Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

AusNOG 2024

Cyber Security for Critical Infrastructure and Government

Gregory Smith, A/g Assistant Secretary
Risk Assessment Branch
Cyber and Infrastructure Security Centre
Department of Home Affairs

6 September 2024

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

The Australian Government's approach to critical infrastructure security regulation

- Secure and resilient critical infrastructure is vital to the functioning of Australian society.
- The telecommunications sector, including ISPs, plays an essential role in enabling economic and social activity in Australia and ensuring the availability and connectivity of other critical assets.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Timeline of security regulation:

2003: **Trusted Information Sharing Network** established as the primary engagement mechanism for business and government information sharing and resilience building initiatives on critical infrastructure.

TISN

2017: **Critical Infrastructure Centre** established within the **Department of Home Affairs** in response to the complex and evolving national security risks to critical infrastructure, including sabotage, espionage and foreign interference.

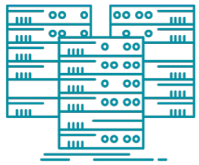
Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security of Critical Infrastructure Act 2018 (SOCI Act)

- Introduced to create a framework for the regulation and protection of Australia's 11 critical infrastructure sectors.

Positive Security Obligations



Register of Critical Infrastructure Assets

Mandatory Cyber Security Incidents Reporting

Critical Infrastructure Risk Management Program

Enhanced Cyber Security Obligations – for Systems of National Significance

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Part 14 of the *Telecommunications Act 1997*

- In 2018, Part 14 of the *Telecommunications Act 1997* was introduced to better manage the national security risks of sabotage, espionage and foreign interference to Australia's telecommunications networks and facilities.
- Key obligations:
  - **Security obligation:** Carriers, carriage service providers (C/CSPs) and carriage service intermediaries must do their best to protect their networks and facilities they own, operate or use, from unauthorised access or interference.
  - **Notification obligation:** Carriers and nominated carriage service providers are required to notify the Government of proposed changes to their networks and services that may have a material adverse effect on their ability to protect their networks.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

5G Security Guidance

- In 2018, the Australian Government issued Security Guidance to Australian telecommunications carriers on their obligations to protect 5G networks.

- The Government considers that the involvement of vendors who are likely to be subject to extrajudicial direction from a foreign government, in a way that conflicts with Australian law, may risk failure by a carrier to adequately protect their 5G networks from unauthorised access or interference.

- The Department is currently working on updating this guidance.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Cyber and Infrastructure Security Centre (CISC)

- Facilitates an all-hazards critical infrastructure resilience regime enabled by strong focus on cyber security, in partnerships with governments, industry and the broader community.

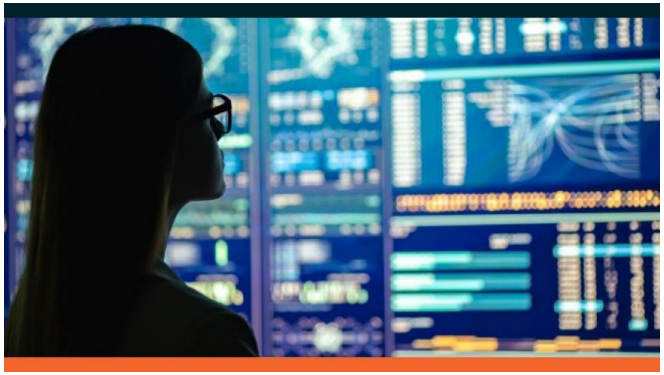
- Actively assists Australian critical infrastructure owners and operators to understand the risk environment and meet their regulatory requirements.

- Direct regulatory responsibility for aviation transport security, maritime transport and offshore facility security as well as telecommunications security.

Australian Government
Department of Home Affairs

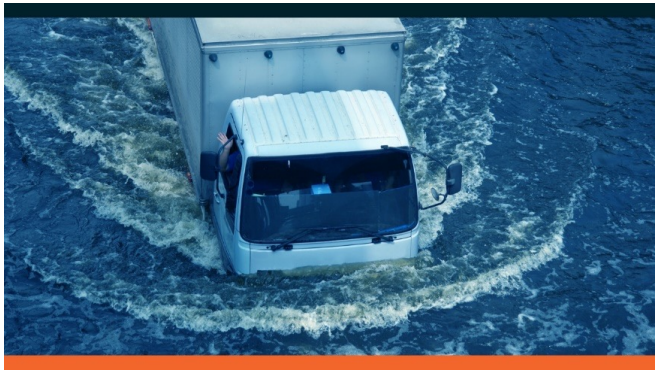
CYBER AND INFRASTRUCTURE SECURITY CENTRE

All-hazards approach to CI security:



Cyber and information security hazards

Personnel hazards



Supply chain hazards

Physical security and natural hazards

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Ongoing reforms

- The Department is progressing reforms to amalgamate and enhance security obligations for telecommunications under the SOCI Act.
- The Department, in coordination with DITRDCA, has been leading a body of work to consult with industry stakeholders on the proposed reforms, incorporating industry views to help shape the proposed provisions.
- This engagement has been conducted through the Australian Telecommunications Security Reference Group (ATSRG).

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

The National Office for Cyber Security (NOCS)

- Established in May 2023 to support the **National Cyber Security Coordinator** in leading consequence management for national cyber incidents, whole of government cyber incident preparedness efforts and the strengthening of Commonwealth cyber security capability.

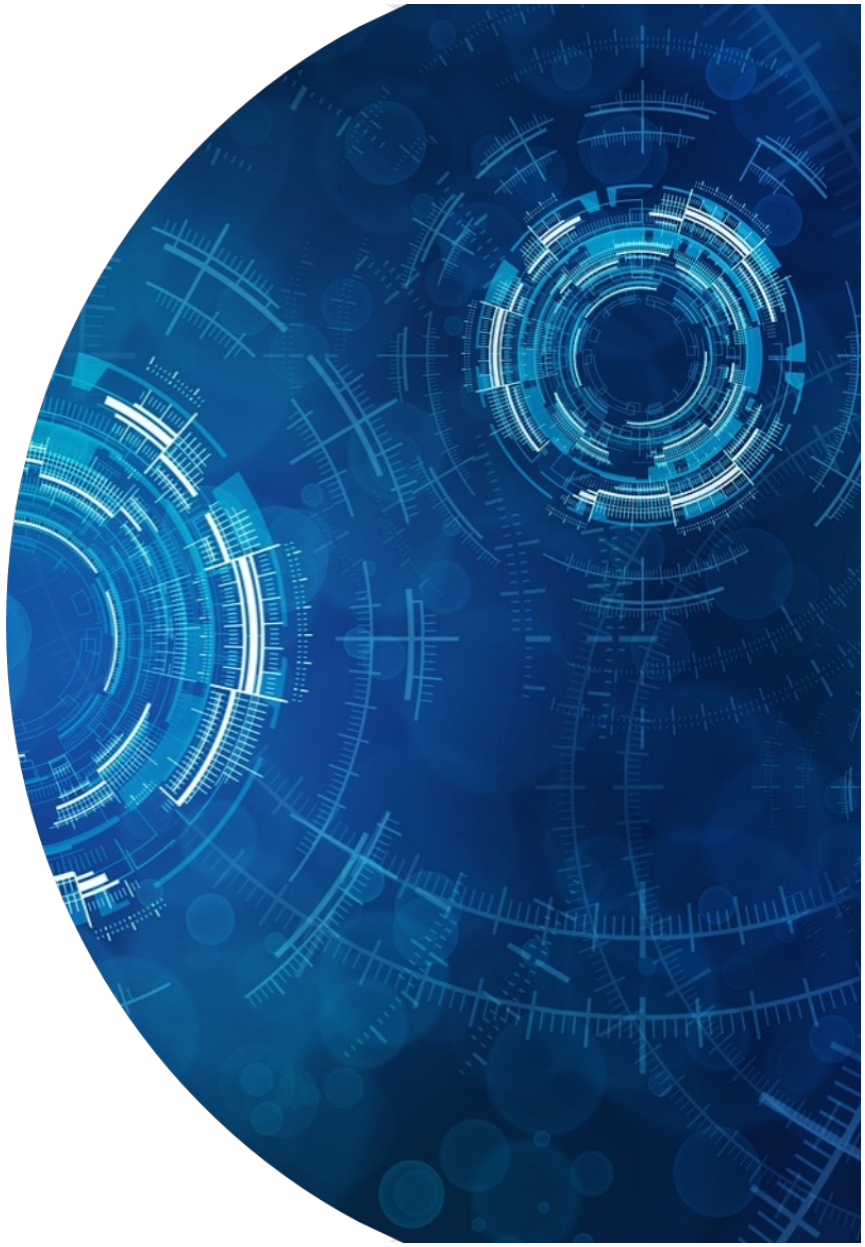
Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

The current state of cybersecurity

- **ASD's Australian Cyber Security Centre's (ACSC)** Annual Cyber Threat Report (2022-23) states: the ACSC received nearly 94,000 cybercrime reports, an increase of 23 percent from the previous financial year; and responded to 143 cyber security incidents related to critical infrastructure.

- CI faces increased susceptibility to attack by nation states, state-sponsored actors, issue motivated groups, or extremist groups seeking to advance their own interests, as well as from natural hazards.



Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Volt Typhoon

- Publicly reported Chinese hacking network had been pre-positioning inside US critical infrastructure, possibly for a number of years.

- It is likely that Volt Typhoon was part of a larger effort to infiltrate western critical infrastructure, including naval ports, internet service providers, communication services and utilities.

- ASD's ACSC assesses Australian critical infrastructure could be vulnerable to similar activity from PRC state-sponsored actors.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Importance of collaboration between industry and government

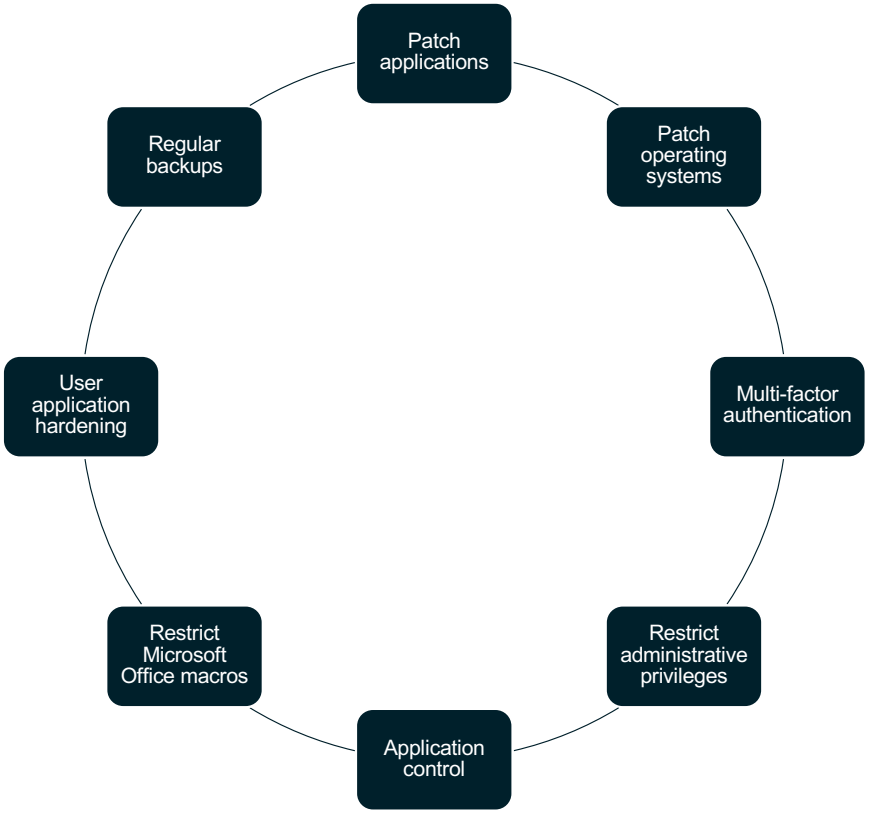
- The CISC works closely with National Intelligence Community partners to share threat and risk information, and to relay releasable risk assessment advice to industry.
- ACSC was established in 2014 as the lead operational agency for responding to cyber incidents. ACSC seeks to improve Australia's national cyber resilience through:
  - Operating the Australian Cyber Security Hotline
  - Publishing vulnerability alerts, technical advice, advisories and notifications
  - Cyber threat monitoring and intelligence sharing
  - Conducting exercises and uplift activities

ACSC Australian Cyber Security Centre

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

The Essential Eight



Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

ISPs are crucial in providing the first line of defence against cyber-threats through their ability to monitor and filter traffic passing over a network.

It is important that ISPs actively ensure that managed service providers (MSPs) and telecommunications providers themselves are prioritising the security of their networks.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Contacts/Resources

Cyber & Infrastructure Security Centre - https://www.cisc.gov.au/

Request to join TISN- https://www.cisc.gov.au/resources/online-forms/request-to-join-tisn

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Questions