliament. This includes performance audit reports. Find out more about the role of the JCPAA on the Parliament

of Australia (https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Role_of_the_Committee) website.

International resources

Our international partners have a range of resources that may be useful for entities implementing the PSPF. This list is not exhaustive – if you use other international resources please contact us (/node/496) and provide details so that we can keep this list up to date.

Canada

Treasury Board of Canada Secretariat

The Treasury Board of Canada Secretariat (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16578) is responsible for Canadian protective security policies, directives, standards and guidelines.

Royal Canadian Mounted Police

The Royal Canadian Mounted Police (http://www.rcmp-grc.gc.ca/physec-secmat/pubs/index-eng.htm) provide policy and practical advice to Canadian agencies on physical security.

New Zealand Security Intelligence Service

The New Zealand Security Intelligence Service (https://www.nzsis.govt.nz/) advises the NZ Government on matters relating to New Zealand's security. They are responsible for the Protective Security Requirements (http://www.protectivesecurity.govt.nz/), the New Zealand equivalent of the PSPF.

United Kingdom

UK Cabinet Office

The UK Cabinet Office (https://www.gov.uk/government/collections/government-security) maintains protective security policies for the UK Government.

This includes the UK Security Policy Framework (https://www.gov.uk/government/collections/government-security), which provides central internal protective security policy and risk management for UK Government departments and associated bodies.

Centre for the Protection of National Infrastructure resources

The Centre for the Protection of National Infrastructure (http://www.cpni.gov.uk/) provides integrated security advice (combining information, personnel and physical) to organisations that make up the UK national infrastructure. CPNI advice helps to reduce the vulnerability of the UK national infrastructure to terrorism and other threats to national security.

Their advice covers security planning, physical security, personnel security and cyber security/information assurance.

The CPNI YouTube channel (https://www.youtube.com/user/UKCPNI) contains short videos that can be used to assist in agency security awareness training.

United Kingdom Security Vetting

United Kingdom Security Vetting (https://www.gov.uk/government/organisations/united-kingdom-security-vetting) is the single government provider of national security vetting. They are responsible for security vetting to enable the UK government to protect its citizens and provide vital public services, by understanding and managing security risks.

United States of America

Department of Homeland Security – Cybersecurity and

Infrastructure Security Agency (CISA)

CISA (https://www.cisa.gov/about-cisa) works with partners at all levels of the US Government, and from the private and non-profit sectors, to share information and build greater trust to make US cyber and physical infrastructure more secure.

Defense Personnel and Security Research Center (PERSEREC)

Researchers at PERSEREC (http://www.dhra.mil/perserec/):

- conduct applied research and development to improve personnel suitability, security, and reliability policy and practice
- conduct long-term programmatic research and development for the human resource management, security, and intelligence communities
- provide quick-response studies and analyses in support of policy formation and systems operation
- disseminate research information to policymakers and practitioners
- develop innovative systems, tools, and job aids for policymakers, managers, and practitioners concerned with personnel suitability, security, and reliability.