CONSULTATION DRAFT v1

Security of Critical Infrastructure Act 2018 Reforms
DRAFT Risk Management Program Guidance

As at 30 September 2022

The Department is providing this document to you in **draft** to support your engagement in the Risk Management Program consultation process and so that you can advise what additional information you need. The Department will update this document for publication once Risk Management Program consultation has finished.

This document does not constitute legal advice. You should obtain independent legal advice if you have questions or concerns regarding your obligations under the *Security of Critical Infrastructure Act 2018* or the associated rules.

Contents

Glossary

ACIC –Australian Criminal Intelligence Commission.

ACSC – The Australian Cyber Security Centre.

ASIC – Aviation Security Identification Card.

ASIO – Australian Security Intelligence Organisation.

AusCheck – Background checking services for security-sensitive critical infrastructure sectors in Australia. AusCheck currently undertakes background checks for the aviation and maritime security identification cards (ASICs and MSICs), the national health security scheme, and checks for Major National Events. AusCheck background checking is also being proposed as a part of establishing a Naval Shipbuilding and Sustainment Identity Card (NSSIC) scheme for the Osborne Naval Shipyard (ONS) in South Australia under a separate rule under the SOCI Act.

Business critical data – has the meaning found in section 5 of the SOCI Act

C2M2 – Cybersecurity Capability Maturity Model.

Cyber and information security hazards – The sections of the RMP rules that relate to cyber and information security hazards.

Cyber frameworks – One of 5 outlined frameworks (or an equivalent framework) listed in the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022 (RMP Rules) that critical infrastructure assets must comply with within 18 months of the RMP Rules becoming legislation.

Cyber Reporting – Mandatory Cyber Incident Reporting. The Part 2B obligation under the SOCI Act.

DISER – Department of Industry, Science, Energy and Resources.

DITRDC - The Department of Infrastructure, Transport, Regional Development, and Communications and the Arts.

Government Assistance – Ministerial powers of last resort that allow the Minister to authorise the Secretary (or a delegate) to assist in preventing or stopping a significant cyber incident in cases where an entity cannot or will not act and may include information gathering, action directions or an intervention request.

Grace period – The period of time between the RMP Rules becoming legislation and compliance day for the relevant obligation. There is no legal expectation to comply with the obligation during this period, although preparations are strongly encouraged.

IACS – industrial automation and control systems.

IGIS – Inspector General of Intelligence and Security.

ISO – International Organization for Standardization. An independent international body that regulates a series of internationally recognised and domestically adopted standards.

ISMF – Information Security Management Framework

IT – Information Technology.

Material risk rules – The sections of the RMP Rules that relates to material risk.

MSIC – Maritime Security Identification Card.

MNE – the Major National Events security model. A similar model is proposed for use with the AusCheck Trusted Insider Check scheme.

OT – Operational Technology.

Part 2 – The Register of Critical Infrastructure Assets.

Part 2A – The risk management program.

Part 2B – Mandatory Cyber Incident Reporting.

Personnel security hazards – The sections of the RMP Rules that relate to personnel security hazards, including the requirement for ongoing checks of critical workers.

Physical security and natural hazards – The sections of the RMP Rules that relate to physical security and natural hazards.

PSOs – Positive security obligations. Three obligations that may be applied to asset classes of critical infrastructure under the SOCI Act using the Application Rules or the RMP Rules

PJCIS – Parliamentary Joint Committee on Intelligence and Security.

Relevant impact – has the meaning found in section 8G of the SOCI Act.

SCRI – Supply Chain Resilience Initiative.

Supply chain hazards – The sections of the RMP Rules that relate to supply chain hazards.

SLACI Act 2021 – the *Security Legislative Amendment (Critical Infrastructure) Act 2021.*

SLACIP Act 2022 – the *Security Legislative Amendment (Critical Infrastructure Protection) Act 2022.*

SOCI Act – the *Security of Critical Infrastructure Act 2018.*

Switch-on – the date that the rules for an obligation become legislation and the grace period commences.

TISN – The Trusted Information Sharing Network. A secure, non-competitive online environment for industry and Government to collaborate in and across sector groups. Further information on the TISN is available here: TISN engagement platform (cisc.gov.au).

The ANU Rules – the Security of Critical Infrastructure (Australian National University) Rules (LIN 22/041) 2022, a legislative instrument written under section 9 of the SOCI Act that prescribes the Australian National University as a critical infrastructure asset.

The Application Rules – the *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022*, a legislative instrument outlining the captured asset classes for the Part 2 (Register of Critical Assets) and the Part 2B (Mandatory Cyber Incident Reporting) obligations and the associated grace periods.

The Centre – the Cyber and Infrastructure Security Centre.

The Definition Rules – the Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021, a legislative instrument that further defines critical infrastructure assets captured by the SOCI Act.

The Department – The Department of Home Affairs.

The Minister – the Minister for the Department of Home Affairs.

The principal legislation – the piece of legislation that enables the legislative instruments, in this case the SOCI Act. It may also be used in connection with other legislation such as the *Telecommunications Act 1997*, which is the principal legislation for the telecommunications amendments.

The Secretary – the Secretary for the Department of Home Affairs.

The Register – The Register of Critical Infrastructure Assets. The Part 2 obligation under the SOCI Act.

The Rules – these are all the legislative instruments enabled by the *Security of Critical Infrastructure Act 2018.*

The RMP – The risk management program, also known as the Part 2A obligation under the SOCI Act. This refers to the RMP Rules as they relate to Part 2A of the SOCI Act.

The RMP Rules – the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022, a draft legislative instrument outlining the requirements for compliance with the Part 2A (risk management program) obligation under the SOCI Act.

TSSRs – the Telecommunications Sector Security Reforms. These reforms, also known as the *Telecommunication and Other Legislation Act 2017* amends the *Telecommunications Act 1997* to establish a regulatory framework to better manage the national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

Frequently Asked Questions

General

This section covers frequently asked questions on the *Security of Critical Infrastructure Act 2018* (the SOCI Act) and Risk Management Program.

Act, rules and reforms

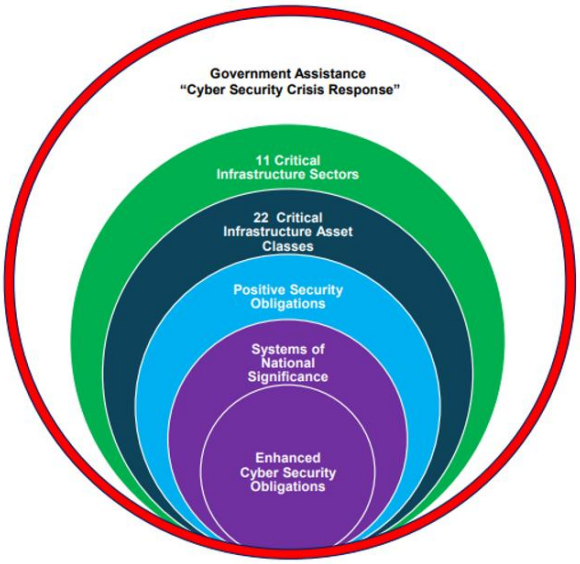
1. Why has the Government undertaken reforms to support the security of Australia's critical infrastructure?

   - Disruptions to critical infrastructure can have serious implications for business, governments and the community, affecting security of resources, supply and service continuity, and damaging economic growth. They could also have detrimental effects on business reputation and financial viability.
   - Over the 2020-21 period, the Australian Cyber Security Centre responded to over 1630 cyber incidents, with around one quarter of these impacting entities associated with Australia's critical infrastructure.
   - Over the past year the world has seen the impact of disruptions to critical infrastructure:
     - In the United States, the ransomware disruption to Colonial Pipeline affected fuel distribution, caused widespread panic, economic harm, and impacted food security by reducing point of contact availability for consumers.
     - Cyberattacks by malicious actors seeking to exploit and profit from the COVID-19 pandemic have targeted critical infrastructure assets, with total disregard for the cost to the community and the essential services that are provided by these assets.
   - Risks to critical infrastructure are not limited to cyber:
     - In Australia, COVID-19 caused drastic impacts to the supply chain for food and groceries. Australia's food security was harmed as essential goods were unable to be transported to point of contact for consumers. Flooding nationally compounded these issues, closing major roads, transport routes and train lines.
     - International geopolitical turmoil is also likely to have flow-on impacts to our critical infrastructure, including impacts on availability and price of fuel, or a decrease in global grain production.
     - The early-2022 floods and rain systems in Queensland and New South Wales are likely to continue to impact food and grocery supply in the coming months. Crops have experienced a shorter planting season with increased growth stress causing decreased yields and decreased nutrients, especially in grains. Health services in the region may see an increase in injuries, mosquito-borne diseases and infections due to the floodwaters and resulting environmental changes. There may also be flow-on effects to the health system from the impact to food and groceries.

2. Where can I find information on the Security of Critical Infrastructure reforms?

   - Information on the reforms is available on the Cyber and Infrastructure Security Centre website at https://www.cisc.gov.au/changes/overview.
   - The full text of the *Security of Critical Infrastructure Act 2018* (SOCI Act) is available on the Federal Register of Legislation at: https://www.legislation.gov.au/Details/C2022C00160.
   - The *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act 2021) as passed both by Houses of Parliament, can be found on the Federal Register of Legislation website at: Security Legislation Amendment (Critical Infrastructure) Act 2021. The explanatory memoranda can be found on the APH website at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

- The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act 2022) as passed both Houses, can be found on the Federal Register of Legislation website at: Security Legislation Amendment (Critical Infrastructure Protection) Act 2022. The explanatory memoranda can be found on the APH website at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6833.
- A visual summary of the changes under the critical infrastructure reforms, and how they relate to each other, is included below:



Systems of National Significance (SoNS) are a significantly smaller subset of critical infrastructure assets that are most crucial to the nation by virtue of their interdependencies across sectors and potential for catastrophic cascading consequences to other critical infrastructure assets and sectors if disrupted.

Enhanced Cyber Security Obligations may apply which will require a SoNS to:

1. develop, update and comply with a cyber security incident response plan;
2. undertake cyber security exercises to build cyber preparedness;
3. undertake vulnerability assessments; and
4. provide systems information

11 Critical Infrastructure Sectors: communications; data storage or processing; financial services and markets; energy; healthcare and medical; higher education and research; food and groceries; transport; space technology; defence industry

22 Critical Infrastructure Asset Classes that may be subject to positive security obligations:

Positive Security Obligations may include:

1. Requirement to provide operational and ownership information to the Register of critical infrastructure assets. *(commenced 8 April 2022, grace period to 8 October 2022 – 7 October for Telco assets under the Telecommunications Act 1997)*
2. Mandatory Cyber Security Incident Reporting *(compliance now in force)*
3. Requirement to have, develop and maintain a risk management program *(pending consultation)*
   - Rules to create baseline security standards – cyber and information; personnel; supply chain; physical and natural
   - Entities must identify and mitigate 'material risks' that have a substantial impact on the availability reliability and integrity of a critical

Government Assistance has commenced and applies to all critical infrastructure sectors and assets. It enables government to assist in the defence of critical infrastructure assets from cyber security threats, in light of their criticality to the socioeconomic stability, defence, and national security of Australia.

3. How are critical aviation and port assets covered?

- The Department is currently considering how the targeted critical infrastructure reforms for the aviation and maritime transport sectors will fit into the broader critical infrastructure, and aviation and maritime security agenda of the new Government.
- Currently, some obligations apply to critical aviation and port assets under the SOCI Act, as outlined in paragraph 10.

4. How are critical telecommunications assets covered?

- The Department is working closely with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) on developing amendments through the Telecommunications Sector Security Reforms (TSSR) and *Telecommunications Act 1997* to regulate critical telecommunications assets. These will regulate equivalent positive security obligations to those found under the SOCI Act (i.e. Risk Management Program) using this existing legislation and regulatory framework.
- Anticipated amendments to the Telecommunications Act are likely to include a strengthening of the TSSR provisions to align them to those required by other critical infrastructure assets under the SOCI risk management program obligations.
- Critical telecommunications assets will continue to be covered under the SOCI Act for the purposes of Systems of National Significance, Enhanced Cyber Security Obligations, and Government Assistance measures.
- See the Telecommunications Sector Security (TSS) page on the Cyber and Infrastructure Security Centre website for more information.

General information

5. What is a 'critical infrastructure asset'?

- Division 2 of the SOCI Act provides definitions for the 22 critical infrastructure asset classes.
- The Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 (the Definition Rules) outline further parameters to these definitions where applicable.
- Critical infrastructure assets also include assets privately declared by the Minister for Home Affairs (the Minister) under section 51 of the SOCI Act; or, prescribed, by legislative instrument, by the Minister under section 9 of the SOCI Act. Those assets privately declared are kept confidential. Legislative instruments are published on the Federal Register of Legislation and are publicly available.

6. What is a 'responsible entity'?

- A 'responsible entity' is an individual or organisation who owns or operates a critical infrastructure asset and may have obligations under the SOCI Act and associated Rules.
- The definition of 'responsible entity' differs for each asset class and can be found at section 12L of the SOCI Act.

7. I don't believe my asset is actually 'critical'. How do I clarify my obligations?

- The definitions for each critical infrastructure asset were developed through extensive consultation with industry and experts within and outside of government with the intent to capture all assets critical to the secure operation of Australia's key sectors.
- You should contact the Cyber and Infrastructure Security Centre if your asset is captured under the SOCI Act and associated Rules, and you do not believe it should be considered a critical infrastructure asset.
- While the Cyber and Infrastructure Security Centre will take into consideration submissions from industry that an asset is non-critical, only the Minister is empowered to make a determination that an asset is non-critical.
- Section 9(2) of the SOCI Act allows the Minister, via a rule, to prescribe that a specified asset is not a critical infrastructure asset.

8. Will entities that operate critical infrastructure assets need to inform third party holders of data that they are affected by the SOCI Act?

   - Yes, in accordance with SOCI Act section 12F(3), if you are a responsible entity and you use a data storage or processing service provider for your commercially-provided business critical data, you must take reasonable steps to tell them that you are operating a critical infrastructure asset.
   - A reasonable step might be for the responsible entity to discuss why the data is considered business critical with third party data holders in order to explain the associated risk that disclosure of this information could entail.

Your obligations and the risk management program under the SOCI Act

9. What is the risk management program obligation?

   - Part 2A of the SOCI Act sets out the requirement to adopt and maintain a critical infrastructure risk management program, and provides the legislative framework to allow the Minister to 'switch on' the obligation.
   - The draft *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022* (the RMP Rules) will specify requirements with which a critical infrastructure risk management program must comply[1].
   - The matters that an entity must consider when developing their risk management program is set out in paragraphs (d) - (i) of subsection 5(2) of the RMP Rules. These matters include whether the program has established and maintained a process for identifying:
     - the operational context for critical assets
     - interdependencies between critical assets
     - critical positions including persons responsible for the risk management program, persons responsible for minimising or eliminating risks and persons responsible for reviewing the program.
   - Further matters include whether the program contains principles of a reasonable risk management methodology and whether the program describes the circumstances in which the entity will review the program.

10. If my critical infrastructure asset is required to comply with the RMP Rules, do I need to comply with any other positive security obligations?

    - Possibly. A critical infrastructure asset may have multiple positive security obligations (PSOs) under the SOCI Act. These may include:
      - The Register of Critical Infrastructure Assets (Part 2). More information can be found here.
      - Mandatory Cyber Incident Reporting (Part 2B). More information can be found here.
      - The risk management program (Part 2A)
    - Before an obligation can apply to an asset, the Minister must make Rules outlining the obligations, and the asset classes to which the obligations will apply.
      - The Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 (the Application Rules) outline specific asset classes that are required to comply with the Mandatory Cyber Incident Reporting and the Register of Critical Infrastructure Assets Reporting Requirement. These Rules came into effect on 8 April 2022.
      - The draft RMP Rules outline asset classes covered by the Part 2A risk management program obligation.

[1] The RMP Rules and the switch-on of this obligation are subject to the approval of the Minister.

- The PSOs apply to specific asset classes under the SOCI Act, as outlined in the following table:

Sector	Asset Class	Register of Critical Infrastructure Assets	Mandatory Cyber Incident Reporting	Risk Management Program
Communications	Broadcasting	Yes	Yes	Yes
	Domain Name Systems	Yes	Yes	Yes
	Telecommunications	No^	No^	No^
Data Storage or Processing	Data Storage or Processing	Yes	Yes	Yes
Defence Industry	Defence Industry	No	No	No[1]
Energy	Electricity	Yes[2]	Yes	Yes
	Energy Market Operator	Yes	Yes	Yes
	Gas	Yes[2]	Yes	Yes
	Liquid Fuels	Yes	Yes	Yes
Financial Services and Markets	Banking	No	Yes	No
	Financial market Infrastructure (excl. Payment System Operators)	No	Yes	No
	Insurance	No	Yes	No
	Payment Systems	Yes	Yes	Yes
	Superannuation	No	Yes	No
Food and Grocery	Food and Grocery	Yes	Yes	Yes
Health Care and Medical	Hospitals	Yes	Yes	Yes
Higher Education and Research	Education	No	Yes	No
Space Technology	No defined Asset Class	No	No	No
Transportation	Aviation	No	Yes	No
	Freight Infrastructure	Yes	Yes	Yes
	Freight Services	Yes	Yes	Yes
	Public Transport	Yes	Yes	No
	Port	Yes[2]	Yes	No
Water and Sewerage	Water	Yes[2]	Yes	Yes

^ Telecommunications assets will comply with Register from 7 October 2022 and Cyber Reporting from 7 July 2022 under the *Telecommunications Act 1997*. TSSR obligations may be enhanced to equivalent to RMP obligations under amendments to the Tel Act

[1] The Minister for Home Affairs is considering making a specific rule under the Security of Critical Infrastructure Act 2018 (SOCI Act) declaring the Osborne Naval Shipyard a critical infrastructure asset, pending formal consultation.

[2] This requirement already applies under the *Security of Critical Infrastructure Act 2018*

11. If I operate a critical infrastructure asset under the RMP, do any other Rules apply to my asset?

- Possibly. If your business operates a critical infrastructure asset, you will be required to comply with the SOCI Act, and any Rules made under the Act that apply to your asset.
    - To date, Rules made under the SOCI Act include:
        1. Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021
            - These Rules further define or refine the critical infrastructure asset definitions for each asset class provided in the SOCI Act.

2. Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022
    - These Rules specify asset classes that are required to comply with the Mandatory Cyber Incident Reporting and the Register of Critical Infrastructure Assets Reporting Requirement.
3. Security of Critical Infrastructure (Australian National University) Rules 2022 (LIN 22/041) 2022
    - These Rules prescribe under section 9, that the Australian National University is considered a critical infrastructure asset under the SOCI Act.

- All Rules enabled by the SOCI Act can be found on the Federal Register of Legislation.

12. What is a 'critical infrastructure risk management program'?

Note: this question refers to the terms "relevant impact", "so far as it is reasonably practicable" and "material risk", these are defined in the following sections of this document.

- The critical infrastructure risk management program is intended to uplift core security practices that relate to the management of critical infrastructure assets. It aims to ensure responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating material risks from all hazards.
- Section 30AH of the SOCI Act defines a critical infrastructure risk management program.
- A critical infrastructure risk management program is a written program that applies to the responsible entity for a critical infrastructure asset. It must identify each hazard where there is a material risk that the occurrence of that hazard could have a relevant impact on the asset, and comply with requirements (if any) as specified in the rules.
- So far as it is reasonably practicable to do so – the risk management program must also minimise or eliminate any material risks of a hazard occurring and mitigate the relevant impact of such a hazard on the asset.
- Responsible entities are required to establish, maintain, and comply with a critical infrastructure risk management program to manage the 'material risk' of a 'hazard' occurring, which could impact the availability, integrity or confidentiality of the critical infrastructure asset.
- Responsible entities must manage risks by meeting the following principles-based outcomes:
    - **Effective governance** – Through the critical infrastructure risk management program, as defined in section 30AH of the SOCI Act, under section 30AG, entities will be required to provide an annual report to the relevant Commonwealth regulator or the Secretary. The report does not need to contain the full risk management program, but must be sufficient to assure the relevant Commonwealth regulator or the Secretary that the program remains up to date and appropriate.
    - **Identify material risks** – Responsible entities have a responsibility to take an all-hazards approach when identifying risks that may affect the availability, integrity, reliability and confidentiality of their critical infrastructure asset.
    - **Mitigate risks to prevent incidents** – Responsible entities will be required to consider risks to their entity and establish appropriate risk mitigation strategies to manage those risks so far as is reasonably practicable. Risk mitigation should consider both proactive risk management as well as establishing and managing processes to detect and respond to threats as they are being realised to prevent the risk from eventuating.
    - **Minimise the impact of realised incidents** – Responsible entities will be required to have robust procedures in place to: mitigate, so far as it is reasonably practicable, the impact should a hazard materialise, and recover from that impact as quickly as possible
        - Mitigations could include enhanced cyber security controls, background checking of critical personnel, having back-ups of key systems, ensuring adequate stock on hand in case of a disruption, installing redundancies for key inputs, out-of-hours processes and procedures, and the ability to communicate with affected customers, clients and agencies.

- The Cyber and Infrastructure Security Centre Factsheet on the risk management program can be found at: https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-risk-management-program.pdf

Material risks

13. Who is responsible for determining if a risk is a material risk?

- Responsible entities for critical infrastructure assets are responsible for determining if a risk is a material risk. Responsible entities for critical infrastructure assets must consider all relevant material risks to their business.
- In order to meaningfully uplift security and resilience, it is vital that responsible entities review their risk management program on a regular basis and take reasonable steps to ensure it is kept up to date. This ensures risk is being continually assessed and managed by the entity rather than taking a 'set and forget' approach to risk management.

14. When is a risk a 'material risk'?

- The SOCI Act requires responsible entities to adopt and maintain a critical infrastructure risk management program. The purpose is to ensure that responsible entities identify each hazard where there is a material risk that the occurrence of that hazard could have a relevant impact on the asset; and so far as it is reasonably practicable to do so, minimise or eliminate the material risk of such a hazard occurring, and mitigate the relevant impact of such a hazard on the asset.
- Responsible entities must take a principles-based approach to identifying the risks to the critical infrastructure asset.
- While responsible entities should take a broad approach to identifying material risk, the RMP Rules provide instances of material risks that must be considered; namely risks that:
    - impact Australia's social or economic stability, defence, or national security;
    - will result in major interruptions to the asset's function;
    - result in substantive loss of access to, or the manipulation of a critical component of the asset;
    - are introduced due to the storage, transmission or processing of sensitive operational information outside Australia;
    - result from remote access or interference with critical operational and information technology systems; or
    - arise from other material risks identified by the responsible entity as affecting the functioning of the asset.
- Responsible entities are responsible for determining if a risk is a material risk and should consider the likelihood of a hazard occurring, and the relevant impact on the asset or a critical component of the asset if a hazard were to occur.
- The Rules may state that the taking of specified action, minimises or eliminates any material risk or mitigates the relevant impact of a specified hazard on the critical infrastructure asset for the purposes of the critical infrastructure risk management program.

15. What is an example of a material risk?

- Some examples of a material risk could be:
    - the substantive loss of access to or deliberate or accidental manipulation of a critical component of the asset such as the position, navigation and timing systems impacting provision of a service or functioning of the asset; or
    - an impact resulting from the storage, transmission or processing of sensitive operational information outside Australia.

- Hazards which would have a significant impact but are incredibly improbable, or hazards that are highly likely but will have an inconsequential impact, are unlikely to be considered material risks. For example:
    - A critical infrastructure asset that is hundreds of kilometres inland would not be required to take steps to mitigate the significant physical impact of a tsunami on the asset.
    - Critical infrastructure assets operated within or below the stratosphere would not need to mitigate the significant physical impact of space debris on the asset.
- In contrast, the impact of a highly virulent, global pandemic on the availability of workforce, supply chain, and day-to-day operations of a critical infrastructure asset is an example of an unlikely event with a significant but mitigatable impact. In this instance, the event could be assessed as a material risk and would need to be addressed in a critical infrastructure risk management program.

16. Will material risk differ between entities?

- Yes. Responsible entities will need to take into consideration and recognise the specific context in which their business operates. This may be by size, maturity and/or likelihood of an incident occurring to determine their material risk and relevant impact.
- Entities should assess and mitigate risks as far as is reasonably practicable for their circumstances.

17. What is sensitive operational information?

- Sensitive operational information is information about the asset that, if shared outside of the organisation, could be used to manipulate the business, creating negative outcomes.
- For an asset specified in the RMP Rules, sensitive operational information includes, but is not limited to:
    - layout diagrams;
    - schematics;
    - geospatial information;
    - configuration information;
    - operational constraints or tolerances information; and
    - data that a reasonable person would consider confidential or sensitive about the asset.
- Information that is already in the public domain or is used to provide services to the public, including geospatial information, is not sensitive operational information.

18. What does 'so far as it is reasonably practicable' mean?

- Responsible entities within the operating context of their business will need to consider what is 'practicable' for their business. 'So far as it is reasonably practicable' allows entities an opportunity to determine how they address material risk and relevant impact in relation to their business size, maturity and income.
- For example, the RMP Rules do not contemplate that a small business compared with a large business will undertake the same measures to consider minimising or eliminating material risk, due to their differing operational context.
- The Cyber and Infrastructure Security Centre will take this into consideration when evaluating responsible entities' critical risk management program, and not hold every entity to the same standards, understanding the diversity of industry.
- Responsible entities should seek to minimise or eliminate material risk where it is reasonably practicable in order to secure their critical infrastructure asset.

Minimising and mitigating relevant impacts

19. What is a 'relevant impact'?

- Section 8G of the SOCI Act defines *relevant impact* of a hazard or cyber security incident on a critical infrastructure asset as the impact (whether direct or indirect) on the *availability*, *integrity*, *reliability* and *confidentiality of information* about the asset, information stored in the asset (if any) and, if the asset is computer data, the computer data.
- For instance, the relevant impact of a ransomware attack on a major telecommunications service provider could be that the telecommunications provider is taken offline or is unable to service customer demand, leaving millions of customers without regular service.
    - This amounts to a 'relevant impact' because the *availability* and *reliability* of the asset has been compromised.
    - A ransomware attack may also involve an unauthorised access to the systems of the service provider which could directly result in a compromise to the *confidentiality of information* held in its data centre, resulting in an impact on businesses ability to trust in the integrity of the data held in that facility.
- The relevant impact of a flash flooding event, in contrast, may have flow on effects to food and groceries and hospitals by cutting off supply chains between primary producers or distribution centres, and supermarkets or hospital point-of-care locations.
    - This amounts to a 'relevant impact' because the *availability* and *reliability* of goods provided by these chains has been compromised.
    - The integrity of freight services and freight infrastructure has also been compromised in this scenario through damage to road and rail, preventing goods from being transported effectively to both major and rural centres.

20. How do you describe relevant impact for availability, integrity, reliability and confidentiality?

- **Availability of an asset** is how accessible and usable the critical infrastructure asset is for authorised users or consumers whenever it is needed or required.
- **Integrity of an asset** is the critical infrastructure asset's capacity and ability to function efficiently, effectively and accurately and maintain the completeness of its data or information.
- **Reliability of an asset** is the critical infrastructure asset's capacity and ability to perform its functions consistently and dependably, without failure, over an extended period of time.
- **Confidentiality of an asset** is the critical infrastructure asset's capacity and ability to protect information from disclosure to unauthorised parties and preserve authorised restrictions on information access and disclosure, including protecting personal privacy, proprietary and any other information that could impact the critical infrastructure asset.

21. How do I minimise or eliminate relevant impacts?

- Responsible entities will be responsible for developing ways to minimise or eliminate any material risk of a hazard occurring, and mitigating the relevant impact of such a hazard on the asset.
- Businesses are best placed to determine ways to best minimise impact. The Cyber and Infrastructure Security Centre does not intend to provide specific guidance or direction on how to mitigate relevant impacts or material risks at this time.
- The Cyber and Infrastructure Security Centre will continue to actively assist business to understand the risk environment through sector specific risk advisories and providing updated threat information through the Trusted Information Sharing Network on a regular basis.

22. Implementation Timeline for the Risk Management Program

Timeframe	Requirements
Rules commence	Begin developing a risk management program in line with Part 2A of the SOCI Act and the RMP Rules.
	Begin identifying material risks, and thinking about the steps needed to minimise the risk of the hazards occurring, and mitigate the consequences should they occur (material risk rules).
In six months	Have and comply with a risk management program in line with Part 2A of the SOCI Act and the RMP Rules, including by: • Outlining in the risk management program, the **specified material risks** that affecting a critical infrastructure asset. Take steps to minimise the risk of the hazards occurring (likelihood) and mitigate the consequences (impact) should they occur (material risk rules) • Establish and maintain a process or system to minimise, mitigate or eliminate the relevant impact on the asset arising from the following (as outlined in the RMP Rules): ○ **Cyber and information security hazards** ○ **Personnel security hazards** ○ **Supply chain hazards** ○ **Physical and natural hazards**
Within 18 months[2]	Ensure that the risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks: • The Australian Cyber Security Centre's *Essential Eight Maturity Model* at maturity level one; • AS ISO/IEC 27001:2015; • The National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*; • The *Cybersecurity Capability Maturity Model* (C2M2) at Maturity Indicator Level 1; • Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or • an equivalent framework. **Note:** The latest version of these standards and frameworks should be considered, regardless of the language in this document or the Rules. Section 30AN and 30ANA of the SOCI Act provide for the incorporation by reference of these documents as in force from time to time.

[2] The 18 month timeframe for compliance with a cyber framework is the total period afforded to responsible entities under the draft RMP Rules. This takes into account the 6 month grace period and an additional 12 months. The 18 month period is for compliance with a cyber framework only. All other is the date from the switch-on of the obligation and the entering of the RMP Rules requirements must be included in the responsible entity's RMP within 6 months.

23. If my business has assets captured by multiple sectors, do I have to complete multiple critical infrastructure risk management programs?

- If your business is the responsible entity for one or more critical infrastructure assets you must adopt and maintain a critical infrastructure risk management program that applies to these assets.
- You could develop a single risk management program that covers all of your assets, including risks unique to each of the asset classes.

24. Can regulators request responsible entities to provide their full risk management program?

- The Secretary may request critical infrastructure risk management program documents from time to time as a part of its monitoring and compliance responsibilities.
- Under Section 37 of the SOCI Act the Secretary may, by notice in writing given to the entity, require the entity to produce documents, such as a critical infrastructure risk management program.
- Relevant Commonwealth regulators specified in the Rules are granted certain powers under the *Regulatory Powers (Standard Provisions) Act 2014* including but not limited to monitoring powers, investigation powers, civil penalty orders, infringement notices and enforceable undertakings.

25. How do I know if I am sufficiently managing risks?

- The Cyber and Infrastructure Security Centre **strongly recommends** that responsible entities for critical infrastructure assets work to secure their operations to the highest practicable standard.
- The conditions set in the SOCI Act and RMP Rules are a baseline only. Entities should look to incorporate security uplift into their business as usual and business continuity plans. Businesses could also join the Trusted Information Sharing Network (TISN) and engage with the national critical infrastructure community to help achieve risk and resilience uplift. Further information on the TISN is available here: TISN engagement platform (cisc.gov.au).

26. Is there a template for the risk management program?

- No. You may develop a critical infrastructure risk management program in the format that is suitable for your business and its operational needs.

27. Does an entity need to demonstrate third-party audit or certification to comply with the risk management program?

- No. An entity is not required to be certified or accredited as 'in compliance' to be complying with their obligations under the SOCI Act.
- Entities may consider undertaking third-party certification and auditing to ensure that their obligations are appropriately fulfilled and assets are appropriately protected; however, this is not a requirement for compliance with the Part 2A of the SOCI Act or the RMP Rules.
- The Department does not suggest that responsible entities attempt to certify against frameworks that do not already have certification or auditing capabilities in place.

28. What level of detail do I need to include in my critical infrastructure risk management program?

- A critical infrastructure risk management program must comply with requirements specified in the RMP Rules. All material risks to the asset, and their mitigation must be addressed so far as is reasonably practicable.
- The level of detail in a risk management program is determined by the individual entity, and will require the approval of your board, council or other governing body if you have one.

29. What if my business already complies with a requirement under the rules? Do I have to develop another risk management program or implement a new process?

- No. The Cyber and Infrastructure Security Centre is committed to allowing responsible entities the flexibility to decide how they discharge their obligations. Responsible entities can provide evidence that they already comply with the rules as a component of their risk management program. For example, if a state government regulator requires an entity to maintain a risk management program for cyber, personnel, supply chain and/or physical security hazards, the responsible entity would reference it in their critical infrastructure risk management program.
- In some instances, critical infrastructure assets will be covered by subsections 30AB (4), (5) and (6) of the SOCI Act. Entities covered by these subsections will only be required to submit an annual report under Part 2AA of the SOCI Act.

Reporting

30. What is the annual report?

- Under subsection 30AG(2) of the SOCI Act, responsible entities must provide an annual report relating to its critical infrastructure risk management program as evidence that the entity is meeting relevant obligations.
- In most cases the annual report will be submitted to the Department as the relevant regulator. However, if there is a relevant Commonwealth regulator that has functions relating to the security of your assets, the report will need to be submitted to them. For example, the Reserve Bank of Australia is the relevant Commonwealth regulator for payment systems operators[3].
- If the entity has a board, council or other governing body, the annual report must be approved by the board, council or other governing body.
- If the entity does not have a board, council or other governing body the annual report may be submitted by the company director or other authorised company officer.
- If a hazard has cause a significant relevant impact to one or more critical infrastructure assets the annual report for the responsible entity must include a statement that identifies the hazard, evaluates the effectiveness of the program in mitigating the impact of the hazard, and any amendments made to the program following the hazard.

31. Does every board, council or other governing body member need to sign?

- No. Responsible entities have the discretion to manage by their board, council or governing body as best suits their business and operational needs.
- For example, a responsible entity may decide that a majority vote to approve the risk management program is sufficient, following quorum rules for their organisation and provided the decision is noted by the organisation. Another responsible entity may decide that every member of their council must sign a document approving the risk management program.

32. What is the 'approved form' that I am required to deliver my annual report in?

- Paragraph 30AG(2)(e) of the SOCI Act requires annual reports regarding risk management programs to be submitted in the approved form.
- The Cyber and Infrastructure Security Centre will release this form prior to the risk management program obligations coming into effect.

[3] Subject to the approval of the Minister.

33. When do I need to submit my annual report to my regulator?

- Under 30AG(2) of the SOCI Act, responsible entities must submit a report to the relevant Commonwealth regulator within **90 days after the end of the financial year**.

34. How is the Department minimising duplicate regulation and reporting?

- When the Minister specifies requirements in rules made for the purpose of the Risk Management Program, the Minister is obliged to consider, amongst other things, existing regulatory systems of the Commonwealth, a state or a territory that impose obligations on responsible entities.
- The Department will continue to work to avoid duplicating obligations on entities in cases where a class of assets is already subject to a regulatory regime that comprehensively addresses the same outcomes as the SOCI Act.
    - These reforms were developed to address gaps in critical infrastructure security protection at both state and territory and federal level, as well as within industry. At time of writing, no state or territory regulatory scheme appropriately covers the all-hazards approach required under the SOCI Act.
- In some cases, responsible entities may be subject to existing regulation that only partially addresses the outcomes of this legislation.
    - To avoid a situation where an entity is required to deliver two separate risk management programs, the principles-based rules allow responsible entities flexibility to determine how they deliver a risk management program that would achieve all of the outcomes of the reforms.
    - For example, if you are a responsible entity developing a risk management program you may decide to incorporate existing regulatory compliance measures into your risk management program by reference.

Regulators

35. Who is my sector's regulator?

- The Department will be the **default** regulator for the all elements of the security of critical infrastructure reforms, including Risk Management Program obligations.
- The Minister may specify an alternative regulator through the rules. At present, it is only intended that the Reserve Bank of Australia operate as the relevant Commonwealth regulator for payment systems operators for the Risk Management Program.

Cost

36. What funds are available for businesses to implement these critical infrastructure reforms?

- At this stage the Government does not intend to provide funding to entities to implement and/ comply these reforms.
- All businesses will benefit from an uplift of security and resilience across critical infrastructure sectors, through enhanced reliability, continuity and security in the networks, systems and services they rely on, and the enhanced partnership with government these reforms, supported by the Trusted Information Sharing Network, will provide.
- Most aspects of the RMP Rules will be extensions of standard business as usual risk management practices.
- Government will aim to minimise costs and avoid regulatory duplication, to ensure that entities who take security seriously are not at a commercial disadvantage.

Other Commonwealth, and State and Territory requirements

37. Do I need to continue to comply with Commonwealth, State and Territory regulatory standards or similar that have similar obligations or objectives, such as licence conditions?

- Yes. If you are a responsible entity, you will need to continue complying with Commonwealth, state and territory regulations in addition to the Risk Management Program obligations. These reforms are designed to address gaps in existing legislation and do not replace or supersede existing Commonwealth, state and territory obligations.
- Actions undertaken by responsible entities to comply with existing Commonwealth, state and territory obligations **may** assist with meeting risk management program requirements.

38. I am required to align with Commonwealth, state or territory requirements for a certain hazard covered by the Rules. Is this sufficient for a risk management program?

- Compliance with another regulatory framework does not necessarily mean that an obligation is discharged under these reforms.
- Responsible entities must continue to comply with all relevant Commonwealth, state and territory requirements. Those requirements could be used as evidence of compliance with obligations under the RMP Rules and Part 2A of the SOCI Act.
- If you are currently required to do something that is equivalent to your requirements under the RMP Rules, referring to this Commonwealth, state or territory requirements is sufficient to the extent that it fulfils the obligation to establish and maintain a process or system to minimise, mitigate or eliminate the relevant impact on the asset arising from certain hazards.

Regulation, compliance and penalties

Compliance posture

39. What is the Cyber and Infrastructure Security Centre's approach to monitoring and compliance?

- The Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy (2022) outlines the Cyber and Infrastructure Security Centre's approach to regulation. Wherever possible, the Cyber and Infrastructure Security Centre will work in partnership with regulated entities to ensure they understand and are able to manage their own risk.
- The Cyber and Infrastructure Security Centre recognises that both educative and enforcement mechanisms are necessary to provide an effective and flexible regulatory system that does not unnecessarily impede the operations of regulated entities. The Cyber and Infrastructure Security Centre may use a number of regulatory options to address non-compliance, including: education and engagement, corrective action plans and enforcement orders.
- Should entities be found to be non-compliant, the Cyber and Infrastructure Security Centre aims to work with them in the first instance to better understand their circumstances and ensure that entities have the knowledge and education they need to appropriately comply with any obligations.

40. What are the compliance timeframes?

- Once the RMP Rules come into effect, there will be a period of time where responsible entities are not required to comply with an obligation. This is referred to as a 'grace period'.
    - 6 months from 'switch-on' (or 6 months from first day of operation for new operators), with an additional 12 months to comply with the chosen cyber framework/standard.
        - Compliance with personnel hazards, supply chain, and physical and natural hazards, and risk mitigation for cyber and information security hazards, must be demonstrable by the end of the 6 month grace period.

- Entities must provide an annual report within 90 days of the first end of financial year after compliance day for the risk management program obligation. If the end of the financial year falls within the 6 month grace period, entities should provide their annual report at the beginning of the following financial year.

Penalties

41. Are individuals liable for Risk Management Program penalties?

- No. Civil penalty provisions in relation to the Risk Management Program framework relate only to the actions of responsible entities, not individuals.
- The 2022 amendments introduce a range of civil penalties for non-compliance with the SOCI Act, including failure to adopt and maintain a risk management program, failure to comply, review, and update a risk management program and failure to make an annual report.
- Civil penalties range up to 200 penalty units.
- Currently, one penalty unit is $222.

Information use and protected information

This is a brief introduction to protected information as it relates to the RMP obligation. Further advice can be found in the Use and Disclosure of Protected Information fact sheet and the draft document Protected Information Guidance Material.

42. What is 'protected information'?

- Protected information is defined in section 5 of the SOCI Act. Relevantly, it includes a document or information that:
  - Is (or is included in) a critical infrastructure risk management program that is adopted by a responsible entity;
  - Is (or is included in) an annual report relating to the risk management program obligation;
  - Is obtained by a person in the course of exercising powers, or performing duties or functions, under the SOCI Act.
- Penalties for unlawfully disclosing protected information can be up to 120 penalty units, 2 years imprisonment, or both.
- An entity is authorised to use and disclose protected information under Division 3, Part 4 of the SOCI Act to certain people in certain circumstances. In general, an entity is authorised to disclose protected information for the purpose of ensuring compliance with their obligations under the SOCI Act.
- As long as the entity can identify a relevant purpose under one of the authorisations in Part 4 and where required discloses to one of the specified entities, an entity is authorised to disclose that information.
- The Secretary (or a delegate) may also disclose protected information to certain specified persons and government officials under Division 3, Part 4 of the SOCI Act.

43. When can protected information generally be disclosed?

- In general terms, the authorisation under section 41 of the SOCI Act enables the use and disclosure of protected information by an entity for the purposes of exercising powers or performing functions or duties under the SOCI Act, or ensuring compliance with the SOCI Act.

Example: Protected information of a critical asset may need to be shared with contractors, consultants and government bodies where the entity must adopt, maintain, comply with, review or update a critical infrastructure risk management program under Part 2A of the SOCI Act.

- An entity will also be authorised to disclose protected information that relates to itself if the disclosure is made to a Commonwealth, state or territory minister with the responsibility for regulatory oversight of the relevant critical infrastructure sector, or a member of their staff, or the head of an agency (or staff member) administered by the Minister (section 43E(1) of the SOCI Act). The disclosure must be for the purposes of enabling or assisting the person to exercise their powers or perform the person's functions or duties.

44. Who should I contact if I have questions about protected information?

- If you are an entity, including a business, and you believe you have a need to make a record of, or use or disclose protected information, you can contact the Cyber and Infrastructure Security Centre at **enquiries@CISC.gov.au**.
    - Further details on this process can be found in the Protected Information Guidance Material.

CONSULTATION DRAFT v1

Risk Management in Practice

The RMP Rules require responsible entities to address risks across four hazard vectors: cyber and information, personnel, supply chain and physical and natural. The following FAQs have been chosen to assist organisations to assess these hazards in their risk management programs.

Cyber and information security hazards

45. I have my own cybersecurity policies in place. Do I still have to comply with one of the frameworks specified in the RMP Rules?

- Yes. The rules require you to comply with a framework including conditions (if any), to ensure that there is a baseline level of cybersecurity across all critical infrastructure assets.

46. What are the cyber and information security hazards frameworks in the RMP Rules?

- Under the RMP Rules responsible entities must comply with a framework contained in one of the following documents or an equivalent. Responsible entities should ensure that if they chose an equivalent framework they justify the use of this framework.
    - ***Essential Eight Maturity Model*** **published by the Australian Signals Directorate** – a maturity assessment that sets out cyber risk mitigation strategies for organisations to implement to meet their identified target maturity level. The Essential Eight was designed to protect Microsoft Windows–based internet-connected networks and it is aligned with C2M2.
    - **AS ISO/IEC 27001:2015 – Information Security Management Systems –** a standard that specifies the requirements for establishing, implementing, maintaining and continually improving information security management systems within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.
    - ***Framework for Improving Critical Infrastructure Cybersecurity*** published by the National Institute of Standards and Technology of the United States of America – a framework that sets out standards, guidelines and practices for owners and operators of critical infrastructure to implement to manage cybersecurity risks according to their unique risk profile, to meet an identified implementation tier. It was designed to protect the information security systems of government agencies.
    - ***Cybersecurity Capability Maturity Model*** **published by the Department of Energy of the United States of America** – a maturity assessment that provides tools to evaluate, implement and manage cybersecurity practices associated with information technology (IT) and operations technology (OT) assets. It was originally designed for the US energy sector. It is aligned with the NIST Cybersecurity Framework.
    - ***The 2020-21 AESCSF Framework Core*** **published by Australian Energy Market Operator Limited** – a cyber-security maturity and uplift capability assessment model, designed for the Australian energy sector. It is aligned with C2M2 and references standards such as IEC 27001.
- In addition to the frameworks listed, the Department **recommends** that responsible entities investigate the below frameworks and standards when developing their critical infrastructure risk management program. This list will be updated over time.
    - Organisations utilising operational technology should consider implementing the IEC 62443 series – *Industrial Automation and Control Systems (IACS) Security* – a series of standards for addressing and mitigating current and future security vulnerabilities in industrial automation and control systems. This standard is broadly aligned with ISO 270001.

47. Does an entity need to demonstrate certification against a cybersecurity framework to be in compliance with the rule?

- No. An entity will be considered to be complying with a cybersecurity framework/standard if they are following and adhering to the chosen framework/standard in good faith.
- An entity is not required to be certified or accredited as 'in compliance' with the chosen framework/standard for the purposes of the risk management program, although it is noted that some entities may already be 'in compliance' with the AS ISO/IEC 27001 standard as part of their existing business requirements.
- The Department **recommends**, but does not propose to require, responsible entities undertake third-party certification and auditing where an appropriate and existing certification process exists.
- The Department does not suggest that entities attempt to certify against frameworks that do not already have recognised certification or auditing capabilities in place.

48. What constitutes 'an equivalent framework'?

- Equivalent frameworks *must at least meet* the cyber security levels provided by the other specified frameworks/standards.
- Responsible entities should be able to justify to their board, council or other governing body that the cybersecurity framework/standard chosen meets or exceeds the level of cybersecurity protection afforded by the frameworks outlined in section 7(4)(b) of the RMP Rules.
- The Cyber and Infrastructure Security Centre **recommends** that any frameworks chosen should be promulgated by a government (such as with the United States Cybersecurity Capability Maturity Model) or international organisation (such as the International Organization for Standardization) wherever possible.
- The Cyber and Infrastructure Security Centre **recommends** responsible entities justify their equivalency in their critical infrastructure risk management program.
- The acceptability of one state or territory framework does not, by default, mean that other frameworks (such as cyber security requirements) are functionally equivalent. Responsible entities should assess their existing cyber security standards against the framework/standard specified in the RMP Rules, *not* any other state or territory requirement.

49. Do my IT systems need to meet the same cyber security frameworks/standards as my OT systems?

- Entities should apply the same security standards to their IT systems if those IT systems support critical infrastructure asset operations.
- For example, if an entity uses cloud-based asset and works software to dispatch crews to repair its network, then that cloud-based asset and works system should have the same security controls applied because it is essential to the delivery of the function of the entity.
- Entities must fully implement any controls outlined in their chosen framework/standard for both information and operational technology.
- It is **strongly recommended** that also you seek specific advice for any operational technology systems used for your critical infrastructure asset as hostile actors have been shown to be able to exploit both IT and OT vulnerabilities, particularly when these systems are not siloed.

Personnel hazards

General information

50. What is a 'critical worker'?

- A critical worker is defined in section 5 of the SOCI Act as an individual, who is an employee, intern, contractor or subcontractor of the responsible entity for a critical infrastructure asset to which Part 2A applies (critical infrastructure risk management programs) whose absence or compromise would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the entity, and the individual has access to, or control and management of, a critical component of an asset.
- In practice, this could include roles such as Chief Information Security Officer or Control Room Operator or workers such as IT administrators with full and unrestricted administrator rights and access to the systems (sometimes referred to as 'god-mode' or 'unlimited' access).
- The Cyber and Infrastructure Security Centre believes that entities are best placed to understand the criticality of their operations and employees. Businesses will be ultimately responsible for this assessment.

51. What is a malicious insider?

- Malicious insiders are individuals such as employee, employees, intern, contractor or subcontractor, or anyone formerly engaged in these roles who have legitimate access to your systems and data, but use that access to destroy data, steal data or sabotage your systems.
- It does not include well-meaning staff who accidentally put your cyber security at risk or spill data.

52. Will the rules relating to personnel hazards apply to both new and existing employees?

- Yes. It is the responsibility of each entity to determine how to implement these rules within their own operations, considering contracts and enterprise agreements as appropriate.

53. Whose responsibility is it to manage personnel security hazards for short-term employees, such as subcontractors and contractors hired for shutdowns and closures?

- Responsible entities must implement methods to ensure the security of short-term employees, including subcontractors and contractors. Responsible entities are best positioned to develop these methods within their own businesses.
- It is the responsibility of each entity to manage personnel, regardless of their length of employment.
    - For example, short-term contractors must be held to the same standard as permanent employees filling similar positions.

54. What standards and frameworks are recommended?

- The Department recommends that responsible entities investigate and consider the below-listed standards when developing their risk management program. This list will be updated over time.
    - AS 4811 – Employment Screening
    - HB 323 – Employment Screening Handbook.
    - HB 167 (Security Risk Management)
    - The Information Security Management Framework (ISMF) Part 10 – Workforce Management Security.
    - AS/NZS ISO/IEC 27002 – Information technology – Security techniques –Code of practice for information security controls – 'Human Resources Security'.

- AS 8000 – Fraud and Corruption Control.

AusCheck and Ongoing Background Checks

The AusCheck Branch in the Department of Home Affairs is proposing a specific treatment of trusted-insider risks in Australia's security-sensitive critical infrastructure sectors through a new Critical Infrastructure Trusted Insider Check. The new scheme has not yet been formally endorsed by the Government therefore the following reflects the proposed design for AusCheck's service delivery to new critical infrastructure stakeholders.

55. Who needs to undertake an AusCheck background check?

- The RMP Rules require that a responsible entity for a critical asset manage the risks their critical workers may represent to that asset.
- Responsible entities may elect to conduct AusCheck background check under their critical risk management program.
- It is not a legislative requirement that these checks are done under the AusCheck scheme. It is the advice of the Department that checks provided by external providers should be approximately equivalent to the proposed AusCheck background check.

56. Where can I find more information about AusCheck?

- Further information can be found at https://www.auscheck.gov.au/.
- *Note: the framework for AusCheck background checking was released for consultation along with the Risk Management Program rules. A copy of the framework is available here. We encourage you to review the framework and consider providing a submission before formal consultation concludes on 4 November 2022. Feedback provided on the framework will inform future amendments to the AusCheck Regulations 2017 and the final AusCheck background checking process.*

57. What is included in an AusCheck background check?

- If a responsible entity adopts the AusCheck scheme, ongoing checks must include:
  - an identity-verification check undertaken by the Department;
  - a national security assessment conducted by the Australian Security Intelligence Organisation (ASIO);
  - an Australian criminal history check undertaken by the ACIC, with any history assessed by the Department against specified 'security-relevant' offence criteria; and
  - an immigration and right-to-work check undertaken by the Department.

58. What will the assessment criteria be for an AusCheck background check?

- AusCheck organises and coordinates the national security assessment conducted by ASIO in accordance with Part IV of the *Australian Security Intelligence Organisation Act 1979*.
  - ASIO national security assessments are not character checks and factors such as criminal history, dishonesty or deceit are only relevant to ASIO's advice if they are linked to national security threats including:
    1. espionage;
    2. sabotage;
    3. politically motivated violence;
    4. promotion of communal violence;
    5. attacks on Australia's defence system; or

6. acts of foreign interference.

- If ASIO issues an adverse security assessment about someone, that person will be advised, and they can appeal the assessment through the Administrative Appeals Tribunal.

- AusCheck organises and coordinates a criminal history statement of findings using information collected by the ACIC. ACIC collects this information from Australia's federal, state and territory criminal history data bases AusCheck takes the ACIC findings and filters them through to the responsible entity as a category of offence[4].

59. One of my staff has been convicted of a relevant offence. Am I required to terminate their employment?

- The onus is on the responsible entity to assess whether an employee poses a material risk based on AusCheck or other ongoing check advice, and undertake any action to minimise, mitigate, or eliminate that risk.
  - For example, action could include reassignment to another area of the business, dual authorisation, or restricted duties. Such strategies must be outlined as part of the entity's risk management program.
- Please note that responsibilities of employers under the *Fair Work Act 2009*, Work Health and Safety legislation, or any relevant laws must still be followed. An employee who is subject to action as a result of an employer's background check, AusCheck or otherwise, is protected by all existing rights at work, such as the right to appeal a decision with the Fair Work Tribunal.

60. How long is an AusCheck background check valid for?

- Under existing schemes, an AusCheck background check is currently valid for 2 years. The Department is proposing to apply the same duration of validity for an AusCheck background check for critical infrastructure.

61. How long does an AusCheck background check take to complete?

- On average AusCheck finalises 80 percent of background checks within 2 weeks of receiving the application from the organising body.
- Some applications may take longer to process depending on the complexity of the applicant's specific circumstances. Delays to processing times can be caused by inaccurate or incomplete information provided at the time of application and other factors beyond our control, such as a need to obtain court transcripts.

62. How much will an AusCheck background check cost?

- Actual costs for new critical infrastructure operators required to comply with the RMP rules will be confirmed during the co-design process for the AusCheck Regulations.
- For reference, an AusCheck background check for the aviation and maritime security identification (ASIC and MSIC) schemes have historically cost approximately $92.50[5].

63. What will the outcome of the AusCheck background check look like?

- Responsible entities will receive an advice outcome which will list any offences that reach the thresholds.

[4] The proposed rule includes a list of proposed offences (Schedule 1).

[5] This is currently under review, and any costs for the CITIC will align with any changes made to other schemes.

- Information provided through a background check is bound by the *Privacy Act 1988*. If the responsible entity requires further information or assessment this may need to be obtained from the person of relevance.
- AusCheck will not issue a physical card, or require employers to issue a physical card to demonstrate that a person has completed an AusCheck background check.

64. Are there ongoing Personnel Hazard obligations after receiving an AusCheck background check or other background check?

- Yes. Under 8(2)(b) of the draft RMP Rules, responsible entities must assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset.
- Responsible entities should determine how this looks for their critical infrastructure asset.

65. What privacy provisions are in place to protect AusCheck background check applicants?

- If an AusCheck background check identifies that a person:
  - has an adverse national security assessment by ASIO; and /or
  - has be found to have been convicted of Critical Infrastructure security-relevant offences (proposed new Schedule 2) of the AusCheck Regulations 2017; and /or
  - not have a legal right to work in Australia; and/or
- That person's employer and the responsible entity (where different) will be provided with general advice *only* to help them manage the associated risks in alignment with the entities risk management program.
- In the interests of personal privacy, where ACIC has returned documents of relevant offences AusCheck provides these findings to the responsible entity only as a category of offences against the schedule of security relevant offences[6].
- Personal details submitted by the applicant to AusCheck will not be provided to their employer without their consent.

66. Some of my critical workers have an Australian or foreign government security clearance. Do they still need to undertake an AusCheck background check or other background check?

- No. Under 8(2)(b) of the draft RMP Rules, responsible entities must assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset.
- Provided that this subsection is met through ongoing clearance, there is no requirement to undertake an addition background check.
- Where a responsible entity determines that an Australian security clearance is a suitable form of background check, they may choose to use this check as their principal vetting control. There is no obligation to undertake an official security clearance if the responsible entity does not deem it is necessary to mitigate their material risk.

Supply chain hazards

67. How far down a supply chain do I have to consider?

- It is the responsibility of each entity to determine how 'far down' the supply chain it chooses to consider relevant when determining supply chain hazards.

[6] The proposed rule includes a list of offence (Schedule 1).

- Responsible entities should consider the likely relevant impact a business may have on the entity's operational function and risk to supply chain when deciding how far down a supply chain to consider.
- The Department encourages responsible entities to have collaborative discussions with their relevant goods and services providers regarding plans to manage risk and potential impact on the supplier.
- Under the RMP Rules, responsible entities' critical infrastructure risk management programs must have processes or system to minimise, eliminate, or mitigate the following risks:
    - unauthorised access or exploitation
    - misuse of access to the supply chain by an authorised provider
    - sanctions of the asset due to supply chain issues
    - threats to supply chain personnel, products services and supply chain intellectual property
    - high risk vendors and any failure of any entity's suppliers and providers
- These categories have been provided to ensure entities are able to determine what they need to consider to sufficiently reduce risks to their supply chains and their operational continuity.
- The Department of Industry, Science, Energy and Resources (DISER) leads the Supply Chain Resilience Initiative (SCRI). Through this initiative, DISER works with industry to build an understanding of supply chains for critical products and identify options to address vulnerabilities. Further information on the SCRI is available here.

68. What is a 'high risk vendor'?

- A high risk vendor is any vendor that by nature of the product or service they offer, has a significant influence over the security of an entity's system.
- An example of a risk may be that a vendor may be subject to adverse external interference due to poor security controls. This means the vendor may transfer unreasonable risk to an entity's systems.

69. What standards and frameworks are recommended for supply chain hazards?

- The Department **recommends** that responsible entities investigate and consider the below supply chain frameworks and standards when developing their risk management program.
- This list will be updated over time. Entities are not required to be certified against any of these frameworks to comply with this rule.

Note: The following documents are referred to in such a way that some or all of their content constitutes guidance or requirements. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 27036 – Securing supplier relationships.
- ISO 28000 – Specification for security management systems for the supply chain.
- ISO 28001 – Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance.
- ISO 28002 – Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
- Australian Cyber Security Centre – *Identifying Cyber Supply Chain Risks*.
- National Institute of Science and Technology – NIST Special Publication 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.
- National Institute of Science and Technology – NISTIR 8276 – *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.*
- (UK) National Cyber Security Centre – *Supply Chain Security Guidance (12 Principles).*

Physical and natural hazards

70. What are physical security hazards and natural hazards?

- **Physical security hazards** include the unauthorised access, interference, or control of critical assets, other than those covered by cyber and information security hazards, including where persons other than critical workers act, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset, as assessed by the entity.
    - These are impacts on the entity's physical environment and could include occurrences such as breaking into a facility or a restricted area, theft of materials or computer assets, damage to or sabotage of physical equipment, or unauthorised operation of a control centre.
- **Natural hazards** include bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis or health hazards (such as a pandemic).
    - These are natural phenomena that may have a negative impact on humans or animals, the environment, facilities or equipment. Natural hazards include severe weather and health hazards, which have the potential to pose a significant threat to human health and safety, property, critical infrastructure, and national security. Natural disasters occur both seasonally and without warning, subjecting the nation to frequent periods of insecurity, disruption, and economic loss. Natural hazard events can be classified into two broad categories: geophysical and biological.
        - Geophysical natural hazards could include earthquakes, heat waves, bushfires, floods, drought, high winds and severe storms.
        - Biological hazards can include pandemics and diseases, including those generated by or related to the operation of an asset, such as sewerage.
- Physical and natural hazards do not need to be declared disasters by the Government to be considered material risks.
- The Cyber and Infrastructure Security Centre intends that responsible entities will evaluate their operating environment and consider what physical and natural hazards would be applicable to their unique operating environment.

71. How do I mitigate against physical and natural security hazards?

- To mitigate against physical and natural hazards, consider the following types of measures:
    - Locking down industrial control systems, including cameras, fire alarm panels from access privileges and onsite security;
    - contingency planning, emergency exercises and simulations;
    - De-clustering of key assets i.e. spreading infrastructure across multiple sites and maintaining backup infrastructure to increase resilience.

72. Do I have to consider all possible physical and natural hazards to my asset?

- Only so far as is reasonably practicable. Not all physical and natural hazards are of equal likelihood or consequence. Responsible entities must consider their assets' individual circumstances when evaluating hazards.
- Not all hazards will require mitigation to the same level; for example, an asset located in the Blue Mountains would likely consider bushfires at a different risk level to an asset located in a metropolitan area.
- You should consider how physical and natural hazards might indirectly affect your operations, including impacts on supply chains.

73. What is a 'critical site'?

- A 'critical site' is the part of the critical infrastructure asset that is a site or part of a critical infrastructure asset of critical importance to the function, performance and/or ongoing viability of the critical infrastructure asset. This should be identified by an entity's resilience, operations, or engineering department and acknowledged or approved by an entity's board (or other governing body).
- Sites should be assessed on a case-by-case basis; what may be a critical site for one responsible entity may not reach the threshold for another entity. The criticality of a site will be determined by what impact the loss or impairment of the site or part of a critical infrastructure asset would have on a critical infrastructure asset.
    - For example, two responsible entities for critical electricity assets may hold two premises a power station and a commercial front office. One responsible entity may be able to influence operation of their power station from the commercial front office and deems both premises to be critical sites. In contrast, the other responsible entity may decide that their power station is a critical site but their commercial front office is only used for paperwork and engagement and is therefore not a critical site.

Consultation and feedback

74. What formal consultation mechanisms are available for the critical infrastructure risk management program?

- Subsection 30AL(2) of the SOCI Act provides that, before making or amending the RMP Rules, the Minister must publish a notice on the Department's website setting out the draft rules and inviting persons to make submissions to the Minister about the draft rules during a minimum 28 day consultation period.
- The Minister must also give a copy of the notice to each First Minister (which is defined in section 5 of the SOCI Act to mean the Premier of a State, or the Chief Minister of the ACT or the NT).
- The Minister may extend this period should they deem it appropriate.
- Details for how to make submissions will also be published on the website.
- In accordance with section 30AL(4)(a) and (b) of the SOCI Act, these consultation requirements do not apply if the Minister is satisfied that there is an imminent threat that a hazard will have a significant relevant impact on a critical infrastructure asset or that a hazard has had, or is having, a significant relevant impact on a critical infrastructure asset.
    - A significant impact is one where both the critical infrastructure asset used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of the essential goods or services delivered by a critical infrastructure asset – such as a critical cyber security incident impacting an electricity asset's operational technology which impacts the generation, transmission, or distribution of electricity.
    - A relevant impact is one that impacts the availability, integrity, reliability or confidentiality of your asset – such as a cyber security incident impacting a bank's corporate network in a manner that could expose information about the asset but not impact the provision of banking services.

75. How can I provide general or consultation-specific feedback to the Cyber and Infrastructure Security Centre?

- The Department welcomes feedback on reforms to the SOCI Act at any time to ci.reforms@homeaffairs.gov.au.

76. What future consultation is planned?

- The period of consultation for the draft RMP Rules will be 45 days, longer than the 28 days or more provided for in the SOCI Act.
- Consultation will involve engaging industry through the Trusted Information Sharing Network, town halls, q & a sessions, roundtables, bilateral meetings, emails and updates to the Cyber and Infrastructure Security Centre website.
- The Cyber and Infrastructure Security Centre will continue to provide support to entities in developing their risk management programs after the consultation period, through the Trusted Information Sharing Network, Cyber and Infrastructure Security Centre website and through guidance materials including case studies.

Useful resources

This section provides a list of resources to consider when implementing a risk management program.

Security of Critical Infrastructure reforms

- Information on the reforms is available on the Cyber and Infrastructure Security Centre website at: Critical Infrastructure (cisc.gov.au)
- The full text of the *Security of Critical Infrastructure Act 2018* is available on the Federal Register of Legislation at: Security of Critical Infrastructure Act 2018 (legislation.gov.au)
- The full text of the *Security Legislation Amendment (Critical Infrastructure) Act 2021* is available on the Federal Register of Legislation at: Security Legislation Amendment (Critical Infrastructure) Act 2021
    - The SLACI Bill 2021 as passed by both Houses of Parliament, and explanatory memorandum (including revised and supplementary explanatory memorandum) as introduced into the House of Representatives can be found on the APH website at: Security Legislation Amendment (Critical Infrastructure) Bill 2021
- The full text of the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* is available on the Federal Register of Legislation at: Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
    - The SLACIP Bill 2022 as passed by both Houses, and the explanatory memorandum (including revised, supplementary and addendum explanatory memorandum) as introduced into the House of Representatives can be found on the APH website at: Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022
- Information on legislative instruments enabled by the principal legislation (the SOCI Act), is available of the Federal Register of Legislation at: https://www.legislation.gov.au/Series/C2018A00029/Enables
- Information on the Definition Rules is available of the Federal Register on Legislation at: Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 (legislation.gov.au)
- Information on the Australian National University Rules is available on the Federal Register of Legislation at: Security of Critical Infrastructure (Australian National University) Rules (LIN 22/041) 2022 (legislation.gov.au)
- Information on the Part 2B *Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022* is available on the Federal Register of Legislation at: Security of Critical Infrastructure (Application) Rules (LIN 22/026) 2022 (legislation.gov.au)

Cyber and Infrastructure Security Centre information

- Cyber and Infrastructure Security Centre's Compliance Strategy: Critical Infrastructure Centre Compliance Strategy (cisc.gov.au)
- The Department welcomes feedback on reforms to the *Security of Critical Infrastructure Act 2018*. Please email CI.reforms@homeaffairs.gov.au
- You can contact the Cyber and Infrastructure Security Centre at: enquiries@CISC.gov.au

Cyber and information security hazard frameworks

- ***Essential Eight Maturity Model*** **published by the Australian Signals Directorate** – a maturity assessment that sets out cyber risk mitigation strategies for organisations to implement to meet their identified target maturity level. The Essential Eight was designed to protect Microsoft Windows–based internet-connected networks and it is aligned with C2M2.
- ***AS ISO/IEC 27001:2015 – Information Security Management Systems*** – a standard that specifies the requirements for establishing, implementing, maintaining and continually improving information

security management systems within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.

- ***Framework for Improving Critical Infrastructure Cybersecurity*** published by the National Institute of Standards and Technology of the United States of America – a framework that sets out standards, guidelines and practices for owners and operators of critical infrastructure to implement to manage cybersecurity risks according to their unique risk profile, to meet an identified implementation tier. It was designed to protect the information security systems of government agencies.
- ***Cybersecurity Capability Maturity Model*** **published by the Department of Energy of the United States of America** – a maturity assessment that provides tools to evaluate, implement and manage cybersecurity practices associated with information technology (IT) and operations technology (OT) assets. It was originally designed for the US energy sector. It is aligned with the NIST Cybersecurity Framework.
- ***The 2020-21 AESCSF Framework Core*** **published by Australian Energy Market Operator Limited** – a cyber-security maturity and uplift capability assessment model, designed for the Australian energy sector. It is aligned with C2M2 and references standards such as IEC 27001.

General cyber and information security standards and guidance

- ACSC Small Business Cyber Security Guide: https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide)
- ACSC Know how to spot phishing (scam) messages: https://www.cyber.gov.au/acsc/view-all-content/campaign/know-how-spot-phishing-scam-messages
- NAB Cyber Safety Training for Businesses: https://www.nab.com.au/about-us/security/cyber-safety-training-modules
- ACCC's Small Business Education program – Scams: https://www.accc.gov.au/about-us/tools-resources/cca-education-programs/small-business-education-program/scams
- ACSC Information Security Manual: https://www.cyber.gov.au/acsc/view-all-content/ism
- ASIC Cyber Resilience: https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/
- ACSC Step-by-step guides: https://www.cyber.gov.au/acsc/small-and-medium-businesses/step-by-step-guides)
- ACSC Securing your business tools: https://www.cyber.gov.au/acsc/small-and-medium-businesses/securing-your-business-tools
- ACSC Quick wins: https://www.cyber.gov.au/acsc/small-and-medium-businesses/quick-wins)
- ACCC Scamwatch: https://www.scamwatch.gov.au/
- ASIO Outreach: https://www.outreach.asio.gov.au/
- ASIO Think Before You Link: ASIO - Think before you link - Online networking guide
- ACSC Annual Cyber Threat Report, 1 July 2020 to 30 June 2021 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21
- ACSC ReportCyber Portal: https://www.cyber.gov.au/acsc/report

Physical and personnel security standards and guidance

- ACSC Guidelines for Physical Security: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-physical-security
- Protective Security Policy Framework for the personnel security framework of the Australian Government: https://www.protectivesecurity.gov.au/
- AS 4811 – Employment Screening: https://store.standards.org.au/product/as-4811-2022

Supply chain security standards and information

- Department of Home Affairs Critical Technology Supply Chain Principles
- CISC Protecting your critical infrastructure asset from foreign involvement risk

General risk standards and information

Note: The following documents are referred to in such a way that some or all of their content constitutes guidance or requirements. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- *ISO 31000 – Risk Management – Guidelines* – provides principles, a framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector.
- AS/NZS ISO 31000 – *Risk management – Guidelines* – gives guidance on managing risks faced by organisations which can increase the likelihood of reaching business objectives, improve the ability to identify risks and allocate resources to tackle issues in any stage.
- HB 327 – *Communicating and consulting about risk* – provides guidance to individuals and organisations to understand communication and consultation when managing risk.
- ISO Guide 73 – *Risk Management – Vocabulary* – provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.
- ISO/TR 31004 – *Risk management – guidance for the implementation of ISO 31000* – provides guidance for organisations on managing risk effectively by implementing ISO 31000. It is not specific to any industry or sector, or to any particular type of risk, and can be applied to all activities and to all parts of organisations.
- Australian Disaster Resilience Handbook Collection Handbook 10 – is a collection of resources developed and reviewed by national consultative committees representing a range of state and territory agencies, governments, organisations and individuals involved in disaster resilience. The Collection is sponsored by the Australian Government Attorney-General's Department.
- Third United Nations World Conference on Disaster Risk Reduction (WCDRR) (2015) *Sendai Framework for Disaster Risk Reduction 2015-2030* – applies to the risk of small-scale and large-scale, frequent and infrequent, sudden and slow-onset disasters caused by natural or man-made hazards, as well as related environmental, technological and biological hazards and risks. It aims to guide the multi-hazard management of disaster risk in development at all levels, as well as within and across all sectors.
- Cybersecurity & Infrastructure Security Agency – ICS-CERT Alerts – provides general critical infrastructure from the Cybersecurity and Infrastructure Security Agency.
- Defence Industry Security Program - managed by the Defence Industry Security Office, this program supports Australian businesses to understand and meet their security obligations when engaging in Defence projects, contracts and tenders.