Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

The enhanced critical infrastructure risk management program – a snapshot

This guidance provides responsible entities subject to the enhanced critical infrastructure risk management program an overview of the arrangements under the *Security of Critical Infrastructure Act 2018* (SOCI Act). This document provides general guidance and responsible entities should familiarise themselves with the *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (CIRMP Rules).*

Part 2A of the SOCI Act requires certain responsible entities to adopt, maintain and comply with a critical infrastructure risk management program. The specifications for what must be included in the entity's CIRMP are provided in the *CIRMP Rules.*

The *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026* (enhanced CIRMP Rules) commenced on 10 June 2026. The enhanced CIRMP builds on the baseline requirements of the CIRMP Rules.

Who must comply with the enhanced CIRMP Rules

The enhanced CIRMP Rules apply to responsible entities that own or operate the following asset subclasses:

- Critical broadcasting assets
- Critical domain name systems
- Critical electricity assets
- Critical energy market operator assets
- Critical freight infrastructure assets
- Critical freight services assets
- Critical gas assets
- Critical liquid fuel assets
- Critical water asset

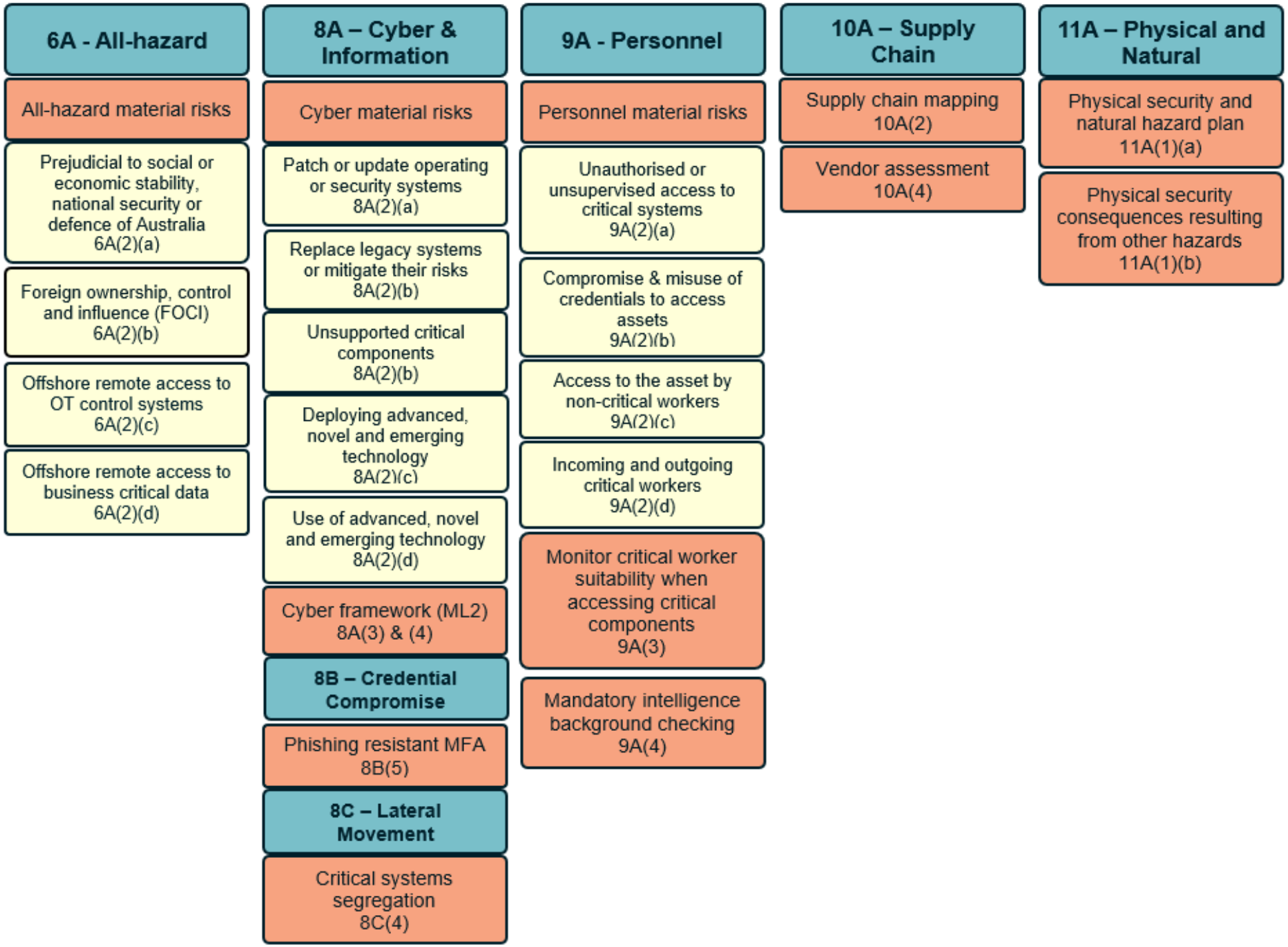
Compliance grace periods

For assets that were critical infrastructure (CI) assets prior to 10 June 2026 and are subject to the enhanced CIRMP Rules, responsible entities must comply by these dates:

New material risks	Sections 6A, 8A(2) and 9A(2)	**10 June 2027**
All other measures	8A (other than subsection 8A(2)), 8B, 8C, 9A, (other than subsection 9A(2)), 10A and 11A	**10 June 2028**

Annual reporting

Responsible entities do not need to provide any information about the enhanced material risks or measures in the 2025-26 reporting period (1 July 2026 – 28 September 2026).


6A - All-hazard
All-hazard material risks
Prejudicial to social or economic stability, national security or defence of Australia 6A(2)(a)
Foreign ownership, control and influence (FOCI) 6A(2)(b)
Offshore remote access to OT control systems 6A(2)(c)
Offshore remote access to business critical data 6A(2)(d)
8A – Cyber & Information
Cyber material risks
Patch or update operating or security systems 8A(2)(a)
Replace legacy systems or mitigate their risks 8A(2)(b)
Unsupported critical components 8A(2)(b)
Deploying advanced, novel and emerging technology 8A(2)(c)
Use of advanced, novel and emerging technology 8A(2)(d)
Cyber framework (ML2) 8A(3) & (4)
8B – Credential Compromise
Phishing resistant MFA 8B(5)
8C – Lateral Movement
Critical systems segregation 8C(4)
9A - Personnel
Personnel material risks
Unauthorised or unsupervised access to critical systems 9A(2)(a)
Compromise & misuse of credentials to access assets 9A(2)(b)
Access to the asset by non-critical workers 9A(2)(c)
Incoming and outgoing critical workers 9A(2)(d)
Monitor critical worker suitability when accessing critical components 9A(3)
Mandatory intelligence background checking 9A(4)
10A – Supply Chain
Supply chain mapping 10A(2)
Vendor assessment 10A(4)
11A – Physical and Natural
Physical security and natural hazard plan 11A(1)(a)
Physical security consequences resulting from other hazards 11A(1)(b)

For further information please contact us at:

ci.strategy.guidance@homeaffairs.gov.au

Australian Government
Department of Home Affairs

CRITICAL
INFRASTRUCTURE SECURITY
CENTRE