Australian Government
Department of Home Affairs

CRITICAL
INFRASTRUCTURE SECURITY
CENTRE

Consultation Paper

Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

Executive Summary

Australia's security and economic resilience depend on the integrity and availability of critical infrastructure. The increasing interconnectedness of our critical infrastructure creates efficiencies and fosters growth but also enables compromise in one part of a network to rapidly cascade across multiple sectors. It is vital that these risks are mitigated, and where possible, eliminated.

The *Security of Critical Infrastructure Act 2018* (SOCI Act) provides the legislative foundation for protecting Australia's most important assets, through which multiple positive security obligations are placed on asset owners and operators, including the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP Rules). The CIRMP Rules require responsible entities to manage material risks across all-hazards, including cyber and information security, physical, personnel and supply chain domains, and minimise or eliminate them, as far as reasonably practicable.

While the CIRMP obligation has driven significant uplift in risk management practices across critical infrastructure sectors, it is a baseline security requirement. Enhancements to the CIRMP Rules are required to keep pace with the evolving threat landscape, especially for the sectors our intelligence agencies are telling us are most at risk. It is imperative that the obligations are commensurate with the threat landscape critical infrastructure operate within.

What the intelligence is telling us

Hostile foreign state actors and their proxies are increasingly targeting critical infrastructure globally to gain strategic leverage, disrupt essential services, and position themselves for coercive advantage. Australia is not immune to these threats.[1] Intelligence is demonstrating an increase in threats across all hazards. Malicious cyber campaigns, supply chain compromise, manipulation of managed service providers, foreign interference activity and vulnerabilities arising from opaque foreign ownership, control and influence (FOCI) structures, many of which are designed to remain undetected and influence operational control over time.

The Director-General of Security's Annual Threat Assessment 2025 highlighted that nation state actors are increasingly mapping and targeting critical infrastructure.[2] In 2024, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) joined FiveEyes intelligence partners in publicly attributing the compromise of multiple United States (US) critical infrastructure sectors to a state-sponsored group known as Volt Typhoon.[3]

The Annual Cyber Threat Report 2024-2025 from ASD's ACSC reported that 13% of the over 1,200 cyber incidents were reported by critical infrastructure – an increase of 2% from the previous year, with the most common types of cyber security incidents involving compromised assets and networks, compromised accounts and credentials, and Denial of Service (DoS)/Distributed DoS attacks.[4]

Threat actors aren't just pursuing cyber vulnerabilities. FOCI arrangements within both critical infrastructure entities and throughout supply chains exacerbate cyber risks.[5] Incidents affecting critical infrastructure frequently start in the supply chain.[6] It has recently been reported that unexplained, undeclared communication equipment had been found installed in foreign state-made solar inverters in critical US energy infrastructure with the capacity to change inverter settings leading to destabilisation of power grids, damage to infrastructure and triggering of widespread blackouts.[7] Similar inverters and controllers to those exposed in the US are deployed across Australia's energy sector, in both residential and commercial-scale distributed energy resources.[8] The renewable energy transition has identified an over-reliance on vendors and suppliers that could be considered high-risk, but equally made clear that diversification isn't necessarily an option, and it is therefore necessary to ensure adequate controls and risk mitigations are implemented.

---

[1] Director-General's Annual Threat Assessment 2025 | ASIO
[2] Director-General's Annual Threat Assessment 2025 | ASIO
[3] PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure | Cyber.gov.au
[4] ASD Cyber Threat Report 2024-25
[5] Foreign Ownership, Control or Influence Risk Assessment Guidance (without Appendices)
[6] Critical Infrastructure Annual Risk Review Second Edition, November 2024
[7] Rogue communication devices found in Chinese solar power inverters | Reuters
[8] It's not just software. Physical critical equipment can't be trusted, either | The Strategist

Espionage has become one of the most significant national security threats to Australia. Recent modelling by the Australian Institute of Criminology (AIC) for the Australian Security Intelligence Organisation (ASIO) in the Cost of Espionage report shows the costs of this degraded environment could cost more than $1 billion per espionage-enabled cyber incident affecting critical infrastructure – regardless of the vector. The same report indicated that insider threats involving state or state-sponsored actors impacting Australian businesses were estimated to cost up to $324.8 million.[9]

Combined, the threat is profound and underscores the need for continued vigilance and maturity in our national resilience settings. While the threat landscape is complex and diverse, we have already taken significant strides in our security posture and should have confidence in our ability to adapt and respond.

Engaging with us

The Australian Government recognises that the security and resilience of Australia's critical infrastructure relies on strong partnerships with industry. This is just one of many ways in which the Department engages with industry. The Trusted Information Sharing Network (TISN), Critical Infrastructure Advisory Council (CIAC), expert advisory groups, TISN briefings, Critical Infrastructure Security Conference, Critical Infrastructure Security Month (CISM), social media, and Critical Conversations podcast are all opportunities for discussion and engagement.

The Department will hold public town halls, and engagements through the TISN throughout the consultation period to support the proposed reforms. Feedback through this consultation process will directly shape the final design of reforms, associated guidance, and implementation timeframes. This will not be the only consultation on these reforms.

Many essential services are owned and operated by the private sector, and effective national security outcomes depend on reforms that are commercially realistic, technically achievable, and proportionate to the risk. These proposed amendments are being developed in consultation with responsible entities, operators and managed service providers, and peak bodies and technical experts to ensure the legislative framework remains practical to implement while preserving the overarching national security intent.

Broader work to uplift the security of Australia's critical infrastructure will continue alongside this consultation process. This includes the Independent Review into the operation of the SOCI Act, amendments to the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) legislative frameworks, and the development of Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*. These processes are out of scope for this paper but will remain aligned to ensure a coherent and nationally consistent security framework. Further information on related Government initiatives is available on the Department of Home Affairs website.

Submissions are invited on the proposals. Feedback may be provided on any aspect of the reforms, including their design, implementation, considerations, sector impacts, or alternative options. The Department will handle submissions confidentially, where requested. 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 13 February 2026 and sent to CI.Strategy.Guidance@homeaffairs.gov.au.

[9] The cost of espionage report

Enhancing the CIRMP Rules

The proposed amendments to CIRMP Rules, including the asset classes to which they apply, are aligned with assessments conducted by the National Intelligence Community (NIC) and implement targeted uplift in areas of greatest risk. Your engagement is critical to ensuring that these reforms are fit for purpose and contribute to practical and achievable security uplift of our most critical asset classes.

Application

It is proposed that the enhanced CIRMP Rules will be applied to asset classes as per *Table 1* below. The proposed application of the enhanced CIRMP Rules aligns with the criticality of the high-risk asset classes to the ongoing availability of other critical infrastructure sectors and the broader economy, and is reflective of intelligence assessments provided by the National Intelligence Community (NIC). All asset classes impacted by this proposal are currently required to develop and maintain a CIRMP under Part 2A of the SOCI Act, with application of the CIRMP obligation to additional asset classes not in scope of this paper.

***Table 1** – Specified asset classes subject to the enhanced CIRMP Rules*

Subject to proposed enhanced CIRMP		Subject to existing CIRMP		Not subject to CIRMP	
Sector	**Critical asset class**	**Sector**	**Critical asset class**	**Sector**	**Critical asset class**
Energy	Energy market operator asset Electricity asset Gas asset Liquid fuel asset	**Financial Services and Markets**	Financial market infrastructure asset mentioned in paragraph 12D(1)(i) of the Act	**Defence Industry**	Defence industry
				Financial Services and Markets	Banking assets Insurance asset Superannuation asset
Communications[10]	Broadcasting asset	**Health Care and Medical**	Designated hospital	**Health Care and Medical**	Critical Hospitals
	Domain name systems	**Communications**	Telecommunications assets through the TSRMP	**Transport**	Aviation asset Ports asset Public Transport asset
Water & Sewerage	Water asset	**Food and Grocery**	Food and grocery asset	**Space Technology**	No defined asset class
Transport	Freight service asset Freight infrastructure asset	**Data Storage or Processing**	Data storage or processing asset	**Higher Education and Research**	Education asset

For asset classes not currently subject to the CIRMP obligation, in some instances it is because they are subject to an alternative program or regulatory framework that involves similar obligations. For example:

- Defence Industry assets are subject to the Defence Industry Security Program (DISP)
- Some Financial Services and Markets assets are regulated by the Australian Prudential Regulatory Authority (APRA) and subject to Prudential Standard CPS 230 – Operational Risk Management
- Critical aviation assets are regulated under the *Aviation Transport Security Act 2004*
- Critical ports are regulated under the *Maritime Transport and Offshore Facilities Security Act 2003*

[10] Telecommunications assets were captured under the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025*

Alignment with the Transport Security Reform

The *Transport Security Amendment (Security of Australia's Transport Sector) Act 2025* (the TSA Act) amended the ATSA and the MTOFSA to introduce an all-hazards security framework. Amendments will be made to the *Aviation Transport Security Regulations 2005* (ATSR), and the *Maritime Transport and Offshore Facilities Security Regulations 2003* (MTOFSR) to require industry participants to comply with all hazard security obligations, including a requirement to identify and mitigate physical, personnel, cyber, supply chain, and natural hazard risks.

When these obligations come into effect, there will be duplicative all-hazard requirements for assets captured under both the ATSR or MTOFSR and the CIRMP Rules. In line with the Department's commitment to reduce regulatory duplication, made before the Parliamentary Joint Committee on Intelligence and Security,[11] it is proposed that where a responsible entity has an all-hazards security program under ATSA or MTOFSA that they are not required to have a CIRMP in place. It is the intention that entities will still have access to AusCheck for critical workers.

For the purposes of the mandatory cyber incident reporting obligation, the *Security of Critical Infrastructure (Application) Rule* (LIN22/026) 2022 will be amended such that critical aviation and ports assets maintain an equivalent cyber incident reporting obligation under the ATSA and the MTOFSA.

It should be noted that responsible entities will still be required to comply with other SOCI Act obligations, including the register requirements and the enhanced cyber security obligations associated with being a System of National Significance.

Overview

Table 2 below highlights the enhanced measures that the Department is seeking to implement for high-risk asset classes under this proposal. All responsible entities in the asset classes subject to the proposed enhanced CIRMP Rules at *Table 1* will be required to comply with the enhanced obligations listed below. All the below measures will be accompanied by additional guidance on commencement of the amended CIRMP Rules to support industry understanding and compliance.

***Table 2** – Summary of proposed CIRMP Rules measures*

<table>
<tr><th>All Hazard</th><th>Cyber Security</th><th>Supply Chain</th><th>Personnel Security</th></tr>
<tr><td rowspan="2">Specified risk advice</td><td>Cyber security framework uplift</td><td rowspan="2">Supply chain vulnerability mapping</td><td>Personnel security plan</td></tr>
<tr><td>Critical system network protection</td><td>Strengthened background checking</td></tr>
<tr><td rowspan="2">All-hazard material risks – foreign ownership control and influence</td><td>Multi-factor authentication</td><td rowspan="2">Vendors of concern</td><td rowspan="2">Enhancing personnel material risks</td></tr>
<tr><td>Enhancing cyber material risks</td></tr>
</table>

[11] Advisory report on the Transport Security Amendment (Security of Australia's Transport Sector) Bill 2024 pg. 35-36

All-hazard measures

All-hazard 1: Consideration of specified risk advice

The issue

The increasingly dynamic, diverse and changing security environment requires a flexible approach to risk identification and mitigation. The CIRMP obligation is underpinned by a principles-based risk-management approach that requires industry to identify the material risks to their asset, and minimise or eliminate them as far as reasonably practicable. As the threat landscape continues to evolve and the threats become increasingly diverse and challenging, it is necessary for government to ensure that industry is aware of certain specified risks that they are to minimise, and in some instances, must eliminate in a timely manner.

What we propose

The Australian Government frequently publishes actionable intelligence-based advice, across all-hazards, that outline specific hazards and threats that could pose a material risk to critical infrastructure assets. To ensure the CIRMP Rules remain a dynamic, fit-for-purpose legislative framework to address all-hazards threats, we are proposing to introduce a provision that enables the Department to specify risk advice that is relevant to specific sectors or asset classes, or broadly applicable to all asset classes. Once risk advice has been specified, affected responsible entities must consider the advice, identify whether it poses a material risk to the availability or function of their asset, and minimise or eliminate the material risks, as far as reasonably practicable.

Specified risk advice is intended to capture a non-exhaustive list of possible products, that could present in a number of formats. For risk advice to be considered specified risk advice, the Department of Home Affairs will have explicitly identified a certain product and published a reference to it, outlining asset classes to which it is applicable. Responsible entities will have 12 months from the identification of specified risk advice to have considered the advice, identified whether it poses a material risk to the availability or function of their asset, and minimised or eliminated the material risks, as far as reasonably practicable.

Case study

The Protective Security Policy Framework (PSPF) prescribes what Australian Government entities must do to protect their people, information and resources, and routinely issues direct instruction through formal direction to do or not do a certain act or thing for the purposes of security.

Under this measure, the Department could identify PSPF directions as specified risk advice, that entities are then required to consider as a part of their CIRMP. For example, the PSPF Direction 001-2025 requires Australian Government entities to prevent the access, use or installation of DeepSeek products, applications and web services due to their security risk. If the Department specified this PSPF direction under this measure, high-risk asset classes would be required to consider the installation and use of DeepSeek as a part of their CIRMP.

This is reflective of the threat landscape; whilst the PSPF requires Government entities to comply, many of the risks facing Government are also facing other high value targets, such as critical infrastructure.

As seen in this example, the PSPF directions would not require mandatory implementation from critical infrastructure assets, however, would require mandatory consideration as part of an entities' CIRMP.

Policy Design Questions

- Are there any controls on the scope of this measure that your organisation would suggest to assist with compliance and implementation?
- Could existing engagement mechanisms be adapted or improved to deliver more value, and support this obligation?

All-hazard 2: All-hazard material risks - foreign ownership, control and influence

The issue

Every time an organisation interacts with a supplier, manufacturer, or vendor they engage with risk, across all-hazards. The threat to the security of an asset posed by FOCI is complex, and can impact all aspects of an asset, leading to compromise, disruption, and degradation. FOCI, if unmitigated, can expose an entity to espionage, sabotage, supply chain disruption, cyber-attacks, and breaches of commercially sensitive and personal information.

The material risks outlined in the CIRMP Rules broadly capture all-hazards risks that responsible entities must minimise and eliminate as far as reasonably practicable, however, certain risks are more specific and need to be afforded appropriate consideration

What we propose

To address this issue, and in addition to the existing material risks that entities must continually mitigate against, the Department is proposing to require responsible entities to consider material risks associated with FOCI, across all aspects of their asset. In line with existing material risks, the expectation is for the responsible entity to minimise or eliminate FOCI risk as far as reasonably practicable. This will include consideration of impacts to the availability, integrity, and confidentiality of the responsible entity's asset that could prejudice the social or economic stability, or national security of Australia arising from, but not limited to dependence on foreign owned, controlled, or influenced:

- Vendors, major suppliers, or managed service providers critical to the operation of the asset
- Components, systems, or software critical to the operation of the asset

Responsible entities will be required to have considered, and minimised or eliminated material risks associated with FOCI, within 6 months of the amended CIRMP Rules commencing. This is in line with the grace periods for material risk in the existing CIRMP Rules.

Policy Design Questions

- Are there other specific material risks, like those arising from FOCI, that your organisation minimises or eliminates in their CIRMP?
- Does your organisation currently consider FOCI risks in their CIRMP?

All-hazard Measures - Regulatory Impact Analysis

Scenario

The Department specifies risk advice which could include (but is not limited to) Directions issued under the Protective Security Policy Framework (PSPF), which could relate to any type of hazard, including those outlined in the CIRMP Rules. Your organisation is notified of the new specified risk advice. On review of the specified risk advice, you identify possible risks to your asset that require consideration in line with your existing supply-chain security procedures, and cyber security program. You then need to develop a plan in your CIRMP to implement necessary changes to relevant procedures and programs to minimise or eliminate the identified risks as far as reasonably practicable.

What this could look like for your organisation

You might need to set up a process to track new risk advice, assess their relevance, and update your CIRMP with actions taken in response. This could involve creating a workflow, assigning staff to consider risk advice, and maintaining evidence for audits.

Questions

1. Does your organisation already respond to risk advice in this manner? For example, acting upon it as soon as practicable to ensure continuity of operations?
2. What changes would you need to make to your current processes?
3. What one-off costs would you expect (e.g., new workflow tools, staff training)?
4. What ongoing costs would you expect (e.g., staff time to review specified advice, update CIRMP)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there any limitations that would make this difficult for your organisation

Cyber and Information Security Hazard measures

Cyber 1: Cyber security framework uplift

The issue

Malicious and state-sponsored threat actors, like Volt Typhoon, Salt Typhoon, and APT29 are well resourced, enduring and willing to target and compromise Australia's critical infrastructure networks and systems. The current requirements in the CIRMP Rules were introduced to create a cyber security baseline across sectors of various maturities and prompt less mature sectors to engage in concentrated security uplift. The requirement to comply with maturity level 1 or equivalent of the prescribed cyber maturity framework has proven to be inadequate in repelling and preventing the compromise of critical infrastructure networks from state-sponsored and cyber-criminal threat actors. Higher minimum standards are required for the most at-risk sectors to ensure that entities are resilient and adequately protected.

In line with this assessment, the cyber maturity framework requirements were recently uplifted for the most critical telecommunications assets, through the *Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025* (TSRMP Rules). The TSRMP Rules requires entities to meet maturity level 2 of their chosen framework, and where their cyber framework does not contain maturity levels, identify what additional controls they have implemented in their TSRMP to make it equivalent.

What we propose

The Department is proposing to amend the cyber and information security hazard provision to require entities within the identified asset classes (*Table 1 refers*) to comply with maturity level 2 of their chosen cyber maturity framework. For clarity, this equates to Maturity Indicator Level 2 of the *Cybersecurity Capability Maturity Model* (C2M2), and Security Profile 2 of the *Australian Energy Sector Cyber Security Framework* (AESCSF). Where an entity has chosen to comply with an equivalent cyber-framework that does not contain maturity levels, they must outline steps taken in their CIRMP to make their cyber program equivalent to maturity level 2 of an appropriate cyber maturity framework, like the C2M2 and AESCSF. In choosing to comply with an equivalent framework, the responsible entity must take into account whether their chosen framework is appropriate for their asset and its functions. If there is an operational technology component of their critical asset, it is the expectation that this is taken into account and appropriately protected.

Updated framework versions

Since the introduction of the CIRMP Rules, 4 of the 5 listed cyber frameworks have been revised and updated in line with necessary improvements to cyber security. In some instances, the newer iterations of a framework require greater cyber maturity and uplift than currently required, which can incur significant regulatory impost. In consideration of these changes, the Department is proposing to amend the currently listed frameworks to include revised and updated versions and encourage responsible entities to consider the most appropriate benchmark for their organisation's cyber program. For clarity, the cyber frameworks in the enhanced CIRMP Rules will include:

- Australian Standard AS ISO/IEC 27001:2023
- The *Essential Eight Maturity Model* published by the Australian Signals Directorate
- *The NIST Cybersecurity Framework (CSF) 2.0 published* by the National Institute of Standards and Technology of the United States of America
- *Cybersecurity Capability Maturity Model (Version 2)* published by the Department of Energy of the United States of America
- *The 2023 AESCSF Framework Core* published by Australian Energy Market Operator Limited (ACN 072 010 327)

The Department is proposing an implementation period of 18 months to achieve compliance with maturity level 2 or equivalent of their chosen cyber framework, which will require the entity to be compliant by 30 June 2028, and attest to compliance in the July to September 2028 attestation period. Given the extended periods for compliance, there will be a requirement to have a documented plan within the CIRMP that details how level 2 maturity will be accomplished in attestation periods leading up to the September 2028 attestation

period. For entities adopting version 2 of their chosen cyber maturity framework, this documented plan will also need to include how compliance with version 2 will be accomplished.

Policy Design Questions

- Where applicable, what maturity/profile does your organisation seek to achieve?
- How does your organisation invest in security beyond achieving minimum cyber framework compliance?
- Does your organisation face challenges in obtaining the necessary investment in security to reach compliance, or (where necessary) go beyond the minimum cyber framework?

Cyber 2: Critical systems network protection

The issue

Malicious state-sponsored threat actors and cyber criminals are increasingly targeting externally facing networks, such as environments where users can access resources like the web, email and other internet services, to laterally move across the network to target systems that are more critical to the function of the asset and sensitive data, such as OT networks. In doing so, malicious actors can pre-position on critical systems for destructive impact when they so choose and monitor sensitive business data that could compromise a business's ability to operate. The 2024 joint cybersecurity advisory on the state-sponsored organisation Volt Typhoon confirmed that the IT environments of multiple US critical infrastructure organisations were compromised with the intent to preposition to enable lateral movement to OT networks to disrupt functions.

Malicious entities can move laterally across networks and operate without detection. It is imperative responsible entities implement architectural defences to increase the difficultly for a malicious actor to move laterally when a compromise occurs and segregate the systems so that the critical asset can continue to function even when other parts of the network are impacted. Understanding critical and supporting systems in your asset is an essential part of preventing critical function disruption and enables faster recovery following a significant incident that compromises or degrades networks and systems. Ensuring entities are equipped to respond to incidents and restore critical systems when network containment fails, is essential to the availability and operation of the critical asset.

What we propose

We propose that responsible entities must outline in their CIRMP how they have implemented the greatest practical level of segregation between their asset's critical systems, and other internet-connected, or less secure components that could result in the compromise of, substantive loss of access to, or deliberate or accidental manipulation of a critical system. Critical systems include vital operational technology, enabling services, and critical components vital to the delivery of the asset's function, or whose compromise or degradation could cause significant harm to the asset. This will require the responsible entity to identify their critical systems and components, and implement the greatest practical level of segregation between their critical systems from all other networks, which could include:

- maintaining an inventory of critical systems important to the delivery of the function of the asset;
- ensuring critical systems are operationally independent from other IT systems and networks to the greatest extent possible, such that they can be isolated for a period of 3 months while maintaining critical services;
- implementing logical access controls for network traffic between critical systems and all other networks;
- consistently reviewing access logs for communication paths between critical systems and other networks; and
- implementing principles of least-privilege across networks that connect to critical systems

Should network segregation or isolation measures not be effective at preventing compromise of critical systems, and where not already present, it is proposed that the responsible entity builds redundancy plans into their CIRMP. Recovery and restoration controls are vital to minimising the potential impact of compromise or sabotage of an asset's critical systems and reducing potential downtime or disruptions to

availability. The responsible entity will be required to have a plan in their CIRMP to completely rebuild critical systems whilst continuing the operation of the asset.

The Department is proposing compliance with critical systems network segregation and recovery requirements by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period. Given the extended periods for compliance, there will be a requirement to have a documented plan within the CIRMP that details how compliance will be accomplished in attestation periods leading up to the September 2028 attestation period.

Case study

A cyber incident occurs involving unauthorised access to an organisation's payroll system. The responsible entity undertakes network containment actions, which involves isolation of the critical asset from the payroll system while incident response is undertaken. The isolation allows the function and service of the critical asset to continue while the payroll system is down.

The entities' inventory of critical systems allows for time effective isolation, when it matters most.

Policy Design Questions

- What current measures does your organisation implement to segregate critical systems from all other internet facing and less secure systems?
- Does your organisation mandate security awareness training for users with access to critical systems?
- What measures does your organisation undertake to log who has access and can make changes to your critical systems?
- Does your organisation undertake logging and monitoring of network traffic?

Cyber 3: Multi-factor authentication (MFA)

The issue

Malicious threat actors are increasingly using compromised user credentials to access sensitive data and critical systems to preposition for destructive attacks or monitor sensitive traffic. Whilst more and more entities are implementing MFA, threat actors are becoming increasingly creative and persistent in their attempts to compromise networks and systems. The ASDs ACSC 2024-25 Cyber Threat Report highlighted that compromised accounts and credentials were one of the top 3 cyber security incident types reported by critical infrastructure entities. Although it doesn't offer absolute security outcomes, MFA is a necessary cyber security practice to mitigate poor cyber hygiene and compromised accounts and credentials. The requirements for MFA across the identified cyber maturity frameworks varies; given a responsible entity can choose an equivalent framework, it is necessary to establish a baseline expectation for MFA application to address associated risks.

Messaging to businesses "has always been the three same principles: use multifactor authentication; do your updates straight away; and use pass phrases" – The Hon Tony Burke MP[12]

What we propose

We propose that where not already present, not adequately required in an entity's chosen cyber maturity framework, or not already part of an entity's cyber program, responsible entities must outline in their CIRMP how phishing-resistant MFA is used to:

- authenticate users to their organisation's online and internet facing networks,
- authenticate privileged and unprivileged users of critical systems, and
- authenticate remote access to their networks and systems.

[12] AFR Summit Keynote Speech

To ensure an entity's MFA controls are robust, they must implement a process or system to ensure that they centrally log successful and unsuccessful authentication attempts and review them in a timely manner.

The Department is proposing compliance by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period. Given the extended periods for compliance, there will be a requirement to have a documented plan within the CIRMP that details how compliance will be accomplished in attestation periods leading up to the September 2028 attestation period.

Policy Design Questions

- What type of systems in your organisation are currently protected by MFA?
- Are there system or/circumstances in which MFA is not reasonably practicable to use? If so, what other compensating controls are, or could be implemented?

Cyber 4: Enhancing cyber material risks

The issue

Critical infrastructure operates in a dynamic, diverse and constantly evolving threat environment. Technological developments present opportunities for industry to automate, uplift and improve efficiencies in processes and service delivery, but can also introduce complex and sophisticated vulnerabilities that pose significant material risks to the integrity and availability of a given asset. These technologies could include artificial intelligence, post-quantum encryption, and other novel technologies on the horizon that will play a central role in the future security, operation and functionality of essential services and critical infrastructure.

Equally, readily available and well-integrated technologies and processes that improve efficiencies and operations are already relied upon by owners and operators but pose significant risks to the integrity and availability of the asset. These include offshoring remote access to critical control systems and business critical data, and other remote workforce applications that reduce data sovereignty, authority and control.

Legacy componentry and systems are often maintained due to limited substitutes and the significant costs involved with replacing components or systems. Where such components have not or cannot be replaced, it is necessary that the responsible entity consider the ongoing vulnerabilities to which they are subject. Failure to replace unsupported or end-of-life components and systems can significantly impact redundancy and an entity's ability to restore operations if disrupted, which can impact economic stability and national security.

What we propose

The Department is proposing to identify and introduce cyber and information hazard specific material risks that the responsible entity will need to minimise or eliminate, as far as reasonably practicable, in their CIRMP. This will include consideration of impacts to the availability, confidentiality, and integrity of the responsible entity's asset that could prejudice the social or economic stability, or national security of Australia arising from, but not limited to:

- the deployment of advanced and emerging technology, and use of such technology by malicious and state-sponsored actors against the asset.
- offshore remote access to critical systems and operational technology control systems.
- offshore remote access to business critical data.
- failure to replace unsupported software, hardware and other critical components, and replace legacy systems or adequately mitigate associated risks and redundancy.

Case study

The responsible entity complies with their chosen cyber maturity framework and implements critical system network segregation and multi-factor authentication (MFA) controls as part of their cyber program, to the greatest extent possible. As part of their cyber program, they are also required to consider advanced and emerging technology risks, both in terms of how they may use such technology in their organisation for automation and efficiencies, but also in terms of use by adversaries seeking to compromise and disrupt their asset.

In considering the material risks posed and given recent guidance and advice released regarding artificial intelligence vulnerabilities arising through use of Large-Language Models (LLMs), the responsible entity must consider what controls they can reasonably implement in their cyber program and CIRMP to minimise or eliminate the material risks to their asset. Where the entity deploys AI, this could involve limitations on application within the entity's organisation and networks, consideration of alternative AI solutions that pose less risk, or updating of organisational policy regarding use of AI. In response to use by malicious and state-sponsored actors, this could include organisational education and awareness sessions and uplifting of cyber program controls where relevant to the threat posed, which could include for protection of business critical data.

Cyber and Information Security Hazard - Regulatory Impact Analysis

Scenario

Your CIRMP would need to include a plan to reach at least maturity level 2 of your chosen cyber maturity framework. You also need to segregate critical systems from IT networks, implement phishing-resistant MFA for sensitive systems, and manage risks from emerging technologies like AI and quantum computing. Overall, your organisation will need to achieve a suitable level of cyber security maturity for today's threat landscape.

What this could look like for your organisation

You might need to upgrade firewalls, deploy MFA tokens, redesign network architecture, and update policies to include AI risk controls. This could involve purchasing new technology, hiring specialists, and conducting audits.

Questions

1. Is your organisation already compliant with one, or more of these four amendments? If so, please tell us which ones.
2. If you are not compliant with these amendments, which one would be most challenging for you? Why?
3. What one-off costs would you expect (e.g., hardware/software upgrades, consultancy)?
4. What ongoing costs would you expect (e.g., monitoring, audits, licence renewals)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes
7. Are there any dependencies or constraints (e.g., physical configuration of OT/IT systems, vendor availability, certification cycles)?

Supply Chain Hazard measures

Supply Chain 1: Supply chain vulnerability mapping

The issue

Malicious state-sponsored actors increasingly use foreign government involvement in supply chains to leverage control and influence, and to preposition for future attacks. Supply chains can introduce critical vulnerabilities and dependencies which malicious actors can exploit, particularly where there is a reliance on third party vendors or an inability to diversify suppliers. Supply chains also introduce interdependencies between critical infrastructure sectors and asset classes, meaning that compromise or disruption of a major supplier can have cascading impacts across multiple sectors. Some sectors are more attractive targets, given the opportunities for disruption they present; these sectors must be more resilient and secure in their approach to supply chain risk management.

What we propose

In addition to existing CIRMP Rules obligations, entities must establish and maintain a process or system to map their supply chain for major suppliers and critical systems across their physical and cyber supply chains. This exercise builds on the existing CIRMP Rules requirement to describe interdependencies between the responsible entity's asset and other critical infrastructure assets (s7(2)(b) of the CIRMP Rules refers). The purpose of this measure is to identify critical vulnerabilities in the entities' supply chain, and to minimise or eliminate, as far as reasonably practicable, any identified material risks as a result.

As part of this exercise, the responsible entity should outline supply chain vulnerabilities and mitigating controls, and where possible, include details regarding supplier diversification and redundancy planning, which relates to the recovery and restoration provision being introduced as part of the critical systems network segregation measure.

The Department is proposing compliance by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period.

Case study

An entity maps their supply chain and discovers a critical component is manufactured in Australia, but the supplier has been listed for sale for a year, with no prospect of a buyer. After further investigation, the entity discovers that this supplier is the only supplier of this component in Australia. Having identified this risk, the entity looks at other options to secure their supply chain and mitigate redundancies and discovers a supplier in New Zealand which can manufacture the critical component. As a result, the entity updates their business continuity plan to include the alternative supplier, should their current supplier no longer be available.

Policy Design Questions

- To what level of upstream and downstream detail does your organisation currently map their supply chain?
- Does your organisation keep a list or record of alterative approved suppliers?
- Does your organisation have real-time access to data surrounding supplier availability?

Supply Chain 2: Vendors of concern

The issue

FOCI poses a significant risk to the security of Australia's critical infrastructure, particularly in high-risk sectors that are highly interdependent and interconnected. For many sectors, vendors are vital to the continued availability and operation of their assets; in some instances, there are limited options when it comes to vendor diversification. Vendors subject to FOCI can be directed to act against their own business interests or could be compelled by a foreign government to conduct malicious actions against a critical infrastructure entity, in a manner that is adverse to Australia's interests.[13] If not properly managed, FOCI risks can lead to unauthorised access to sensitive information, compromise of critical systems, and acts of sabotage and interference. Identifying and managing vendors of concern, whether that be through diversification or alternative control measures, is an important part of maintaining your businesses resilience in the face of sophisticated and targeted threats.

What we propose

To complement the supply chain hazard requirement in the CIRMP Rules, responsible entities will be required to develop and maintain a process or system in their CIRMP to manage material risks posed by vendors of concern that expressly consider FOCI risks. The process or system will need to identify risks associated with certain vendors, consider the material risks and their impact if realised, and outline risk-based treatments and controls. In developing a process or system to manage vendors of concern, responsible entities could consider the principles underpinning the vendor assessment in the FOCI Risk Assessment Guidance.

Adverse assessments against vendors, identified through the responsible entities vendor assessment process or system, does not exclude their use where no practical alternatives exist. In those instances, additional security measures must be implemented to manage ongoing supply chain compromise risks.

The Department is proposing compliance by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period. Given the significant lead time to develop a process or system to assess vendors, the expectation is that responsible entities have implemented the process and have had assessed all existing major suppliers by 30 June 2028. Once established, the responsible entity will be required to assess new and proposed vendors using their vendor assessment procedure as part of their procurement process.

Case study

An engineering company is based overseas and engaged to design a critical component of an asset. Through the vendor management process, a FOCI risk is identified. To mitigate the identified risk, the entity considers diversifying options for delivery, but further market research clearly outlines that diversification is not an option. The entity considers options to mitigate this risk given no feasible alternative and implements contractual conditions to limit offshoring, through design and implementation phases, restrict access arrangements, and include remediation and step-in clauses.

Policy Design Questions

- How does your organisation currently map vendors of concern in your supply chain?
- What current security measures are put in place if a vendor of concern is identified?
- Does the wider government provide adequate material to support you to identify a vendor of concern and mitigate their potential impact?
- Are there other options to reduce the FOCI risk posed by vendors of concern, either in addition to or instead of the proposed approach?

[13] Foreign Ownership, Control or Influence Risk Assessment Guidance pg. 2

Supply Chain Hazard - Regulatory Impact Analysis

Scenario

Your CIRMP would need to include a map of your critical suppliers, identify dependencies, and show steps taken to secure your supply chain. You would also need to assess foreign ownership, control and influence risks for vendors and apply additional security measures if high-risk vendors are unavoidable.

What this could look like for your organisation

You might need to implement supplier assurance questionnaires, maintain a database of critical suppliers, and introduce stricter procurement checks. If a vendor is high-risk, you may need to add compensating controls or diversify suppliers.

Questions

1. Is your organisation already compliant with one, or both, of these amendments? If so, please tell us which ones.
2. What changes would you need to make to your procurement or supplier management processes?
3. What one-off costs would you expect (e.g., mapping tools, supplier audits)?
4. What ongoing costs would you expect (e.g., periodic reviews, monitoring)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there practical limitations (e.g., lack of alternative suppliers)?
8. Would this limit the supply of good and services you provide, or potentially your competitiveness in the market? If yes, please describe how.

Personnel Security Hazard measures

Personnel 1: Personnel security plan

The issue

Personnel security hazards pose significant risks to critical infrastructure entities, from intentional sabotage through misuse of privileged access, to the unintentional sharing of sensitive data. A trusted insider may also be acting on behalf of a malicious actor, such as a foreign power, issue motivated group, organised crime groups or violent extremist group, to either intentionally or unintentionally gain access to official, or sensitive information.[14]

Under the current CIRMP Rules, responsible entities are required to ensure they implement adequate personnel risk mitigations in their CIRMP, particularly for their critical workers, which could include contractors with access to sensitive assets or systems. Many responsible entities will already have a mechanism or process in place to minimise or eliminate personnel security hazards but these aren't always applied holistically across an entire organisation and often perform general corporate functions rather than being targeted at personnel security threats, limiting their ability to minimise or eliminate material risks.

What we propose

The Department is proposing to introduce a requirement for responsible entities to establish and maintain a personnel security plan for their organisation. The personnel security plan obligation will incorporate existing personnel hazard obligations in the CIRMP Rules, and require the responsible entity to develop and maintain a process or system to minimise or eliminate risks associated with, but not limited to:

- unauthorised, unescorted or privileged access to critical assets
- compromised credentials and exploitation resulting from personnel travel, both official and personal
- exposure of physical and digital critical assets from visiting officials and delegations

In addition to the existing personnel hazard obligations, the personnel security plan will need to consider the proposed amendments below, which includes strengthened background checking requirements to assess critical worker suitability, and consideration of material risks that could impact the integrity, confidentiality, or availability of their asset.

The Department is proposing compliance by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period. Given the extended periods for compliance, there will be a requirement to have a documented plan within the CIRMP that details how compliance will be accomplished in attestation periods leading up to the 2028 attestation period.

The Department will develop best practice guidance to help entities meet this obligation, including guidance on identifying critical workers.

Personnel 2: Strengthened background checking

The issue

Critical workers often have unescorted and privileged access to the most sensitive systems and components of a critical infrastructure asset and are uniquely poised to cause catastrophic damage to the functioning and availability of the asset. Responsible entities are required to ensure they implement adequate personnel risk mitigations in their CIRMP, particularly for their critical workers, which could include contractors with access to sensitive assets or systems. There are also many sectors that have contracted and shared workforces, who use different background checking standards with varying application and controls, which can result in some entities compromising on their security protocols to ensure they are adequately staffed.

What we propose

The Department is proposing to mandate the identification of all critical workers and require onshore critical workers to undergo an AusCheck background check as part of pre-employment screening, unless the critical worker holds an Australian Government security clearance of Negative Vetting 1 or above. A revalidation

[14] PSPF Release 2025 pg. 31

check through AusCheck is required at minimum every 5 years, however, the responsible entity can choose to revalidate at an increased frequency if they identify a business requirement to do so.

For offshore critical workers, where it is not possible to undertake an AusCheck background check or another form of intelligence background check, the responsible entity will need to ensure they identify risks associated with such employment, and outline in their CIRMP how they minimise or eliminate, as far as reasonably practicable, the material risks to their asset.

The Department is proposing compliance by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period. Given the extended periods for compliance, there will be a requirement to have a documented plan within the CIRMP that details how compliance will be accomplished in attestation periods leading up to the 2028 attestation period.

The Department will develop additional guidance to help entities meet this obligation, including best practice guidance on how to identify critical workers.

Personnel 3: Enhancing personnel material risks

The issue

Much like the rationale behind the personnel security plan and strengthening background checking requirements, it is necessary to better articulate the material risks posed by trusted insiders, which could include intentional sabotage to unintentional sharing of sensitive data. A trusted insider may also be acting on behalf of a malicious actor, such as a foreign power, issue motivated group, organised crime groups or violent extremist group, to either intentionally or unintentionally gain access to official, or security classified information.[15] Expanding on material risks associated with personnel hazards in the CIRMP Rules will require responsible entities to consider a wider array of risks, and strengthen their security settings.

What we propose

To address this issue, the Department is proposing to identify and introduce personnel hazard specific material risks that the responsible entity will need to minimise or eliminate, as far as reasonably practicable, in their CIRMP. This will include considering how trusted insiders could impact the integrity or availability of their asset through unauthorised use or misuse of privileged access to critical systems which compromises the security and function of a relevant critical infrastructure asset. This could include major suppliers, critical workers, or managed service providers.

Policy Design Questions

- Does your organisation have a personnel security plan, or equivalent in place?
- Would a personnel security plan requirement improve security posture or duplicate existing controls?
- Does your organisation currently use background checking as a security control?
- How many AusCheck background checks do you anticipate undertaking each year?
- What practical limitations do you foresee for your organisation if required to implement a personnel security plan?

[15] PSPF Release 2025 pg. 31

Personnel Security Hazard - Regulatory Impact Analysis

Scenario

As part of developing or implementing your personnel security plan you will need to undertake a stocktake of existing personnel security measures, guidelines, processes and frameworks. You will also need to identify which roles in your organisation are considered “critical workers”, and ensure those employees complete an AusCheck background check before commencing employment and are then subject to reassessment under AusCheck at regular intervals throughout employment.

What this could look like for your organisation

Your HR team might need to update onboarding processes, embed a security culture through the development of training and awareness programs**,** manage applications through AusCheck, establish reporting channels for security concerns or breaches, and track compliance. This could involve system changes, staff training, and handling delays if checks take time.

Questions

1. Is your organisation already compliant with this amendment, or does it have a similar onboarding process in place. Please describe the similar process if it exists.
2. What changes would you need to make to your HR or onboarding processes?
3. What one-off costs would you expect (e.g., system updates, training)?
4. What ongoing costs would you expect (e.g., fees per check, staff time)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there any challenges in defining “critical workers” for your organisation?

Physical and Natural Hazards

We have not specified any measures under physical security, as we consider that responsible entities are adequately mitigating physical and natural security risks to their assets. We welcome feedback on including a physical security measure.

Policy Design Questions

- Does your organisation have a broader physical security plan?
- What type of physical security measure would be beneficial?
- Would a mandated physical security measure would be beneficial and how it could be effectively applied to your asset?
- Are there other additional material risks that your organisation considers could be included for physical or natural hazards?

Next Steps

How to provide feedback

The Australian Government invites written submissions on the detailed questions in this Consultation Paper. For your reference, the full list of questions has been extracted at **Attachment A** and **Attachment B**. We acknowledge there is some duplication in the questions, however we are seeking to understand the impact of each measure, as well as the package of proposed reforms.

Written submissions will be accepted up until 11.59 PM AEDT, Friday 13 February 2026.

Submissions on this Consultation Paper are welcome from all stakeholders including critical infrastructure entities, government, academia, and members of the general public.

We welcome written submissions in response to any or all of the consultation questions listed in this Consultation Paper. Please provide your submissions through the Submissions Form and direct any questions relating to the submission process to: CI.Strategy.Guidance@homeaffairs.gov.au.

What we will do with your feedback

Feedback from written submissions and other engagement will be used by the Department to refine the reform proposals described in this Consultation Paper. Your feedback will help us fully understand the costs and benefits of options to inform the policy development process and advice to Government. Any regulatory burden will be carefully considered alongside the benefit from proposed changes to strengthen our resilience and security posture. The Department appreciates all responses, but recognises not all questions are able to be answered. Each answer helps the Department in assessing the impact of the proposed reform.

The Department will publish your submissions on its website, unless you advise at the time of submission that your submission is confidential.

After reviewing your feedback on the proposals in this Consultation Paper, the Department will provide advice to Government on new legislation and subordinate legislation.

Privacy collection notice

The Department is bound by the Australian Privacy Principles (APPs) in the Privacy Act. The APPs regulate how we collect, use, store and disclose personal information, and how you may seek access to, or correction of, the personal information that we hold about you.

Providing personal information in your submission is voluntary. Please refrain from including personal information of any third parties. The Department may publish your submission (including your name), unless you request that your submission remain anonymous or confidential, or we consider (for any reason) that it should not be made public. If you do not tell us that your submission is to remain anonymous or confidential, you acknowledge that by providing your submission it may be accessible to people outside Australia and that you are aware that:

- any overseas recipient(s) will not be accountable under the Privacy Act for any acts or practices of the overseas recipient in relation to the information that would breach the APPs; and
- you will not be able to seek redress under the Privacy Act if an overseas recipient handles your personal information in breach of the Privacy Act.

The Department may redact parts of published submissions, as appropriate. For example, submissions may be redacted to remove defamatory or sensitive material. Submissions containing offensive language or inappropriate content will not be responded to and may be destroyed.

Information you provide in your submission, including personal information, may be disclosed to the Commonwealth; state and territory governments and their departments and agencies; and third parties who provide services to the Department, for the purposes of informing and supporting the work of implementing reforms to the SOCI Act and its subordinate CIRMP Rules. This information may also be used to communicate with you about your submission and the consultation process.

For more information about the Department's personal information handling practices, including how you can seek access to, or correction of, personal information that the Department holds about you, or how to make a complaint if you believe that the Department has handled your personal information in a way that breaches our obligations in the APPs, please refer to the Department's privacy policy, which you can access here.

Attachment A - Regulatory Impact Analysis questions

All-hazard Measures

Scenario

The Department specifies risk advice, which could relate to any type of hazard, including those outlined in the CIRMP Rules. Your organisation becomes aware of the new specified risk advice, having developed a process to track new advisories, assess their relevance to your asset, and consider any potential risks posed to your asset that are outlined in the specified risk advice.

On review of the specified risk advice, you identify possible risks to your asset that require consideration in line with your existing supply-chain security procedures, and cyber security program. You then develop a plan in your CIRMP to implement necessary changes to relevant procedures and programs to minimise or eliminate the identified risks as far as reasonably practicable.

What this could look like for your organisation

You might need to set up a process to track new risk advice, assess their relevance, and update your CIRMP with actions taken in response. This could involve creating a workflow, assigning staff to consider risk advice, and maintaining evidence for audits.

Questions

1. Does your organisation already respond to risk advice in this manner? For example, acting upon it as soon as practicable to ensure continuity of operations?
2. What changes would you need to make to your current processes?
3. What one-off costs would you expect (e.g., new workflow tools, staff training)?
4. What ongoing costs would you expect (e.g., staff time to review specified advice, update CIRMP)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there any limitations that would make this difficult for your organisation?

Cyber and Information Security Hazard Measures

Scenario

Your CIRMP would need to include a plan to reach at least maturity level 2 of your chosen cyber maturity framework. You also need to segregate critical systems, implement phishing-resistant MFA for sensitive systems, and manage risks from emerging technologies like AI and quantum computing. Overall, your organisation will need to achieve a suitable level of cyber security maturity for today's threat landscape.

What this could look like for your organisation

You might need to upgrade firewalls, deploy MFA tokens, redesign network architecture, and update policies to include AI risk controls. This could involve purchasing new technology, hiring specialists, and conducting audits.

Questions

1. Is your organisation already compliant with one, or more of these amendments? If so, which ones?
2. If you are not compliant with these amendments, which would be most challenging for you? Why?
3. What one-off costs would you expect (e.g., hardware/software upgrades, consultancy)?
4. What ongoing costs would you expect (e.g., monitoring, audits, licence renewals)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there any dependencies or constraints (e.g., physical configuration of OT/IT systems, vendor availability, certification cycles)?

Supply Chain Hazard Measures

Scenario

Your CIRMP would need to include a map of your critical suppliers, identify dependencies, and show steps taken to secure your supply chain. You would also need to assess foreign ownership, control and influence risks for vendors and apply additional security measures if high-risk vendors are unavoidable.

What this could look like for your organisation

You might need to implement supplier assurance questionnaires, maintain a database of critical suppliers, and introduce stricter procurement checks. If a vendor is high-risk, you may need to add compensating controls or diversify suppliers.

Questions

1. Is your organisation already compliant with one, or both, of these amendments? If so, please tell us which ones.
2. What changes would you need to make to your procurement or supplier management processes?
3. What one-off costs would you expect (e.g., mapping tools, supplier audits)?
4. What ongoing costs would you expect (e.g., periodic reviews, monitoring)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there practical limitations (e.g., lack of alternative suppliers)?
8. Would this limit the supply of good and services you provide, or potentially your competitiveness in the market? If yes, please describe how.

Personnel Security Hazard Measures

Scenario

As part of developing or implementing your personnel security plan you will need to undertake a stocktake of existing personnel security measures, guidelines, processes and frameworks. You will also need to identify which roles in your organisation are considered “critical workers”, and ensure those employees complete an AusCheck background check before commencing employment and are then subject to reassessment under AusCheck at regular intervals throughout employment.

What this could look like for your organisation

Your HR team might need to update onboarding processes, embed a security culture through the development of training and awareness programs**,** manage applications through AusCheck, establish reporting channels for security concerns or breaches, and track compliance. This could involve system changes, staff training, and handling delays if checks take time.

Questions

1. Is your organisation already compliant with this amendment, or does it have a similar onboarding process in place? Please describe the similar process if it exists.
2. What changes would you need to make to your HR or onboarding processes?
3. What one-off costs would you expect (e.g., system updates, training)?
4. What ongoing costs would you expect (e.g., fees per check, staff time)?
5. How did you estimate these costs?
6. How much time would you need to implement these changes?
7. Are there any challenges in defining “critical workers” for your organisation?

Attachment B – Policy design questions

All-hazard 1 – Consideration of specified risk advice

- Are there any controls on the scope of this measure that your organisation would suggest to assist with compliance and implementation?
- Could existing engagement mechanisms be adapted or improved to deliver more value, and support this obligation?

All-hazard 2 – All-hazard material risk

- Are there other specific material risks, like those arising from FOCI, that your organisation minimises or eliminates in their CIRMP?
- Does your organisation currently consider FOCI risks in their CIRMP?

Cyber 1 – Cyber security framework uplift

- Where applicable, what maturity/profile does your organisation seek to achieve?
- How does your organisation invest in security beyond achieving minimum cyber framework compliance?
- Does your organisation face challenges in obtaining the necessary investment in security to reach compliance, or (where necessary) go beyond the minimum cyber framework?

Cyber 2 – Critical systems network segregation

- What current measures does your organisation implement to segregate their critical systems from all other internet facing and less secure systems?
- Does your organisation mandate security awareness training for users with access to critical systems?
- What measures does your organisation undertake to log who has access and can make changes to your critical systems?

Cyber 3 – Multi-factor authentication (MFA)

- What type of systems in your organisation are currently protected by MFA?
- Are there system or/circumstances in which MFA is not reasonably practicable to use? If so, what other compensating controls are, or could be implemented?

Supply chain 1 – Supply chain vulnerability mapping

- To what level of upstream and downstream detail does your organisation currently map their supply chain?
- Does your organisation keep a list or record of alterative approved suppliers?
- Does your organisation have real-time access to data surrounding supplier availability?

Supply chain 2 – Vendors of concern

- How does your organisation currently map vendors of concern in your supply chain?
- What current security measures are put in place if a vendor of concern is identified?
- Does the wider government provide adequate material to support you to identify a vendor of concern and mitigate their potential impact?
- Are there other options to reduce the FOCI risk posed by vendors of concern, either in addition to or instead of the proposed approach?

Personnel 1 – Personnel Security Hazards

- Does your organisation have a personnel security plan, or equivalent in place?
- Would a personnel security plan requirement improve security posture or duplicate existing controls?
- Does your organisation currently use background checking as a security control?

- How many AusCheck background checks do you anticipate undertaking each year?
- What challenges do you foresee for your organisation to implement a personnel security plan?

Physical and Natural Hazards

- Does your organisation have a broader physical security plan?
- What type of physical security measure would be beneficial?
- Would a mandated physical security measure would be beneficial and how it could be effectively applied to your asset?
- Are there other additional material risks that your organisation considers could be included for physical or natural hazards?