

Verizon offering for recent Protective Security Directions under PSPF

verizon business

Directions update

The Secretary of the Department of Home Affairs has issued three mandatory Protective Security Directions under the Protective Security Policy Framework (PSPF) to government entities to manage cybersecurity risks to the Australian Government.

Direction 001-2024 on managing foreign ownership, control or influence (FOCI) risks in technology assets

PSPF Direction 001-2024 requires Australian Government entities to identify indicators of FOCI risk as they relate to procurement and maintenance of technology assets and appropriately manage and report those risks.

Direction 002-2024 on 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.

Direction 003-2024 on Supporting Visibility of the Cyber Threat

PSPF Direction 003-2024 requires Australian Government entities using threat intelligence sharing platforms to share cyber threat information with the Australian Signals Directorate (ASD).

How Verizon can help

Verizon cybersecurity consulting teams can help government entities to comply with the recent Protective Security Directions under PSPF in the following ways:

- Verizon will perform a Network Discovery exercise using both automated and manual processes to develop an inventory of existing internal and external facing network environments - it will include details about all technology assets (hardware, software or information system, platform, mobile application or as-a-service offering, etc.) including manufacturer, supplier and end-of-life information.
- A Risk Assessment will be performed by expert Verizon consultants, which can include a vulnerability assessment of internet facing devices, penetration testing, as well as an assessment of potential FOCI risks identified during the procurement process of technology assets.
- Verizon will assist in developing and implementing a process to identify and manage potential FOCI risks when undertaking procurement of technology assets.
- Verizon security practitioners will work with government entities to help develop, update and maintain the Security Risk Management Plan to include the following -
- Technology Lifecycle Management practices in accordance with PSPF
- Controls to mitigate cybersecurity vulnerabilities
- Controls to mitigate FOCI risks associated with technology supply chains
- Processes to maintain continuous visibility and monitoring of an entity's resource and technology footprint
- Share analysis from Verizon's Data Breach Investigations Report, of data breaches and cybersecurity incidents worldwide, including insights into trends, attack patterns, and the effectiveness of security measures

Why Verizon

As a leading cybersecurity and connectivity provider trusted by 98% of Fortune 500 companies and more than half of Australia's Federal Government entities, Verizon stays ahead of rapidly evolving cyber threats by processing billions of security events annually. Our global security operations centres analyse these threats, and we conduct forensic investigations worldwide, sharing our expertise through industry-recognised content like the annual Data Breach Investigations Report. Unlike other security service providers, we are a global hyperscaler with extensive experience in managing risks and incidents, delivering practical security solutions. With 25 years of dedicated investment and expertise in Australia, we prioritise the long-term success of organisations across all industries.

verizon business