PSPF Direction 002-2024

Technology Asset Stocktake

PSPF Direction 002-2024 requires Australian Government entities to identify and actively manage the risks associated with vulnerable technologies they manage, including those they manage for other entities.

Further information about this Direction is detailed in Policy Explanatory Note 02/24 – Managing the risk of vulnerable technology assets.

On advice from the Protective Security Board, there is a pressing need for Australian Government entities to harden their technology management practices, and to proactively seek out vulnerabilities that may be present on Australian Government networks.

By PSPF Reporting Period 2024-25 (June 2025) all entities **must**:

1. Conduct a technology asset[1] stocktake on all internet-facing systems or services[2] to identify all technology assets managed by, or on behalf of, the entity. The stocktake must capture for each asset:
    - Manufacturer, supplier and provider
    - Outsourced manager, where applicable
2. Develop a Technology Security Risk Management Plan for all internet-facing systems or services, as part of the entity's overall Security Plan. The plan must include:
    - Approach to implement Technology Lifecycle Management practices in accordance with PSPF Policy 11: Robust ICT Systems, C1 and Figure 1
    - Controls to mitigate identified cyber security vulnerabilities
    - Controls to mitigate Foreign Ownership, Control or Influence risks associated with technology supply chains
    - Processes to maintain continuous visibility and monitoring of an entity's resource and technology footprint

[1] For the purposes of this Direction, a technology asset is defined as *any hardware, software or information system, platform, mobile application or as-a-service offering, which stores, processes, transmits or transforms official or security classified information belonging to, or utilised by, the Australian Government.*

[2] For the purposes of this Direction, an internet-facing system or service is directly accessed by untrusted or unknown entities over the internet, as opposed to a service or system accessed solely through the entity's internal network.

Entities **must** submit their stocktake and Technology Security Risk Management Plans to the Department of Home Affairs' Government Cyber and Protective Security Branch at PSPF@homeaffairs.gov.au (up to PROTECTED), or call 02 5127 9999 for advice on reporting above PROTECTED.

For further information, contact PSPF@homeaffairs.gov.au or 02 5127 9999.

Stephanie Foster

Stephanie Foster PSM
Secretary
Department of Home Affairs
5 July 2024