



Australian Government

Department of Home Affairs
Protective Security Policy Framework

OFFICIAL

PSPF Direction 003-2024

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.

On advice from the Protective Security Board, there is a pressing need for Australian Government entities to share cyber threat information with the Australian Signals Directorate.

By PSPF Reporting Period 2023-24 (July 2024) all entities **must**:

1. Participate in Australian Signals Directorate's Cyber Security Partnership Program.
2. Advise Australian Signals Directorate of any cyber threat hunting capability employed by the entity.
3. Connect to the Australian Signals Directorate's Cyber Threat Intelligence Sharing (CTIS) platform.
4. Continue to report cyber security incidents to the Australian Signals Directorate in accordance with PSPF Policy 5: Reporting on security, Requirement 2.

Entities **must** submit their response 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 PSM

Secretary

Department of Home Affairs

5 July 2024

OFFICIAL