Consultation on the Exposure Draft of the Critical Infrastructure Risk Management Program Rules

The Minister for Home Affairs is opening consultation on the Exposure Draft of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (Exposure Draft of the CIRMP Rules) (**Attachment A**) under the *Security of Critical Infrastructure Act 2018* (SOCI Act) and is seeking submissions on the proposed changes from 30 March 2026 to 1 May 2026.

Engagement to support the Exposure Draft of the CIRMP Rules

The Department of Home Affairs (the Department) will hold a public town hall and engage through the Trusted Information Sharing Network throughout the consultation period. Details of these engagements will be posted on the Department's website and on the CISC website.

Providing a submission to the Minister for Home Affairs

Written submissions are invited on the Exposure Draft of the CIRMP Rules. All submissions will be provided to the Minister for Home Affairs for consideration. Under section 30ABA of the SOCI Act, the Minister must publish on the Department's website the Exposure Draft of the Rules and invite submissions for a period no shorter than 28 days.

Feedback may be provided on any aspect of the Exposure Draft, including their design, implementation, considerations, sector impacts, or alternative options. As part of this Exposure Draft period, we are also seeking your specific advice on key wording of certain provisions. These will be marked in italics and brackets in **Attachment A**.

The Department will publish all submissions unless they are marked as confidential. Respondents should clearly identify any information in their submission that is protected under the SOCI Act, to enable appropriate handling. The Department requests that submissions are provided by 1 May 2026 and are provided to the submissions portal on the Department's website.

Background

Between 9 December 2025 and 13 February 2026, the Department consulted on the Enhancing the CIRMP Rules Consultation Paper (Consultation Paper). The proposals build on the existing obligations of the CIRMP Rules across all hazards. They remain principles-based obligations and the 'as far as reasonably practicable principles' apply.

During this period, the Department received over 60 submissions and engaged over 1900 individuals in a variety of consultation activities including:

- two public townhalls,
- two Trusted Information Sharing Network (TISN) briefings, and
- five TISN impact analysis sessions.

Submissions were overall broadly supportive of the measures in principle. Specific feedback was balanced, with some concerns surrounding implementation. Feedback from the consultation period, as well as early co-design through the TISN was considered when drafting the Exposure Draft of the CIRMP Rules. The Department's response to submission feedback and any changes based on advice provided are highlighted at **Attachment B**.

A summary of the consultation conducted is below:

Engagement summary: 9 December 2025 – 13 February 2026	
Total number of online engagements (industry and all levels of government)	11
Total number of attendees at online engagements	1910
TISN engagements	7
Total number of attendees at TISN engagements	1652
Public online engagements	2
Total number of attendees at public online townhalls	234
Targeted engagement with utility regulators across all states	2
Total number of attendees of utility regulators across all states	24

Overview of all engagements: 9 December 2025 – 13 February 2026	
Date	**Engagement**
12 December 2025	Enhanced CIRMP Public Townhall
17 December 2025	TISN Cross Sector Townhall: Enhanced CIRMP
18 December 2025	TISN Cross Sector Townhall: Impact Analysis Enhanced CIRMP Review
21 January 2025	Discussion with Australian Energy Regulators
27 January 2026	Enhanced CIRMP Public Townhall
29 January 2026	Impact Analysis Deep Dive – Water and Sewerage TISN Sector Group
29 January 2026	Impact Analysis Deep Dive – Energy TISN Sector Group
30 January 2026	Impact Analysis Deep Dive – Land Transport TISN Sector Group
30 January 2026	Impact Analysis Deep Dive – Communications TISN Sector Group
4 February 2026	Enhanced CIRMP TISN Townhall
5 February 2026	Discussion with Water Regulators

Attachment A – Amendments to the CIRMP Rules

Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026

I, Tony Burke, Minister for Home Affairs, make the following rules.

Dated 2026

Tony Burke **DRAFT ONLY—NOT FOR SIGNATURE**
Minister for Home Affairs

Contents

1 Name

This instrument is the *Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument.	The day after this instrument is registered.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 61 of the *Security of Critical Infrastructure Act 2018*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Schedule 1—Amendments

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023

1 Section 3 (after paragraph (e) of the note under the heading)

Insert:

(ea) managed service provider;

2 Section 3

Insert:

AGSVA means the Australia Government Security Vetting Agency.

baseline CIRMP requirement means any requirement specified in Part 2 of this instrument for the purpose of paragraph 30AH(2)(b) of the Act, other than an enhanced CIRMP requirement.

critical system means any system, vital operational technology, enabling systems and critical components vital to the delivery of a CI asset's function, or the compromise or degradation of which could [*reasonably*] have a relevant impact on the asset.

enhanced CIRMP requirement means a requirement specified in subsection 4A(5).

FOCI means foreign ownership, control or influence.

maximum tolerable outage means the maximum period of time for which a critical system, service or another thing for the CI asset can be unavailable without *[unreasonably]* disrupting the ongoing availability of the CI asset.

offshore critical worker means a critical worker who is located outside of Australia *[and Australian waters]*.

onshore critical worker means a critical worker who is in Australia *[, including in Australian waters]*.

3 Subsection 4(4)

Insert:

(aa) the CIRMP Rule asset is not an asset specified in subsection 4A(1); and

4 After subsection 4(4) (note)

Repeal the note, substitute:

Example: Where an entity is the responsible entity for two types of assets – one is an asset specified in subsection 4A(1) of this instrument (*subsection 4A(1) asset*), and the other is a relevant critical infrastructure asset, that is specified in another instrument. The entity will need to comply with the requirements in the other instrument for the relevant critical infrastructure asset, while complying with the requirements in Part 2 of this instrument for the subsection 4A(1) asset.

Example: Where an entity is the responsible entity for two types of assets – one being an asset that is not specified in subsection 4A(1) (*baseline asset*), and the other is a relevant critical infrastructure asset that is specified in another instrument. The entity applies the requirements in the other instrument to the baseline asset as if that asset were the relevant critical infrastructure asset. If the entity complies with the requirements in the other instrument for both assets, it is taken to have complied with the requirements in this instrument.

5 After section 4

Insert:

4A Application of enhanced CIRMP requirements

Asset classes subject to enhanced CIRMP requirements

(1) For the purpose of paragraph 30AH(2)(b) of the Act, the following CI assets are specified to be subject to enhanced CIRMP requirements:

(a) a critical broadcasting asset;

(b) a critical domain name system;

(c) a critical electricity asset;

(d) a critical energy market operator asset;

(e) a critical freight infrastructure asset;

(f) a critical freight services asset;

(g) a critical gas asset;

(h) a critical liquid fuel asset; and

(i) a critical water asset.

Note: Requirements specified under paragraph 30AH(1)(c) of the Act may relate to one or more specified CI assets.

Enhanced CIRMP requirements

(2) For the purposes of paragraph 30AH(2)(b) of the Act, the requirements specified in subsection (5) for paragraph 30AH(1)(c) and subsections 30AKA (1), (3) and (5) of the Act, apply to a CI asset that is:

(a) specified in subsection (1); or

(b) covered by paragraph 30AB(1)(b) of the Act.

(3) A CIRMP for a responsible entity of a CI asset that is specified in subsection (1) must comply with both enhanced CIRMP requirements and baseline CIRMP requirements.

(4) To the extent that any inconsistency may arise between a baseline CIRMP requirement and an enhanced CIRMP requirement, the responsible entity must comply with the enhanced CIRMP requirement.

(5) For the purpose of subsection (2), the matters specified in the following provisions are enhanced CIRMP requirements:

(a) section 6A;

(b) section 8A;

(c) section 9A;

(d) section 10A;

(e) section 11A.

Grace periods

(6) For the purposes of subsection 30AB(3) of the Act, the following provisions do not apply to a CI asset specified in subsection (1) during the period:

(a) for section 6A:

(i) for an asset that is a CI asset before the commencement of *[this subsection / name of amending instrument]*—beginning when the asset becomes a CI asset and ending at the end of the last day of the period of 6 months after the commencement of this subsection;

(ii) for an asset that becomes a CI asset on or after the commencement of *[this subsection / name of amending instrument]*—beginning when the asset first becomes a CI asset and ending at the end of the last day of the period of 6 months after the asset has become a CI asset;

(b) for subsections 8A(2) and 9A(2) and sections 10A and 11A:

(i) for an asset that is a CI asset before the commencement of *[this subsection / name of amending instrument]*—beginning when the asset becomes a CI asset and ending at the end of the last day of the period of 18 months after the commencement of this subsection;

(ii) for an asset that becomes a CI asset on or after the commencement of *[this subsection / name of amending instrument]* —beginning when the asset first becomes a CI asset and ending at the end of the last day of the period of 18 months after the asset has become a CI asset;

(c) for section 8A, other than subsection 8A(2), and for section 9A, other than subsection 9A(2):

(i) for an asset that is a CI asset before the commencement of *[this subsection / name of amending instrument]* —beginning when the asset becomes a CI asset and ending at the end of the last day of the period of 24 months after the commencement of this subsection;

(ii) for an asset that becomes a CI asset on or after the commencement of *[this subsection / name of amending instrument]* —beginning when the asset first becomes a CI asset and ending at the end of the last day of the period of 24 months after the asset has become a CI asset.

6 After section 6

Insert

6A Material risks—enhanced requirements

For the purposes of paragraph 30AH(1)(c) of the Act, a responsible entity for a CI asset specified in subsection 4A(1) must consider the following material risks in the CIRMP:

(a) any impairment of the CI asset's functions that could prejudice the social stability, economic stability, national security or defence of Australia;

(b) the *[potential/possible risk of]* compromise or impairment of the functions of the CI asset as a result of, or in connection with FOCI.

7 After section 8

Insert:

8A Cyber and information security hazards—enhanced requirements

(1) For paragraph 30AH(1)(c) of the Act, subsections (2), (3), (4), (5) and (8) of this section specify enhanced requirements in relation to cyber and information security hazards.

(2) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process in the entity's CIRMP to—so far as it is reasonably practicable to do so—minimise or eliminate *[all of]* the following material risks:

(a) failure to replace or update unsupported software, hardware and other critical components in a timely manner;

(b) failure to patch or update operating or security systems in a timely manner;

(c) failure to replace legacy systems, or adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued;

(d) deployment of advanced, novel and emerging technology;

(e) use of advanced, novel and emerging technology against the asset, in a manner that could prejudice the social stability, economic stability, national security or defence of Australia;

(f) offshore remote access to operational technology control systems;

(g) offshore remote access to business critical data.

(3) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the CIRMP in order to:

(a) comply with a framework contained in a document specified in column 1 of an item in the following table as in force from time to time; and

(b) meet any conditions mentioned in column 2 of the same table item in relation to the framework specified in column 1 of the item.

Item	Column 1 Document	Column 2 Condition
1	Australian Standard AS ISO/IEC 27001:2023	
2	*Essential Eight Maturity Model* published by the Australian Signals Directorate	Meet maturity level two as indicated in the document
3	*The NIST Cybersecurity Framework (CSF) 2.0* published by the National Institute of Standards and Technology of the United States of America.	
4	*Cybersecurity Capability Maturity Model* (Version 2.1) published by the Department of Energy of the United States of America	Meet Maturity Indicator Level 2 as indicated in the document
5	*The 2023 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327)	Meet Security Profile 2 as indicated in the document

Note: Section 30AN and 30ANA of the Act provide for the incorporation of the documents mentioned in this subsection as in force from time to time.

(4) A responsible entity for a CI asset specified in subsection 4A(1) may otherwise comply with subsection (3) of this section by establishing and maintaining a process or system in their CIRMP to comply with a framework that is equivalent to a framework in a document mentioned in subsection (3), including any *[relevant]* conditions.

Multi-Factor Authentication

(5) Subject to subsections (6) and (7), a responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the entity's CIRMP to—so far as it is reasonably practicable to do so—implement phishing-resistant multi-factor authentication controls to:

(a) authenticate:

(i) users to their organisation's online and internet-facing networks;

(ii) privileged and unprivileged users of critical systems;

(iii) remote access to their networks and systems; and

(b) centrally log, monitor and routinely review both successful and unsuccessful multi-factor authentication attempts.

(6) Subsection (5) applies if a responsible entity complies with a framework specified under subsection (3) or (4) which does not require the implementation of phishing resistant multifactor authentication controls.

(7) Where a responsible entity for a CI asset specified in subsection 4A(1) cannot practically implement phishing resistant multi-factor authentication controls, reasonable steps must be taken to adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued.

Critical systems network protection

(8) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the entity's CIRMP to:

(a) identify critical systems and maintain an inventory of critical systems that are important to the delivery of the function of the asset;

(b) subject to subsection (9)—implement network segregation between critical systems and other networks; and

(c) subject to subsection (10)—recover and restore critical systems in the event where:

(i) CI asset networks are compromised or no longer trusted; or

(ii) where a cyber security incident has occurred, or is occurring

(9) For the purposes of paragraph (8)(b)—so far as it is reasonably practicable to do so—a responsible entity must consider whether the following *[elements/activities]* are required to implement network segregation:

(a) ensuring critical systems can be operationally independent from information technology;

(b) ensuring critical systems including its components can continue to be operational for a period of at least three months while other networks are in a state of restoration and recovery;

(c) implementing logical access controls or network traffic between critical systems and all other networks;

(d) centrally log, monitor and routinely review access logs for communication paths between critical systems and other networks; and

(e) implementing principles of least privilege across networks that connect to critical systems.

(10) For the purposes of paragraph (8)(c)—so far as it is reasonably practicable to do so—a responsible entity must consider whether the following *[elements/activities]* are required:

(a) implementing a plan to completely rebuild critical systems; and

(b) ensuring the continued availability of the asset whilst rebuilding critical systems.

(11) For subsections 30AKA(1), (3) and (5) of the Act, a responsible entity for a CI asset specified in subsection 4A(1) must also have regard to whether the entity's CIRMP:

(a) describes the cyber and information security hazards that could have a relevant impact on the asset; and

(b) contains appropriate measures (including measures required to address the additional material risks under subsection 8A(2)) that minimise or eliminate those material risks or to minimise the relevant impact of the cyber and information security hazard on the CI asset.

8 Subsection 9(2) (note)

Repeal the note, substitute:

Note: Subject to subsections 9A(4), a responsible entity is not required to use the AusCheck scheme to assess the suitability of critical workers, unless the responsible entity is a responsible entity of an asset specified in subsection 4A(1).

9 After section 9

Insert:

9A Personnel hazards—enhanced requirements

(1) For paragraph 30AH(1)(c) of the Act, subsections (2), (3), (4), (5), (6), (7) and (8) specify enhanced requirements for personnel hazards.

Personnel security—access management

(2) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the entity's CIRMP to minimise or eliminate the material risk of associated with:

(a) unauthorised or unsupervised access to critical systems including their components; and

(b) the compromise and misuse of credentials and privileged access used by critical workers to access the CI asset; and

(c) access to the CI asset by persons other than critical workers for the CI asset.

Mapping of onshore and offshore critical workers

(3) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the entity's CIRMP to:

(a) assess the suitability of an onshore or offshore critical worker that have access to critical systems including their components; and

(b) permit an onshore or offshore critical worker access to critical systems and their components only where the critical worker has been assessed to be suitable in accordance with subsection (4) and (5); and

(c) proactively monitor, identify and take action in relation to any developments or changes that may affect the ongoing suitability of an offshore or onshore critical worker; and

(d) minimise, mitigate or eliminate the risks posed by incoming or outgoing critical workers.

(4) For paragraph (3)(b) of this instrument and paragraph 30AH(4)(a) of the Act, an onshore critical worker may have access to critical systems including their components only where:

(a) after an AusCheck background check has been conducted in accordance with subsection (7)—the person has been assessed as suitable in line with subsection (8); or

(b) the person already holds an AGSVA Negative Vetting 1 (***NV1***) clearance at the time the person was identified to be an onshore critical worker.

Note: Where an onshore critical worker presently holds an NV1 clearance from AGSVA they will not be required to undergo an AusCheck background check. However, where that worker is yet to receive their NV1 AGSVA clearance as their application is pending, they must undergo an AusCheck background check while the clearance is pending.

(5) For paragraph (3)(b), an offshore critical worker may have access to critical systems including their components only where:

(a) after an AusCheck background check has been conducted in accordance with subsection (7)—the person has been assessed as suitable; or

(b) the person holds an AGSVA NV1 clearance at the time the person was identified to be an offshore critical worker; or

(c) if an offshore critical worker is unable to meet the requirements in paragraphs (a) and (b)—the responsible entity must outline in their CIRMP:

(i) the risk associated with the employment of the offshore critical worker; and

(ii) as soon as it is reasonably practicable to do so—any actions undertaken to minimise or eliminate the material risk to the asset.

(6) Where a person is assessed to be suitable on the basis that they already hold an AGSVA NV1 clearance for the purposes of paragraphs (4)(b) and (5)(b), the responsible entity for a CI asset specified in subsection 4A(1) must maintain a process or system in their CIRMP to ensure that the person's suitability is re-assessed prior to the lapse or expiration of the person's clearance, through either:

(a) revalidation of their AGSVA NV1 clearance; or

(b) by obtaining an AusCheck background check in accordance with subsection (7) and to be assessed as suitable.

AusCheck background check and suitability assessment

(7) Where an AusCheck background check is required, the background check must:
  (a) include an assessment of the information outlined in subsection 9(3);
  (b) be conducted in accordance with subsection 9(4);
  (c) If the background check relates to a person requiring ongoing access to critical systems including its components – for a background check to be conducted (at minimum) every 5 years.

(8) In making a suitability assessment mentioned, a responsible entity must consider the matters specified in subsection 9(5).

(9) For subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must also have regard to whether the entity's CIRMP includes processes or systems capable of identifying the matters in subsections (2) and (3) of this section for their CI asset.

10 After section 10

Insert:

10A Supply chain hazards—enhanced requirements

(1) For paragraph 30AH(1)(c) of the Act, subsections (2), (3), (4) and (5) specify enhanced requirements for supply chain hazards.

Supply chain mapping

(2) A responsible entity of a CI asset specified in subsection 4A(1) must establish and maintain a system or process in the entity's CIRMP to map their supply chain for major suppliers and critical systems across their physical and cyber supply chains.

(3) In accordance with subsection (2), the entity's CIRMP must:
  (a) identify vulnerabilities and risks in the entity's supply chain; and
  (b) identify the maximum tolerable outage for the CI asset or any of its critical systems, components, major suppliers or providers; and
  (c) as far as is reasonably practicable to do so—include measures to mitigate those vulnerabilities and risks, or an outage specified in paragraph (3)(b).

Note: Mitigation measures for the purpose of paragraph (2)(c) may include, but are not limited to, supplier diversification, redundancy planning, recovery, resilience and restoration processes.

Vendor assessment

(4) A responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a system or process in the entity's CIRMP to assess the risks associated with an existing or proposed major supplier for the CI asset.

(5) The system or process outlined in subsection (4) must identify, for each existing or proposed major supplier:
  (a) in relation to FOCI risks—legislative or other legal requirements to which the supplier is subject to; and
  (b) restrictions, sanctions or other impediments affecting the jurisdiction in which the supplier is based; and
  (c) the access, influence and control the supplier has over the CI asset in connection with the product or service the supplier provides; and
  (d) the extent to which the matters in paragraphs (a), (b) and (c) together may present a material risk for the CI asset, or could exceed a maximum tolerable outage of the service or product provided by the supplier; and

(e) as far as reasonably practicable to do so—*[steps/actions/activities]* to minimise or eliminate material risks and mitigate the relevant impact of the hazard on the CI asset.

(6) For subsections 30AKA(1), (3) and (5) of the Act, a responsible entity must have regard to:
   (a) whether the CIRMP includes a process or system capable of identifying the matters in paragraphs (3)(a), (b) and (c) for their CI asset; and
   (b) whether the CIRMP includes a process or system capable of identifying the matters in paragraphs (5)(a) to (e).

11 After section 11

Insert:

11A Physical security hazards and natural hazards—enhanced requirements

(1) For the purpose of paragraph 30AH(1)(c) of the Act, for physical security hazards and natural hazards, a responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the entity's CIRMP to:
   (a) centrally manage physical security and natural hazards; and
   (b) as far as it is reasonably practicable to do so—minimise or eliminate the risk associated with physical security consequences arising from the occurrence of both physical or other hazards, including cyber and information security hazards, personnel hazards and supply chain hazards.

Note: Some examples of non-physical hazards that have physical security consequences could include malicious cyber incidents that opens gates to allow unauthorised access, or a supply chain delay that results in changes to workplace operations that decrease the ability to deter, detect, delay, deny and defend.

(2) For the purposes of paragraph (1)(a), the responsible entity for a CI asset specified in subsection 4A(1) must outline:
   (a) the location, ownership, and nature of the site upon which their asset is located; and
   (b) the physical critical components of the CI asset; and
   (c) sensitive areas within the asset that hold business critical data, or contain critical systems and critical components; and
   (d) physical access controls to the CI asset for authorised personnel, official visitors, and the public, including but not limited to:
      (i) appropriate access controls for physical critical components and critical systems to restrict access to critical workers or accompanied visitors;
      (ii) maintaining appropriate surveillance and security alarm systems, such that critical components and critical systems are subject to continuous monitoring;
      (iii) specific protective security measures for business hours and out-of-hours;
      (iv) other protective security measures that increase the ability to deter, detect, delay, deny and defend for all critical systems including their components; and
   (e) mitigation and response measures taken where unauthorised access has been detected.

(3) For the purposes of subsections 30AKA(1), (3) and (5) of the Act, a responsible entity for a CI asset specified in subsection 4A(1) must have regard to whether the CIRMP contains systems or processes capable of identifying the matters in paragraphs (1)(a) and (b).

Additional reporting requirement under s 30AG of the Act – implementation updates

The Department is considering introducing a new requirement into the Rules that would require responsible entities to provide updates on the implementation of the enhanced CIRMP obligations as part of their annual reporting obligations under s30AG. The Department is currently seeking legal advice and considering how this could be implemented.

Attachment B – Feedback from the Enhancing the CIRMP Rules Consultation Paper (Consultation Paper)

General feedback

What we heard	How we have addressed it
Feedback outlined industry's understanding and agreement of why measures were being implemented. Common concerns regarding upfront and ongoing cost implications, insufficient timeframes for implementation.	The Department is conducting an impact analysis to ensure the proposed reforms are proportionate and that their cost implications for high-risk assets are properly understood. This will be made public following completion. The Department has considered submission feedback concerning implementation timeframes and has extended grace periods for key obligations.
Many high-risk asset classes are subject to budget and funding cycles which can limit availability to additional funding to implement security uplift measures.	The Department has engaged with relevant price regulators to ensure these bodies are aware of the security requirements for high-risk critical infrastructure assets. This includes highlighting the importance of enabling necessary security enhancements through appropriate pricing and regulatory settings. The Department is committed to continuing this engagement.
Submissions commonly suggested the inclusion of additional asset classes and sectors to the enhanced CIRMP Rules.	The asset classes included for the enhanced CIRMP obligations were identified due to their risk profile. Intelligence and open-source advice on state-sponsored attacks such as Volt Typhoon specifically call out these sectors as holding a heightened risk of targeted attack. The expansion of the CIRMP Rules to additional asset classes is not being considered in these reforms, however, the Department will continue to consider to the risk profiles of asset classes. These enhancements are considered to be best practice. The Department encourages voluntary compliance for all assets.
Industry submissions commonly called for further guidance and a principles-based approach to the enhanced CIRMP requirements. Some entities raised concerns around duplication of certain provisions with current operating practices or other obligations.	Best practice guidance for the enhanced CIRMP amendments, will be developed alongside the published CIRMP Rules. The Department encourages engagement through the TISN to assist in its development. The Department maintains a principles-based approach to the CIRMP, however baseline security needs to be lifted.

All-hazard measures

What we heard	How we have addressed it
Feedback for the 'consideration of specified risk advice measure' generally appreciated the obligation in principle. It was highlighted that many organisations already consider Commonwealth-issued risk advice and implement where appropriate. Stakeholders raised concerns about achieving compliance within the proposed timeframe and the potential for this measure to cause significant upfront and ongoing costs. Stakeholders also expressed concerns should specified risk advice become prescriptive or duplicative, requiring unnecessary costs and administrative burden on responsible entities.	The Department has considered advice from industry and government and determined that the most appropriate mechanism to enable the intent of this measure is to incorporate a new material risk into the proposed CIRMP Rules. This will require responsible entities to consider an impairment of the relevant critical infrastructure asset's functions that prejudices the social or economic stability, national security, or defence of Australia. Advice provided by the Department or other government concerning social or economic stability, national security, or defence of Australia must be considered as part of this material risk.
Industry feedback indicated delays to procurement and administration processes if a prescriptive approach was taken. Issues were also raised around timelines for implementation. Some stakeholders suggested that some suppliers indicated FOCI risk are inherent in their organisation. On the other hand, some stakeholders requested prescriptive identification of FOCI risk.	The Department maintains a principles-based approach to the CIRMP. The identification of FOCI risk does not preclude the procurement or use of products or services or engagement of personnel. The Department understands that some FOCI risk mitigation strategies may take time to implement. Responsible entities should take a risk-based approach to FOCI risk and be able to demonstrate how they will address outstanding assessments, including their estimated timeline for completion. The Department does not intend to whitelist or blacklist specific vendors thought the CIRMP framework.

Cyber and Information Hazards

What we heard	How we have addressed it
Whilst uplifting cyber maturity for high-risk assets was broadly supported, industry feedback highlighted significant barriers to achieve compliance within the proposed timeframes. Stakeholders outlined concerns such as costs and technological limitations to uplifting to Maturity Level 2, particularly for smaller operators and those with legacy OT environments.	The Department is extending the proposed timeframes for this measure. Responsible entities will now have 24 months to achieve compliance with this measure. Extension of timeframes for compliance with this measure will allow additional time for responsible entities, particularly those that are constrained by budget cycles, to implement the necessary uplift.
Industry feedback was generally supportive of the multi-factor authentication measure in principle, however, there was some division on its implementation.	The Department is extending the proposed timeframes for multi-factor authentication. Responsible entities will now have 24 months to achieve compliance with this measure.

What we heard	How we have addressed it
There were calls for recognition that MFA may only be feasible for new assets, with reasonable-practicability principles applied for older systems.	The Department has amended the multi-factor authentication measure to clarify where an asset cannot viably implement phishing resistant multifactor authentication controls due to technical limitations of a system, all reasonable steps must be taken to adequately mitigate risks associated with components or technology that are redundant, unsupported, obsolete or discontinued.
Some entities raised concerns around the feasibility of network segregation as part of the network protection measure, including that they were unsure they could meet a 3-month isolation period between their critical systems and broader network.	The Department is extending the proposed timeframes for the network protection measure. Responsible entities will now have 24 months to achieve compliance with this measure. On balance with advice from government, including published products, the 3-month isolation period will be maintained. Responsible entities should, as far as is reasonably practicable, be able to isolate critical systems while continuing to provide critical services for a minimum of 3 months.

Personnel Hazards

What we heard	How we have addressed it
Industry feedback noted that many organisations already operate strong personnel security practices, with several welcoming the opportunity to formalise existing controls into a consolidated personnel security plan and improve consistency across sites. Some feedback indicated that the Rules should include an ongoing requirement to monitor personnel security.	The Department maintains a principles-based approach to the CIRMP, including the enhanced personnel hazard obligations. The Department will not mandate an approach or standard for how responsible entities present their personnel security plan. The personnel security plan measure has also been amended to include a new provision that a responsible entity must have appropriate mitigations in place to assess monitoring of personnel suitability on an ongoing basis, including the threat of insider risk.
Feedback supported clearer guidance on defining critical workers.	The Department does not intend to expand the definition of critical worker or propose any changes to it. Guidance will be developed to support industry with defining critical workers in their organisation.
Feedback indicated a preference for risk-based, flexible approach that recognises equivalent vetting regimes and existing controls rather than imposing a single prescriptive model. Concerns were also raised around equivalent checks for offshore workers.	The intent of this measure is for critical workers working for high risk critical infrastructure to have an intelligence assessment as part of their background check. For this reason, the Department proposes to maintain the mandate of AusCheck or a Negative

What we heard	How we have addressed it
	Vetting 1 as they are the only background checking regimes that includes all appropriate checks. AusCheck or The Department does not consider any foreign check to be equivalent to the requirements placed on onshore workers. Appropriate mitigations will need to accompany recruitment and continuous monitoring of offshore workers.
Concerns were also raised around vetting timelines.	The Department is proposing background checking reforms and has commenced co-design through the Background Checking Advisory Group. These reforms will look to streamline the background checking process and aims to deliver improvements including portability of a background check. With regards to the timeliness of checks, the Department notes its service target is 20 business days. In the Department of Home Affairs 2024/25 Annual report, the Department met this target with 86.28% of checks were completed in that timeframe.

Supply Chain Hazards

What we heard	How we have addressed it
Generally, industry participants understood the intent and supported the measure in principle. However, concerns were raised regarding supply chain mapping. These predominantly questioned the balance of cost-benefit, scope and required detail for the obligation.	The obligation is intended to be principles based, with mapping achieved as far a reasonably practicable. The Department notes that there are similar obligations such as APRA standards and the Modern Slavery Risk Assessment.
Industry participants held mixed views on vendors of concern and vendor assessment. Submissions highlighted issues around vendor supply chains and inability to source redundancy or alternative suppliers. Delays for procurement and administrative process were also raised. Several submissions also noted a lack of guidance around vendor assessment and sought further clarity from the Department.	The Department does not suggest that entities must cease use of a vendor who holds a supply chain risk. It is acknowledged that there may be monopolies in suppliers. Responsible entities must assess if mitigations applicable to their current provider, or an alternative or backup supplier is the most suitable risk mitigation strategy. The Department does not intend to whitelist or blacklist specific vendors. Responsible entities must assess their risks and mitigate as far as reasonably practicable.

Physical and Natural Hazards

What we heard	How we have addressed it
Industry feedback suggested that a mandated physical security measure would be beneficial, provided it allowed for a flexible risk-based approach with clear milestones that minimised duplication as much as possible. Concerns were raised on being prescriptive in the CIRMP with a proposed physical security plan.	The Department maintains a principles-based approach to the CIRMP, including the enhanced physical and natural hazard obligations. The Department will not mandate an approach or standard for how responsible entities present their physical security plan. The responsible entity must define how they integrate the physical security plan into their broader risk management program. This plan must consider how other hazards and risks may impact their physical security, including natural hazards such as fire.