Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Critical Infrastructure Risk Management Program

Sam Grunhard
Cyber and Infrastructure Security Centre
Department of Home Affairs

28 July 2023

OFFICIAL

Critical Infrastructure Risk Management Program (CIRMP)

- CIRMP uplifts the security and resilience of critical infrastructure assets.

- A CIRMP needs to identify and manage ‘material risks’ of ‘hazards’ that could have a ‘relevant impact’ on the ongoing operation of an asset.

Assets the CIRMP obligation applies to

Sector	Asset Class
Communications	Broadcasting
	Domain Name Systems
Data Storage or Processing	Data Storage or Processing
Energy	Electricity
	Energy Market Operator
	Gas
	Liquid Fuels
Financial Services and Markets	Payment Systems
Food and Grocery	Food and Grocery
Health Care and Medical	Hospitals
Transportation	Freight Infrastructure
	Freight Services
Water and Sewerage	Water

End of the CIRMP grace period

- By **18 August 2023**, existing entities must have a process or system that ensures material risks are identified and managed.

- New CI assets have six months to comply from the date they become a CI asset.

- Entities have until 18 August **2024** to meet the cybersecurity requirements of the rules.

Hazard: Cyber and Information Security

- Entities must have a process or system in place for identifying and mitigating cyber and information security hazards.

- Examples of cyber security hazards include:
  - Phishing
  - Malware
  - Credential harvesting
  - Denial-of-Service (DoS)
  - Distributed-Denial-of-Service (DDoS)

- <u>Reminder</u>: Entities have until 18 August **<u>2024</u>** to have a cyber security framework implemented, but voluntary compliance earlier will lower your risk.

Hazard: Supply Chains

Entities should consider supply chain risk in the context of:

- Unauthorised access or interference with their asset;
- Disruption to their critical supplies, software, components, or services.

Reminder: The CIRMP Rules are principles based – there is no prescriptive definition of a ‘supply chain’ in the Rules.

Hazard: Physical and Natural

The CIRMP must include a process to manage material risks posed by natural elements to the physical components of the asset.

- **Physical security hazards could include:**
    - Unauthorised access;
    - Sabotage or interference;
    - Malicious or accidental damage.

- **Natural hazards could include:**
    - Bushfires;
    - Floods;
    - Cyclones;
    - Biological hazards (such as a pandemic)

Hazard: Personnel

Responsible entities are required to manage any risks posed by 'critical workers' who have access to, or control over, critical components for the asset.

'Critical worker' has a specific meaning under the Rules.

The definition is not intended to apply to an entity's entire workforce, but may involve workers in the following areas:

- Information Security
- Control room operators
- IT administrators
- Support staff with access to secure areas.

A background check is one way to manage personnel risk.

AusCheck

- AusCheck background checks include a national security assessment by ASIO; this is not available from private sector background checking providers.

- From 1 July 2023, the cost of an AusCheck background check is $136.

- For specific inquiries relating to the AusCheck background checking scheme, please see - https://www.auscheck.gov.au

Protected Information

Provisions relating to the protection of certain information are intended to:

- Prevent the malicious use of sensitive data;
- Safeguard operational information;
- Prevent exploitation of vulnerabilities.

These provisions are **not intended** to limit or impede:

- the sharing of information with Government or with regulators;
- the ability of other regulators to carry out their functions;
- an organisation’s ability to respond to an incident.

Entities can disclose information for purposes including:

- Performing a function or duties under the SOCI Act
- Complying with Australian law.

Compliance

- Responsible entities must submit a Board approved-Annual Report within 90 days of the end of each Australian financial year.

- Therefore, the first Annual Report is due by **28 September 2024.**

- We are accepting voluntary reporting for the 2022/2023 Financial Year.

- For voluntary reporting this FY, Annual Reports can be submitted:
  - via web form: https://www.cisc.gov.au/resources-and-contact-information/forms/rmp-approval
  - or via email: enquiries@cisc.gov.au

Q&A

Further Information

Contact us:

- **Website:** www.cisc.gov.au
- **Email:** CI.Reforms@homeaffairs.gov.au & enquiries@cisc.gov.au
- **Trusted Information Sharing Network (TISN):** CIR@homaffairs.gov.au
- **AusCheck:** AusCheck.CI@homeaffairs.gov.au

- **Twitter:** twitter.com/CISC_AU
- **LinkedIn:** linkedin.com/showcase/cisc-au/