



Australian Government

2023–2030

Australian Cyber Security Strategy: Legislative Reforms

CONSULTATION PAPER

© Commonwealth of Australia 2023

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at <https://creativecommons.org/licenses/by/4.0/legalcode>.



This means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website at <https://creativecommons.org/> as is the full legal code for the CC BY 4.0 license at <https://creativecommons.org/licenses/by/4.0/legalcode>.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of the Prime Minister and Cabinet website—<https://www.pmc.gov.au/honours-and-symbols/commonwealth-coat-arms>.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

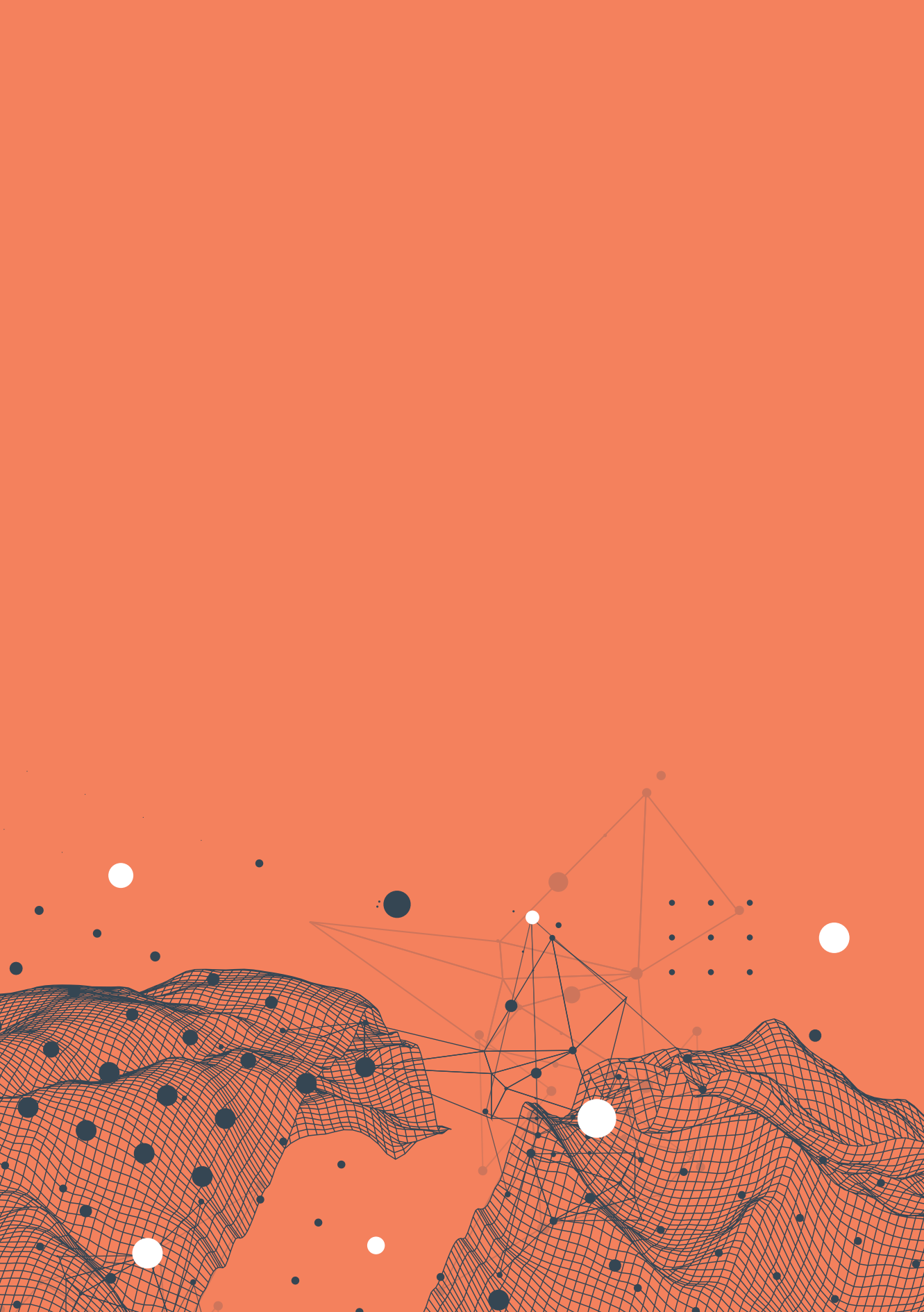
P - 23-02503-c



2023–2030

Australian Cyber Security Strategy:
Legislative Reforms

CONSULTATION PAPER



Contents

Executive Summary	4
Part 1: New cyber security legislation	7
Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices	8
Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses	13
Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator	18
Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board	22
Part 2: Amendments to the <i>Security of Critical Infrastructure Act 2018</i>	30
Measure 5: Protecting critical infrastructure – Data storage systems and business critical data	35
Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers	41
Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions	47
Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers	51
Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act	54
Next steps	56
How to make a written submission	56
Evaluating impacts	56
Face-to-face consultation	56
What we will do with your feedback	57
Privacy collection notice	58
Attachment A: Consultation Paper questions	59
Part 1 – New cyber security legislation	59
Part 2 – Amendments to the SOCI Act	61



Executive Summary

The *2023–2030 Australian Cyber Security Strategy* (the Strategy) and associated *2023–2030 Australian Cyber Security Action Plan* (the Action Plan) outlines the pathway to Australia becoming a world leader in cyber security by 2030. To implement the Strategy and Action Plan, the Australian Government is committed to continuing close consultation with industry and civil society. We need to work together to enable our citizens and businesses to prosper and bounce back quickly after a cyber incident.

This Consultation Paper outlines a number of legislative reforms included in the Action Plan. These legislative reforms aim to strengthen our national cyber defences and build cyber resilience across the Australian economy. We seek your genuine consideration of the proposed reforms, and ask for your feedback on the proposed design and implementation of these measures. Your engagement is critical to ensure that these reforms are fit for purpose and address the needs of Australian citizens and businesses.

Why we need to amend existing cyber security laws

Through the development of the Strategy, the Government has identified a number of opportunities to strengthen and improve our cyber security laws. Reviews of recent cyber incidents have indicated that there are gaps in our current legislative and regulatory framework for cyber security. The opportunities for reform outlined in this paper are intended to provide the right level of protection to Australian citizens and businesses. These measures aim to build basic cyber risk mitigations across the community and help our citizens and businesses engage confidently in the digital economy.

Why we are engaging you in consultation

The Australian Government is committed to shepherding a new era of public-private co-leadership to enhance Australia's cyber security and resilience. We understand that changes to legislation can have significant impacts on how businesses make decisions. By working together to co-design these reforms, we can ensure that any new requirements are easy to comply with, limit unnecessary regulatory burden, and add value for Australian businesses and citizens.

This Consultation Paper includes proposals initially outlined in the *2023–2030 Australian Cyber Security Strategy Discussion Paper* that was released on 27 February 2023. The Cyber Security Strategy Discussion Paper sought initial feedback on potential reforms, including public views on amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act). Public submissions to the Cyber Security Strategy Discussion Paper have helped identify and shape proposals for legislative change. This Consultation Paper is the next step in this consultation process, where we seek your feedback on specific details of proposed reforms.

What is in scope

This Consultation Paper outlines two areas of proposed legislative reform – new legislated initiatives to address gaps in existing regulatory frameworks, and amendments to the SOCI Act to strengthen protection of Australia’s critical infrastructure. These reforms will strengthen our cyber shields and provide better protection to Australian citizens and businesses. The table below shows a summary of the proposed reforms where we are seeking your input.

New cyber security legislation	SOCI Act
<ul style="list-style-type: none">• Secure-by-design standards for Internet of Things devices• Ransomware reporting• Limited use obligation for information provided to the Australian Signals Directorate (ASD) and the National Cyber Security Coordinator (Cyber Coordinator)• Establishing a Cyber Incident Review Board	<ul style="list-style-type: none">• Data storage systems and business critical data• Consequence management powers• Simplifying protected information provisions• Review and remedy powers• Consolidation of telecommunications security requirements under the SOCI Act

What is out of scope

In addition to proposed legislative reforms in this paper, the Government will work with industry and civil society to co-design other initiatives in the Strategy and Action Plan. These initiatives are out of scope of this Consultation Paper, but will be consulted through separate processes. Consultation on these initiatives will be closely coordinated with consultation on the proposed reforms in this Consultation Paper. This consultation process will also be coordinated with other adjacent programs of work across Government, including the Privacy Act Review.

Interim approach for limited use obligation

In addition to legislating a limited use obligation for cyber incident information provided to ASD and the Cyber Coordinator, the Government is also exploring options to develop an interim non-legislative mechanism for ASD. Further information about the limited use obligation is provided in Part 1 of this Consultation Paper.

Non-legislative cyber initiatives and partnerships

We will also be working with industry to co-design other cyber initiatives and partnerships that do not require legislative reform at this stage. These include, but are not limited to:

- Cyber health check scheme for small businesses
- App store code of practice
- Voluntary labelling scheme for IoT devices
- Incident response code of practice
- Providing clear cyber guidance for businesses
- Diversity in the cyber workforce
- Options to encourage uptake of threat sharing and blocking
- Industry data classification models

Consultation for these measures and other initiatives in the Action Plan will commence in early 2024, and are out of scope of this Consultation Paper.

Other adjacent programs of work

There are several adjacent programs of work across Government that support the delivery of the Strategy. These include the Attorney-General's National Plan to Combat Cybercrime, the Privacy Act Review, the Australian Signals Directorate REDSPICE program, the Digital ID program, and the Digital and Tech Skills Compact. These programs of work will be appropriately coordinated with the legislative reform proposed in this Consultation Paper to ensure that Government builds a consistent framework of cyber legislation and regulation.

How you can share your feedback

As detailed in the Next Steps section, we are seeking your views on the proposals in this Consultation Paper to ensure that proposed new legislation is fit for purpose. A number of questions have been proposed throughout this Paper, but your input is welcomed on the measures more generally. Feedback may be provided either through written submissions or during face-to-face engagements and will be used to inform the policy development process and advice to Government. Written submissions are requested on or before Friday, 1 March 2024 using the [Submissions Form](#), and any questions relating to the submission process can be directed to: AusCyberStrategy@homeaffairs.gov.au.

Part 1: New cyber security legislation

As part of the Cyber Security Strategy Discussion Paper, the Australian Government considered the viability of a Cyber Security Act that harmonises a broad spectrum of domestic cyber security legislation into a unified instrument. Feedback on the process identified other opportunities to improve cyber security regulatory processes¹.

Part 1 of this Consultation Paper seeks your views on legislative options to address gaps in current regulatory frameworks, as identified in the Strategy and Action Plan. These measures are:

- Mandating a security standard for consumer-grade Internet of Things (IoT) technology to incorporate basic security features by design and help prevent cyber attacks on Australian consumers;
- Creating a no-fault, no-liability ransomware reporting obligation to improve our collective understanding of ransomware incidents across Australia;
- Creating a 'limited use' obligation to clarify how the ASD and the Cyber Coordinator use information voluntarily disclosed during a cyber incident, in order to encourage industry to continue to collaborate with the Government on incident response and consequence management; and
- Establishing Cyber Incident Review Board to conduct no-fault incident reviews and share lessons learned to improve our national cyber resilience.

1. These include establishing clearer expectations of corporate governance and adopting a phased reporting approach to simplify incident reporting for entities affected by a cyber incident. These are being explored as other initiatives of the Strategy, and will be consulted separately.

Measure 1

Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

The issue

IoT devices – also called ‘smart devices’ – are increasingly used by individuals and businesses in Australia for everyday transactions, communication, work, and leisure. Devices like smart TVs, smart watches, home assistants and baby monitors are widely used across Australia. Industry research estimates forecast an average of 33.8 connected devices per household in Australia by 2025.² The Australian Government supports consumers embracing the benefits of technology while ensuring the technology they use offers adequate protection against cyber threats.

Evidence provided to Government, including through industry reports of cyber incidents, indicates that consumer-grade devices continue to be used by cyber threat actors to target consumers. For example, given the prevalence of universal default passwords, cyber threat actors are able to deploy relatively simple cyber attacks to access sensitive personal information held by Australians on their smart devices.

To date, the Government has taken a voluntary approach to IoT device security. In 2020, the Government introduced a voluntary *Code of Practice: Securing the Internet of Things for Consumers* (the Code of Practice) setting out guidance for IoT manufacturers aligned to the international ETSI EN 303 645 standard. However, evidence provided to Government suggests that this guidance continues to have low levels of adoption across industry.

The international market is moving towards regulated standards to accelerate the adoption of secure-by-design principles and standards in IoT devices available to consumers. The United Kingdom has introduced a legislated mandatory standard for consumer-grade smart devices through its *Product Safety and Telecommunications Infrastructure Act 2022* (UK) (PSTI Act). The European Union has introduced its Cyber Resilience Act which similarly sets mandatory standards for IoT devices. The US and Singapore have adopted a voluntary labelling scheme, although the US scheme is mandatory for the purposes of government procurement.

As a relatively small technology market, it is critical that Australia remains in step with the international market to minimise regulatory burden for vendors, ensuring consumers in Australia have access to the same protections as their international counterparts and do not become easy targets.

What we have heard so far

An evaluation of the domestic Code of Practice in March 2021 suggested that voluntary, principles-based guidance had a limited impact on business decision-making, with evidence suggesting that low-cost manufacturers were least likely to make more security-conscious design choices. Although major IoT manufacturers generally demonstrated a strong commitment to cyber security, the evaluation found that many high-priority and low-cost parts of the Code of Practice had not been implemented consistently.

2. Telsyte Australian IoT@Home Market Study 2021.

During further consultation in 2021, the Government heard feedback from consumer advocate groups and manufacturers suggesting a possible market failure in the IoT market. Feedback strongly suggested that it is reasonable to expect IoT device manufacturers to incorporate basic security features into their products given their capability and understanding of the manufacturing process. However, the Government also heard that manufacturers are not sufficiently incentivised to build secure-by-design products. Manufacturers who prioritise cost and time to market over cyber security can attract higher demand as consumers are typically price-sensitive and generally lack the expertise to distinguish products based on security features.

The Government has heard that any regulation on IoT devices should only be used as a last resort and must demonstrate a net benefit to society. However, the majority of stakeholders across the nation were supportive of introducing a mandatory standard for IoT devices in Australia. There was strong support for Australia adopting international standards because we are a small technology market. Industry stakeholders told us that aligning with international standards would help reduce regulatory burden and lower barriers to entry in the Australian market. There were also views that regulation would need to be future-proofed to adapt to changes in the threat environment and would need to be accompanied by strong enforcement to ensure compliance by industry.

The Cyber Security Strategy Discussion Paper sought industry and community views on the adoption of a mandatory product standard for consumer-grade IoT devices in Australia. Submissions supported a long-term vision for the Australian cyber security landscape where digital goods and services sold are secure-by-design. Many submissions noted that small businesses and vulnerable communities would be the primary beneficiaries of regulation requiring stronger security standards. By allocating more cyber security risk to manufacturers and other entities better placed to mitigate those risks, we can create a safer digital economy.

What we have committed to in the Action Plan

Under Initiative 8 of the Strategy, we committed to:

Adopt international security standards for consumer-grade smart devices by working with industry to co-design a mandatory cyber security standard.

Voluntary labelling scheme for consumer-grade IoT devices

Under the Strategy and Action Plan, Government has also committed to developing a voluntary, industry-led labelling scheme for consumer-grade smart devices. While not in scope of the issues being considered by this Consultation Paper, a labelling scheme will need to be interoperable with the proposed standard. The Government will separately consult and co-design the labelling scheme with industry. Further information about co-design processes for voluntary labelling will be made available on the Home Affairs website.

We seek your views on designing a secure-by-design standard for consumer-grade IoT devices

In response to stakeholder feedback, Government is considering establishing a mandatory cyber security standard for consumer-grade smart devices. Our objective would be to align with international standards, ensure consistency between jurisdictions and minimise regulatory burden on Australian businesses, while also meeting our national security objectives.

Responsible entities

Many entities contribute to the supply chain that provides Australian consumers with access to IoT devices. This includes manufacturers, subcontractors, software developers, importers and distributors. The Department seeks your views on which entities should be covered within the scope of a mandatory security standard. One option could be to use the approach taken for consumer product safety, which requires vendors, suppliers, importers and manufacturers to comply with the standard. This would align with the approach taken in the UK's PSTI Act.

If this approach is adopted, the Department estimates that a one-off implementation cost will be required for retailers in Australia to comply with the standard. Regulated entities would incur costs associated with familiarisation of new requirements, communicating these requirements to suppliers and monitoring stock for compliance. Over time, these costs will decrease as industry adapts manufacturing processes that align with these standards by default. The Government will engage online marketplaces to promote alignment with the mandatory standard, similar to the model for engaging marketplaces for consumer product safety.

Standards to be adopted in Australia

Feedback received from industry and consumer groups in response to the Cyber Security Strategy Discussion Paper supported the Australian Government in adopting the ETSI EN 303 645 standard in the Australian context. Adopting the ETSI EN 303 645 standard would bring Australia in line with our international partners, noting recent developments in smart device standards across other jurisdictions.

The Department seeks your views on whether the first three principles of the ETSI EN 303 645 standard would be an appropriate minimum standard to mandate for cyber security of smart devices in the Australian market. This would be aligned to the requirements in the UK's PSTI Act. Legislating the first three principles of the ETSI EN 303 645 standard would require regulated entities to:

- ensure that smart devices do not have universal default passwords;
- implement a means to receive reports of cyber vulnerabilities in smart devices; and
- provide information on minimum security update periods for software in smart devices.

Globally, the ETSI EN 303 645 standard is a common benchmark for setting either voluntary or mandatory expectations on IoT device security. Several jurisdictions either explicitly require that industry participants meet all or part of the ETSI EN 303 645 standard, or allow industry participants to use the ETSI EN 303 645 standard as an equivalent set of requirements.

These jurisdictions include:

- Brazil;
- Canada;
- China;
- the European Union;
- Finland;
- India;
- Japan;
- Oman;
- United States' State of California;
- United States' State of Oregon;
- Singapore;
- the United Arab Emirates;
- the United Kingdom; and
- Vietnam.

During prior consultation, stakeholders indicated a preference for ETSI EN 303 645 to be adopted as the basis for mandatory cyber security standards for IoT devices sold in Australia. Some stakeholders suggested that other standards relevant to IoT device security could be considered. It may be appropriate to recognise multiple standards, replicating the approach taken in the SOCI Act, which provides regulated entities the flexibility to choose one of several specified standards to adopt. To do so, the Government could draw on international standards mapping, such as the *C2 Consensus on IoT Device Security Baseline Capabilities*.

Smart devices to be regulated

The proposal outlined in this Consultation Paper is to establish a standard that would be broadly applied to all consumer-grade IoT devices in Australia. The UK PSTI Act takes an exception-based approach to defining which IoT devices are regulated—i.e. broadly capturing products capable of connecting with the internet or a network, from which specific devices can be exempted by prescription in delegated legislation (the *Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023* (UK)).

The types of devices within scope of the UK legislation include:

- smart phones;
- connected cameras, TVs and speakers;
- connected children’s toys and baby monitors;
- connected safety-relevant products, such as smoke detectors and door locks;
- wearable connected fitness trackers;
- connected home automation and alarm systems;
- connected appliances, such as washing machines and fridges; and
- smart home assistants.

The only products that have been excluded from UK legislation are charge points for electric vehicles, smart meters, medical devices and computers. A similar exception provision in Australia could accommodate the work already underway across Government to develop specific, tailored security requirements for certain devices such as connected vehicles, medical devices and distributed energy devices.

Smart devices can be special-purpose devices or general-purpose devices. Special-purpose devices are products designed for a specific purpose and are embedded with software and network connectivity to collect and exchange data. This includes products such as smart fridges and other home appliances, connected toys, and connected home automation devices. General-purpose devices can do many tasks and are not designed for a specific purpose, such as smart phones.

The Department seeks your views on the types of devices that should meet a mandatory smart devices standard in the Australian context. We seek your feedback on whether it is appropriate to adopt an approach similar to the definition used in the UK’s legislation regarding which products are included and excluded from the scope of the proposed mandatory standards. Alternatively, it may be appropriate to build our own list of devices that should meet a mandatory standard in the Australian context. This approach could help ensure that the standard remains adaptable and targets particular vulnerabilities emerging in the Australian market, such as digital health devices and solar energy systems.

Introduction timeframes

The Government recognises that manufacturers and vendors will require time to adjust to new security requirements for IoT devices. Several business processes and practices may need to shift to meet new standards. However, consumers will continue to face risks as more products are developed and sold prior to commencement of the standard. The Department seeks your views on an appropriate time period to enable industry to adjust to any new requirements. Based on domestic precedence and international models, a 12 month transition period (as seen in the SOCI Act) may be an appropriate time period after legislation is passed and prior to commencement of any new obligations.

Monitoring and enforcement

Designing an appropriate regulatory model is critical to achieving effective compliance with the proposed standard. A regulatory function will need to be established within the Department of Home Affairs that will oversee the implementation of the standard, and we seek your views on appropriate remediation mechanisms and proportionate penalties for non-compliance.

General Australian Government policy is for the existing framework under the *Regulatory Powers (Standards Provisions) Act 2014* (the Regulatory Powers Act) to be adopted for any new regulatory scheme unless exceptional circumstances apply. This is consistent with the approach taken with respect to the compliance framework under the SOCI Act.

Further information is available on the Attorney-General's Department website about:

- the Regulatory Powers Act: [Regulatory powers | Attorney-General's Department \(ag.gov.au\)](https://www.ag.gov.au/regulatory-powers)
- the framing of offence, compliance and enforcement provisions: [Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers | Attorney-General's Department \(ag.gov.au\)](https://www.ag.gov.au/framing-commonwealth-offences)

Your input

The Department is seeking your views on the design and implementation of a mandatory cyber security standard for IoT and smart devices.

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?
2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?
3. What alternative standards, if any, should the Government consider?
4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?
5. What types of smart devices should not be covered by a mandatory cyber security standard?
6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?
7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for smart devices?

Measure 2

Further understanding cyber incidents – Ransomware reporting for businesses

The issue

Ransomware and cyber extortion incidents pose some of the most significant and destructive cybercrime threats to Australian individuals and organisations. Ransomware uses malicious software to cripple digital infrastructure by encrypting devices, folders and files, rendering essential computer systems inaccessible unless a ransom is paid. Cyber extortion occurs where cybercriminals exfiltrate commercially sensitive or personal data from victims, threatening sale or release if extortion demands are not met.

Limited visibility of the ransomware and cyber extortion threat restricts the capacity of the government and private sector to help Australian organisations prepare for, and respond to, these incidents. Timely reporting of ransomware and cyber extortion incidents would accelerate law enforcement action, enhance whole-of-economy risk mitigation and help tailor victim support services. A better threat picture will ultimately bolster our collective security and strengthen our defences against future cyber attacks. Greater understanding of the threats we are facing will also help us to adapt to the rapidly evolving cyber security landscape.

A clear threat picture requires up-to-date data about cyber incidents as they occur. This includes the number of ransomware and cyber extortion incidents impacting Australian organisations, the type of ransomware used, the vulnerabilities that are being exploited, the overall impact of an incident and whether a ransom or extortion payment was made by the victim.

The Australian Government strongly discourages businesses and individuals from paying ransoms or extortion claims to cyber criminals. If a ransom is paid, there is no assurance that data will be recovered. Your data is likely to be on-sold or released regardless of whether you make a payment. However, the Government recognises that there may be some circumstances where an organisation is compelled to make a payment. In these circumstances, we need to understand the reasons why a payment is made, the amount of the payment and any information regarding the cybercriminal or organisation to whom the payment was made. This information will help law enforcement agencies move faster to stop cyber criminals and break the business model of ransomware.

What we have heard so far

Like many cybercrimes and cyber security incidents, ransomware and cyber extortion attacks are underreported, with research conducted by the Australian Institute of Criminology (AIC) indicating that only one in five respondents who suffered a ransomware incident reported the attack to the police or ASD's Australian Cyber Security Centre.

During consultation on the Strategy, many stakeholders suggested that government should take more substantial action to deter criminal groups from targeting Australian entities. This includes acting through international partnerships, preventing the use of necessary infrastructure by criminal groups, and raising awareness among the public regarding the risks of ransomware and cyber extortion.

Stakeholders also noted the need to increase reporting of ransomware and cyber extortion incidents to ASD. During consultation in 2022, 88 per cent of responses (out of 197 total responses) agreed that Government could develop a mandatory ransomware and cyber extortion notification requirement if anonymised information was also provided to industry to support threat mitigation measures across the broader economy.

However, stakeholders have also acknowledged the regulatory burden and complexity of existing cyber reporting obligations across the economy.³ Minimising additional regulatory burden and maximising the benefits of increased visibility of the threat environment will be key design considerations as part of this consultation process.

What we have committed to in the Action Plan

Under Initiative 4 of the Strategy, we committed to:

Work with industry to co-design options for a mandatory no-fault, no-liability ransomware reporting obligation for businesses to report ransomware incidents and payments.

We seek your views on designing a ransomware reporting obligation for businesses

To maximise the capacity of government and industry to prepare for, and respond to, a ransomware or cyber extortion incident, the Department seeks your views on establishing new ransomware reporting obligations that will be used to develop our national threat picture rather than making findings of fault or liability.

Scope of reporting obligations

The Government is proposing to establish two reporting obligations. It is proposed that an entity would report to Government:

- if an entity is impacted by a ransomware or cyber extortion attack and receives a demand to make a payment to decrypt its data or prevent its data from being sold or released; or
- if an entity makes a ransomware or extortion payment.

This means that if a business pays a ransom, then they would need to make two reports (once on being impacted and again if a payment is made).

3. Through the Strategy, the Government has committed to take further action to address the complexity of current regulatory reporting requirements. Further information on how the Government proposes to simplify cyber regulatory reporting is included in the Action Plan. We will separately consult with industry stakeholders on options to streamline reporting processes.

Information regarding a ransomware attack or cyber extortion demand is vital for Government to enhance our national threat picture. Some of the information that may be required to be reported could include:

- when the incident occurred, and when the entity became aware of the incident;
- what variant of ransomware was used (if relevant);
- what vulnerabilities in the entity's system were exploited by the attack (if known);
- what assets and data were affected by the incident;
- what quantum of payment has been demanded by the ransomware actor or cybercriminal, and what method of payment has been demanded;
- the nature and timing of any communications between the entity and the ransomware actor or cybercriminal;
- the impact of the incident, including impacts on the entity's infrastructure and customers; and
- any other relevant information about the incident or actor that could assist law enforcement and intelligence agencies with mitigating the impact of the incident and preventing future incidents.

The Department seeks your views on what information should be reported to Government as part of this ransomware reporting obligation.

Which entities are required to report

It is important to strike an appropriate balance between maximising our visibility of the ransomware threat and minimising the regulatory burden imposed by a new reporting obligation. To balance these considerations, the Department seeks your views on which entities should be required to make ransomware reports to Government.

Many entities may not be in a position to absorb the additional regulatory burden imposed by a new reporting obligation. For example, small businesses may find it challenging to acquit a reporting obligation due to limited capacity and resources.

To reduce regulatory burden, it may be appropriate to acquit the proposed ransomware reporting obligation through existing reporting obligations. In some cases, an entity may be subject to other incident reporting obligations that could collect the relevant information about a ransomware or cyber extortion incident. For example, approximately 1,000 Australian entities fall under the mandatory cyber incident reporting obligations under the SOCI Act, which require critical infrastructure owners and operators to report cyber incidents, including ransomware or cyber extortion incidents, within 72 hours.

It may also be appropriate to limit the scope of the ransomware reporting obligation to specific types of entities. For example, the obligation could be restricted only to businesses with an annual turnover of more than \$10 million per year. This threshold, which is consistent with the small business threshold used by the Australian Tax Office, would capture approximately 42,000 businesses or 1.7% of all Australian businesses and would exempt small businesses from this new reporting obligation. While this would significantly restrict the sample size for ransomware information, this would still result in an increase in the number of entities subject to a cyber incident reporting obligation.

Timeframes for reporting

Timely reports of ransomware and cyber extortion attacks would enable the Department to generate time-sensitive threat assessments and provide targeted advice to impacted industries.

Through consultation on the Strategy, the Government heard that industry has a preference for consistent reporting timeframes to simplify reporting processes following a cyber incident. Timeframes for reporting a ransomware or cyber extortion attack could align with the reporting timeframes already prescribed in other reporting obligations. For example, mandatory incident reporting obligations under the SOCI Act require a report to be made within 72 hours of an incident occurring. Reporting obligations for payment of a ransom or a cyber extortion payment could adopt a similar timeframe.

'No-fault' and 'no-liability' protection principles

The Government recognises the importance of not further victimising entities that are subject to a ransomware or cyber extortion attack. It may be appropriate to consider a 'no-fault' principle to help entities report ransomware incidents. The 'no-fault' principle aims to provide assurance to entities that the agency receiving ransomware reports under this obligation will not seek to apportion blame for the incident.

It may also be appropriate to consider a 'no-liability' principle in relation to any reports of ransomware payments to provide confidence for entities that they will not be prosecuted for making a payment. While the Australian Government continues to strongly discourage businesses and individuals from paying ransoms to cybercriminals, there is currently no ban on ransomware payments.

However, entities must still continue to meet their legislative and regulatory obligations before, during and after a cyber incident. This means that making a ransomware report would not preclude entities from upholding their existing regulatory obligations, and would not exempt businesses from being held accountable for their cyber security.

Penalties for non-compliance

While the proposed ransomware reporting obligation is not intended to enforce penalties on victims of cyber incidents, a proportionate compliance framework for the mandatory reporting scheme, such as a civil penalty provision, will also be required should a business not comply with its ransomware reporting obligations. This would not violate the intention of the no-fault, no-liability principles, as discussed above.

Criminal penalties are out-of-scope and will not be considered for entities failing to meet a ransomware reporting obligation.

Sharing ransomware reporting information

Industry stakeholders have acknowledged the importance of sharing information regarding ransomware and cyber extortion incidents to support national preparedness and victim support functions. As flagged above, industry has supported the creation of a ransomware reporting obligation if anonymised information was also shared with businesses to help them strengthen their own cyber defences and prepare for cyber attacks.

The Department seeks your views on sharing information on ransomware incidents through a publicly released quarterly report, as well as in targeted formats to benefit particular industry participants or sectors of the economy. The Department acknowledges that some information shared under the reporting obligation may be sensitive and will need to be anonymised or aggregated. Information shared could include anonymised summaries of the types of incident, levels of impact and quantum of ransom payments (if any).

Your input

The Department is seeking your views on options for a mandatory ransomware reporting obligation:

8. What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?
9. What additional mandatory information should be reported if a payment is made?
10. Which entities should be subject to the mandatory ransomware reporting obligation?
11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than \$10 million per year?
12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?
13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?
14. How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?
15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?
16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format?

Measure 3

Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

The issue

Under the *Intelligence Services Act 2001* (ISA), ASD has a statutory function to provide cyber security advice and assistance to government, industry and the community. ASD is not a government regulatory body. Critical to the performance of this function is ASD's ability to:

- develop and maintain a comprehensive national cyber threat picture;
- provide advice on the uplift of cyber security; and
- provide incident management support services to entities affected by a cyber incident.

The Cyber Coordinator has been appointed to oversee a coordinated approach to prepare for and manage the consequences of cyber incidents. The Cyber Coordinator leads the coordination and triaging of government action in response to a major cyber incident. This includes collaboration with the private sector and state, territory and local governments through the National Coordination Mechanism.

Timely incident reporting is vital for ASD and the Cyber Coordinator to perform their functions and help manage the consequences of a cyber attack. Up-to-date information about cyber incidents is essential for ASD and the Cyber Coordinator to build our national cyber threat picture, uplift cyber resilience across the economy and minimise harm following an incident.

The Government has observed that industry are increasingly reluctant to share detailed and timely cyber incident information. ASD has observed that cyber security reporting by industry and critical infrastructure operators has remained steady despite an increase in cyber incidents across the economy. In addition, ASD has experienced delays in entities providing technical information relevant to ongoing cyber security incidents. Some entities refer ASD to their legal representatives rather than incident response leads for ongoing communication. This is reducing the Government's visibility of cyber threats and limiting our ability to offer support to citizens and businesses during an incident. Reduced transparency can have a detrimental impact on incident response, as information shared at early stages of a cyber incident can be critical in supporting a rapid response and informing our national threat picture.

What we have heard so far

Consultation with industry stakeholders has indicated that reduced engagement with government agencies could be partly driven by a shift to a more compliance-based approach to incident reporting. Businesses are concerned that information shared with ASD or the Cyber Coordinator about cyber incidents could be used for regulatory purposes.

The Cyber Security Strategy Discussion Paper sought industry and community views on whether 'an explicit obligation of confidentiality' would improve engagement between government agencies and victims of cyber incidents.

Overall, there was positive feedback about introducing an explicit obligation of confidentiality on ASD and the Cyber Coordinator to promote the sharing of threat information during a cyber incident. This would address calls from industry to clarify how information shared with ASD and the Cyber Coordinator might be used by regulators.

A number of stakeholders pointed to the US *Cyber Security Information Sharing Act 2015* (CISA Act) as a model to consider. The CISA Act provides a regime for the sharing of industry threat information with relevant federal agencies and also clarifies that information provided:

- does not satisfy any mandatory reporting requirement; and
- cannot be used to bring an enforcement action, while regulators continue to have access to their existing set of information gathering powers.

What we have committed to in the Action Plan

Under Initiative 6 of the Strategy, we committed to:

Consult industry on options to establish a legislated limited use obligation for ASD and the National Cyber Security Coordinator to encourage industry engagement with Government following a cyber incident by providing clarity and assurance of how information reported to ASD and the National Cyber Security Coordinator is used.

Interim measures

The Government is exploring a non-legislative limited use obligation for ASD ahead of the proposed legislative reform. This interim measure is being consulted separately with industry on an accelerated timeframe to enable any interim measure to be implemented ahead of a legislated mechanism. The interim measure for ASD is out of scope of this Consultation Paper which is focused on the legislated limited use obligation for ASD and the National Cyber Security Coordinator.

'Safe harbour' vs. 'limited use'

There have been calls for the Australian Government to introduce a 'safe harbour' for entities who provide cyber incident information to ASD and the Cyber Coordinator. A safe harbour would provide entities with a shield against any legal liability incurred as a result of a cyber security incident. However, the Australian public rightly expects that entities should comply with their legal obligations and do what they can to proactively respond to cyber security incidents. When entities experience a cyber security incident, they may be subject to a range of other regulatory frameworks, which play an important role in protecting citizens, supporting the protection of personal information, and promoting the health of the digital economy. This proposal will not exempt an organisation from regulatory obligations, nor reduce an organisation's legal liability on the basis of voluntary reporting to ASD or the Cyber Coordinator, as this would be out of step with public expectations and is not currently being considered.

By contrast, a 'limited use' obligation would restrict how cyber incident information shared with ASD and the Cyber Coordinator can be used by other Australian Government entities, including regulators. This obligation would only allow cyber incident information to be used for prescribed cyber security purposes, including helping businesses respond to cyber incidents. This means that incident information reported to ASD and the Cyber Coordinator could not be used for regulatory purposes. However, such a limited use obligation would not impact other regulatory or law enforcement actions, or provide an immunity from legal liability.

The proposed limited use obligation aims to strike the right balance between encouraging early and open engagement with ASD and the Cyber Coordinator, and protecting broader public interests by ensuring the obligation does not impede an efficient and effective regulatory environment.

We seek your help to design a limited use obligation for ASD and the Cyber Coordinator

We seek your views on a legislative solution that encourages industry to voluntarily provide information to ASD and the Cyber Coordinator about a cyber incident, whilst enabling appropriate information sharing for cyber security purposes.

Limiting the use of cyber incident information

Under the limited use obligation, information shared with ASD or the Cyber Coordinator would be limited to prescribed cyber security purposes defined in appropriate legislation. This means that regulatory agencies could not use this information for compliance action against entities.

The Department seeks your feedback on what functions should be included in the definition of 'prescribed cyber security purposes' for the sharing and use of incident information. These purposes could include:

- to assist the entity with preventing, responding to and mitigating the cyber security incident;
- to facilitate consequence management after a cyber incident;
- to identify further potential cyber security vulnerabilities and take steps to prevent further incidents;
- to analyse and report trends across the cyber threat landscape, including the provision of anonymised cyber threat intelligence to government, industry and international cyber partners;
- to inform relevant Ministers and government officials of the fact of a significant cyber security incident;
- to share incident information with other agencies for law enforcement, intelligence and national security purposes, such as taking action to identify, disrupt or deter cyber threat actors;
- to provide stewardship and advice to industry, including provision of advice to industry on cyber maturity and best practice risk mitigation across sectors; and
- to improve existing incident response mechanisms, such as incident reporting processes and coordination between government and industry.

Government proposes that regulatory agencies would continue to have a critical role during and after a cyber incident due to their expertise in overseeing specific market sectors and mitigating any risk to the broader industry or economy. Under the definition above, regulators could use incident information for industry stewardship to help manage cyber risks across sectors and to mitigate harms to individuals arising from cyber security incidents. However, they would not be able to use the information as part of an investigation or compliance activity.

A regulator would still be able to contact organisations directly (which doesn't require specific legal powers) and would also continue to be able to use their regulatory powers to compel information from an entity if needed, and entities will need to continue to meet reporting obligations.

Sharing cyber incident information

It is important that any limited use obligation does not preclude ASD and the Cyber Coordinator from sharing appropriate information with other agencies – including law enforcement, national security, intelligence agencies and regulators. The proposed model of a 'limited use' obligation would restrict the *use* of cyber incident information, but not the *sharing* of this information.

The Department seeks your views on whether any restrictions should apply to the sharing of incident information with other Australian Government entities.

Incentives to engage with Government after a cyber incident

The Department also seeks your input on other incentives or assurances that could be provided to industry to help encourage engagement with the Government before, during and after a cyber incident.

Your input

The Department is seeking your views on options for a limited use obligation for ASD and the Coordinator:

17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?
18. What restrictions, if any, should apply to the sharing of cyber incident information?
19. What else can government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

Measure 4

Learning lessons after cyber incidents – A Cyber Incident Review Board

The issue

Recent high-profile cyber security incidents have highlighted that government, industry and the community must do more to learn lessons from cyber attacks. To stay ahead of the growing cyber threats across today's complex technology landscape, we need to invest time and resources to understand the vulnerabilities that led to the attack. We also need to examine the effectiveness of government and industry responses to cyber incidents. Once we've identified lessons learned from cyber attacks, we need to share them widely across industry and the broader community to ensure we are better prepared to respond in the future.

As it stands, there is currently no national mechanism to review the root causes of cyber incidents and assess the effectiveness of post-incident response. There is no unified national approach to share lessons learned from cyber incidents. We need a mechanism that can disseminate clear, attributable and concrete recommendations to strengthen our collective cyber resilience. This mechanism needs to have a clear focus on developing and publicly issuing recommendations, as modelled in other sectors across the economy.

What we have heard so far

The Cyber Security Strategy Discussion Paper sought industry and community views on Government developing a post-incident review capability.

There was strong support for the Government to establish a review mechanism to share high-level lessons learned from major cyber incidents.⁴ Many responses highlighted the United States' Cyber Safety Review Board (CSRB) as a potential model.⁵ Several responses noted that a CSRB model would provide an opportunity to demonstrate the benefits of reporting cyber incidents to Government.⁶

Other industries – such as the aviation and transport sectors – have existing models that could provide a starting point for a post-incident review mechanism. The Australian Transport Safety Bureau (ATSB) is responsible for investigating transport-related accidents and incidents, through an independent 'no blame' review process.⁷ Industry stakeholders have recommended that the ATSB could be used as a model for establishing a similar review mechanism for cyber incidents.

4. ANZ; IoT Alliance Australia; Macquarie University Cyber Security Hub; PwC; Ashurst; BAE Systems Digital Intelligence; AUCloud; Macquarie Telecom Group.

5. [Cyber Safety Review Board \(CSRB\) | CISA](#).

6. Queensland University of Technology.

7. [About the ATSB | ATSB](#).

Feedback also highlighted a range of design choices for the post-incident review mechanism, including the question of who leads and contributes to the review process. Stakeholders emphasised the importance of involving academic perspectives, the perspectives of groups particularly at risk from cyber attacks and involving industry partners in regular post-incident review sessions.

A number of submissions also suggested that the Australian Government work closely with stakeholders from both industry and civil society to co design approaches to post-incident reviews.

What we have committed to in the Action Plan

Under Initiative 5 of the Strategy, we committed to:

*Co-design with industry options to **establish a Cyber Incident Review Board** to conduct no-fault incident reviews to improve our cyber security. Lessons learned from these reviews will be shared with the public to strengthen our national cyber resilience and help prevent similar incidents from occurring.*

We seek your help to design a Cyber Incident Review Board

The Department is seeking input from industry on the design and implementation of a Cyber Incident Review Board (CIRB). It is proposed that the CIRB would conduct no-fault incident reviews to reflect on lessons learned from cyber incidents, and share these lessons learned with the Australian public.

Functions of the CIRB

It is proposed that the CIRB has the following functions:

- To conduct no-fault, post-incident reviews of cyber incidents, by understanding:
 - the factual technical details of the cyber incident;
 - the root cause of the cyber incident, including the nature of the vulnerabilities that led to the incident and the methodologies used by cyber threat actors to exploit these vulnerabilities;
 - the actions taken by both industry and government before, during and after an incident;
 - the effectiveness of coordination and consequence management between industry and government; and
 - the impacts of the incident on the affected entity, the sector and the broader community.
- To publicly share findings and best practice learnings to enhance collective cyber security and help prevent similar incidents from occurring in the future, including by:
 - making public reports that outline lessons learned from cyber incidents;
 - making appropriate recommendations to government and industry to reduce the risk of future cyber incidents and improve post-incident response; and
 - engaging stakeholders from industry and civil society to ensure that these findings and lessons learned are widely understood and incorporated into our national cyber defences.

The CIRB would not be a law enforcement, intelligence or regulatory body. This means that the CIRB would:

- Ensure that any public report or recommendations released by the CIRB do not prejudice or interfere with ongoing activities of law enforcement, national security and intelligence agencies, regulators and judicial bodies;
- Be distinct from regulators and have no regulatory function itself, while appropriately engaging with regulators to uplift our collective cyber security; and
- Uphold public interest criteria to manage sensitive information considered in the scope of a post-incident review. This could include not publicly revealing vulnerabilities, personal information or non-personal information that may expose individuals and businesses to harm.

'No-fault' principle

A no-fault principle is critical to maximise stakeholder engagement with the CIRB, particularly if findings are made public. A no-fault principle would mean that the CIRB does not make findings of fault or apportion blame as a result of its reviews. Further, the outputs and recommendations of a CIRB review should not be used to make findings of fault or apportion blame.

Industry feedback has suggested that the 'no-blame' approach of the ATSB could be used as a model for the CIRB. Under the *Transport Safety Investigations Act 2003*, the ATSB does not make findings of fault or blame when investigating transport-related incidents:

*'ATSB investigations do not apportion blame or provide a means for determining liability, and we do not investigate for the purposes of taking administrative, regulatory or criminal action. Our investigations are aimed at determining the factors which led to an accident or safety incident so that lessons can be learned and transport safety improved in the future. Our ability to conduct an investigation would be compromised if we sought to lay blame, as the future free-flow of safety information could not be guaranteed. As such disciplinary action and criminal or liability assessment are not part of an ATSB safety investigation and would, if necessary, be progressed through separate parallel processes by regulatory authorities or the police. The no-blame approach also supports cooperation with the investigation process, and the reporting of safety occurrences.'*⁸

Similarly, the Inspector of Transport Security conducts inquiries into major transport or offshore security incidents. Under the *Inspector of Transport Security Act 2006*, the role of the Inspector is to improve the security of aviation or maritime transport security systems through independent inquiry without apportioning blame. The *Inspector of Transport Security Act 2006* does not provide the means to determine liability in relation to a security incident or allow adverse inferences to be drawn when a person is the subject of an inquiry into a matter.⁹

The Department seeks your input on how Government should develop a similar 'no-fault' principle for the CIRB. Similar to the approach for the ATSB, this could include requiring that the CIRB does not:

- Apportion blame or fault for cyber incidents;
- Provide the means to determine the liability of any entity in respect of a cyber incident;
- Assist in court proceedings between parties relating to a cyber incident; or
- Allow any adverse inference to be drawn from the fact that an entity was involved in a cyber incident.

8. Commonwealth of Australia, *About the ATSB*, Australian Transport Safety Bureau, Canberra, 2023

9. Section 9(3) *Inspector of Transport Security Act 2006*

Initiating a CIRB review

Setting the right threshold for initiating a CIRB review will help ensure that any CIRB review is well-targeted, effective and a prudent use of resources. As such, the CIRB is likely to focus on reviewing significant cyber incidents rather than all cyber incidents. Existing frameworks may be sufficient to establish this threshold, or a unique definition may be required for the CIRB.

The Department seeks your views on the factors to take into account in determining whether an incident is significant for the purposes of meeting the threshold for a CIRB review. Relevant factors could include:

- the technical severity and complexity of the incident;
- the likelihood and severity of the consequences of the incident, including the impacts on our national security, economy and the broader public;
- public interest in the incident;
- the cost of conducting a review;
- the availability of relevant information and intelligence relating to the incident; and
- the potential to capture lessons learned from the incident that will demonstrably improve our national cyber resilience and preparedness for future cyber incidents.

The consequences of a cyber incident would be an important factor to consider when deciding whether to initiate a CIRB review. While a cyber incident might not be technically complex, a CIRB review should be triggered if the consequences of the incident are likely to be significant. For example, the threshold for an issue to be considered by the US Cyber Safety Review Board is whether an incident (or group of related incidents) is likely to result in demonstrable harm to national security interests, foreign relations, the economy, public confidence, civil liberties, public health and safety. The CIRB could adopt a similar definition as its threshold for commencing a review.

CIRB membership

The composition of the CIRB needs to be appropriately designed to ensure that CIRB reviews are impartial and credible. The Department seeks your views on who should be appointed to a CIRB, how they should be appointed and remunerated, and how conflicts of interest should be managed.

There are different models for the composition of a CIRB, including:

- **Standing CIRB members:** The CIRB is established as a multi-stakeholder advisory committee, with standing members drawn from across the public and private sectors. These members are selected to combine the expertise of government, industry, and academia. Government members could be from prescribed offices and agencies. Having standing CIRB members would facilitate consistency in decision-making and enable CIRB members to deepen experience over the course of various CIRB reviews. This option builds on the US model, and aligns with stakeholder feedback on the Cyber Security Strategy Discussion Paper.
- **A pool of CIRB members:** A new CIRB could be stood up for each individual review. Non-government members could be selected from a pool of appropriate individuals, ensuring that the composition balances expertise across industry and academia while also preventing anti-trust behaviour. This option draws from the model used by the Takeovers Panel.
- **A blend of the above two options:** The CIRB could consist of a set of standing members plus a pool of individuals who could be appointed to facilitate a specific review depending on the impacted entity, the nature of the cyber incident and the type of vulnerability being reviewed.

When appointing CIRB members, the following considerations should also be taken into account:

- **Expertise:** What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?
- **Personnel security:** How should the Government manage access to classified information by CIRB members? Should some or all CIRB members be required to hold security clearances?
- **Conflicts of interest:** How would possible conflicts of interest be managed when appointing CIRB members? While industry expertise would be critical in informing the work of a CIRB, industry engagement would need to be balanced with robust management of potential conflicts of interest.

In addition to regular board members, the CIRB would require a Chair. The Department seeks your input on whether the Chair should be a new, independent official appointed by the Australian Government.

Power to initiate a CIRB review

The Department also seeks your views on who should be able to initiate a CIRB review.

Options include CIRB reviews being initiated by:

- the Minister for Cyber Security;
- the National Cyber Security Coordinator;
- the Cyber Incident Review Board; and/or
- agreement between the Minister for Cyber Security and relevant Ministers, depending on the nature of the proposed review.

Investigatory powers

The proposed intent of the CIRB is to issue public recommendations that help uplift cyber security across Australia. As a result, the 'no-fault' principle defined above remains a cornerstone of the CIRB model. However, the CIRB also needs to access relevant information to inform its reviews and to be able to deliver actionable recommendations. Therefore, a CIRB may require proportionate information gathering powers to effectively discharge its purpose and provide accurate and relevant advice to the Australian community.

There are two main options for investigatory powers held by the CIRB. Firstly, the CIRB could have voluntary powers to request information but no powers to compel entities to participate in reviews. Alternatively, the CIRB could have limited information gathering powers to require entities to provide appropriate information to facilitate the review of cyber incidents. The Department seeks your views on whether a CIRB should have voluntary powers or limited information gathering powers to gather information relevant a review.

Voluntary powers to request information

The CIRB could be established with voluntary powers to request information. This would mean that the CIRB has powers to request that entities provide information related to a cyber incident, but cannot compel entities to provide this information. Under this model, an entity could refuse to cooperate with a CIRB review.

Limited information gathering powers to gather information for incident reviews

Alternatively, the CIRB could have limited information gathering powers to acquire information required to facilitate the review of a cyber incident.

This model would align with that adopted by the ATSB. Under the *Transport Safety Investigation Act 2003*, the ATSB has limited powers to require entities to answer questions relating to matters relevant to an investigation or produce specified evidence to the ATSB.¹⁰ Normally, the ATSB seeks to obtain information with the consent of the individual concerned, but these limited powers can be exercised if required.¹¹

Information gathering powers range from modest powers to more intrusive powers. For example, powers to require the production of documents and the ability to access and handle classified information are less intrusive powers. In contrast, more intrusive powers include the power to enter premises, intercept telecommunications or seek search warrants. Intrusive powers are not being considered for the CIRB. To align with the ATSB model, this discussion is restricted to modest information gathering powers.

New powers are generally granted only in exceptional circumstances, where existing powers are inadequate and where a clear policy justification exists. Limited information gathering powers would only be required for the CIRB if there is reasonable grounds to believe that voluntary powers would be insufficient to allow the CIRB to deliver its intended functions and provide accurate advice to the Australian public.

The Department seeks your views on whether a CIRB should have modest information gathering powers and what should be considered in exercising such powers. When developing a detailed proposal for any new information gathering powers, consideration must be given to:

- who can exercise the powers – whether all members of the CIRB or only certain authorised members should be able to exercise these powers;
- the threshold for demanding information – whether the notice to produce information should only be issued where the issuer reasonably believes that the person required to produce has control of the documents, information, or knowledge that will assist the CIRB;
- the issuer of the notice to produce – whether the notice to produce be issued by the CIRB as an entity or by the Chair;
- the interaction of proposed powers with information that is privileged – whether a privilege against self-incrimination should be given precedence over a notice to produce;
- the enforcement of investigatory powers – the type of penalty regime enforced in response to a failure to comply with an information request;
- the oversight of investigatory powers – whether the Commonwealth Ombudsman, who oversees Commonwealth, State and Territory law enforcement and integrity agencies' use of investigatory powers, or another entity should be responsible for oversight of these powers; and
- the discretion to produce – whether the CIRB should initially request information be provided voluntarily before using information gathering powers.

10. Under Section 32 of the *Transport Safety Investigation Act 2003*, the ATSB can require a person to attend before the ATSB and answer questions put by any person relevant to matters relevant to the investigation, and require a person to produce specified evidential material to the ATSB. The ATSB may also require questions to be answered on oath or affirmation.

11. [ATSB Privacy Policy](#) | ATSB

These considerations draw on information on designing powers for agencies in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.¹²

The Secretary's information gathering powers in Part 4, Division 2 of the SOCI Act could be used as a model for an information gathering power option for a CIRB.

If the CIRB had limited information gathering powers, it would be important that a CIRB only relies on those powers as a last resort. The CIRB must maintain productive and collaborative relationships with any entities that are under review. As discussed above, the CIRB is not a regulatory body – therefore, information gathered by the CIRB should only be used for the purposes of sharing lessons learned with the public, and not be used for regulatory or compliance activities. This could mean that the CIRB may need to be covered by a 'limited use' obligation, similar to the obligation proposed for the ASD and the Cyber Coordinator described above. The Department seeks your views on whether the CIRB would require a limited use obligation of this nature.

As per the ATSB model, proportionate enforcement mechanisms may be required to enforce compliance with information gathering powers. The *Transport Safety Investigation Act 2003* includes appropriate penalties if an entity fails to participate in an ATSB investigation or fails to produce requested evidence.¹³ Similar enforcement mechanisms may be required for the CIRB to ensure that entities adhere to information gathering requests and enable effective reviews of cyber incidents. Any enforcement mechanisms would need to be proportionate and align with the 'no-fault' principle described above.

Impartiality

A CIRB would need to have a high level of trust and transparency to support its reviews and ensure that it meets its objective of strengthening our collective cyber resilience. A CIRB would need to operate in a way that builds and maintains trust with entities to maintain its effectiveness.

To ensure that its work is credible with the public, a CIRB would need to be impartial in the way it conducts its activities. This includes making unbiased recommendations that align with the 'no fault' principle described above. The Department seeks your perspective on how the CIRB can be designed to ensure it remains impartial and maintains credibility as it conducts incident reviews.

Protecting sensitive information

Making public recommendations would be an important part of sharing lessons learned from cyber incidents. Given that some findings relating to a cyber incident are likely to be sensitive, the CIRB may need a mechanism to ensure that sensitive information remains appropriately protected. This includes ensuring that findings and recommendations do not prejudice any law enforcement or judicial proceedings. Potential safeguards to protect sensitive information could include granting the CIRB powers to provide confidential reports to Government and producing redacted reports for public consideration.

¹² [Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers](#)

¹³ Under Section 32 of the *Transport Safety Investigation Act 2003*, any person who fails to comply with the limited investigatory powers of the ATSB receives a penalty of 30 penalty units.

Your input

The Department seeks your input on the proposed purpose, scope, composition, and operating model of the CIRB.

20. What should be the purpose and scope of the proposed CIRB?
21. What limitations should be imposed on the CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?
22. How should the CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?
23. What factors would make a cyber incident worth reviewing by a CIRB?
24. Who should be a member of a CIRB? How should these members be appointed?
25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?
26. How should the Government manage issues of personnel security and conflicts of interest?
27. Who should chair a CIRB?
28. Who should be responsible for initiating reviews to be undertaken by a CIRB?
29. What powers should a CIRB be given to effectively perform its functions?
30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?
31. What enforcement mechanism(s) should apply if entities fail to comply with the information gathering powers of the CIRB?
32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?
33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

Part 2:

Amendments to the *Security of Critical Infrastructure Act 2018*

The Australian Government has committed to consulting on options to reform the *Security of Critical Infrastructure Act 2018* (SOCI Act) to address gaps identified following recent major cyber security incidents. Reviews of these incidents indicated that there are opportunities to clarify and strengthen existing cyber security obligations on critical infrastructure sectors captured under the SOCI Act.

This part of this Consultation Paper will seek your views on the following proposed measures:

- clarifying obligations for critical infrastructure entities to protect data storage systems that store 'business critical data', where vulnerabilities in these systems could impact the availability, integrity, reliability or confidentiality of critical infrastructure;
- introducing a last resort consequence management power for the Minister for Home Affairs to authorise directions to a critical infrastructure entity (with safeguards in place and where no other powers are available) in relation to the consequences of incidents that may impact the availability, integrity, reliability or confidentiality of critical infrastructure;
- simplifying information sharing to make it easier for critical infrastructure entities to respond to high-risk, time-sensitive incidents;
- providing a power for the Secretary of Home Affairs or the 'relevant Commonwealth regulator' to direct a critical infrastructure entity to address deficiencies in its risk management program; and
- consolidating security requirements for the telecommunications sector under the SOCI Act.

Why we need to protect critical infrastructure

Australians rely on critical infrastructure to deliver the essential services crucial to our way of life. Our critical infrastructure ecosystem provides essential goods and services that underpin Australia's national security, defence, and socioeconomic stability.

However, we currently face a heightened geopolitical and cyber threat environment, which means that our critical infrastructure is increasingly under threat. Cyber attacks on our critical infrastructure can be highly lucrative for malicious state actors and cybercriminals. ASD's Annual Cyber Threat Report 2022–23 reported that ASD responded to 143 cyber incidents related to critical infrastructure. This represents approximately 13 per cent of their cyber incident reporting for this period.

The Optus and Medibank cyber incidents on 22 September 2022 and 12 October 2022 respectively were both attacks on the systems and networks of critical infrastructure entities that held personal data. These attacks led to millions of customers' data being compromised. Data breaches of this nature are increasing in scale and frequency, and the loss of personal data can cause significant harm to Australian citizens and businesses. The theft of sensitive data can result in large-scale fraud, put strain on the economy, destabilise the financial sector and reduce consumer confidence in our digital goods and services.
























But data held by critical infrastructure entities is not the only thing at risk. Critical infrastructure entities are themselves valuable targets, as they provide essential services to support Australian life and business – including our electricity, water, health, transport, logistics and telecommunication networks. In the Australian Security Intelligence Organisation's 2021–22 Annual Report, the Director General wrote that "malign foreign powers will consider using sabotage to coerce, disrupt or retaliate during times of escalating geopolitical tensions. Pre-positioning malicious code in Australia's critical infrastructure is the most likely means."

While many cyber attacks are focused on exfiltration of data from corporate databases, there is also a risk of lateral transfer to operational technology or network infrastructure. Large-scale attacks on these systems could cause major outages of essential services, resulting in widespread disruption of the Australian economy and our society. In extreme cases, outages of essential systems could lead to loss of life.

Current critical infrastructure regulation

The SOCI Act is the primary framework for regulation and protection of Australia's critical infrastructure. Amendments to expand the scope of the SOCI Act to better capture the complexities and interconnectedness of Australia's critical infrastructure occurred in two tranches in December 2021 and April 2022. These amendments expanded its application from four sectors to 11 sectors and 22 asset classes, as seen in the figure on the next page.

Figure 1: The 11 sectors and their asset classes

Energy	Communication	Financial services	Transport
 Liquid fuel	 Telecommunications	 Superannuation	 Aviation
 Gas	 Domain name systems	 Insurance	 Freight infrastructure
 Energy market operator	 Broadcasting	 Financial markets and infrastructure	 Freight services
 Electricity	Data storage or processing  Data storage or processing	 Banking	 Port
Water and sewage	Higher education and research	Food and grocery	
 Water	 Education	 Food and grocery	 Public transport
Space technology	Defence industry	Health care and medical	
 No asset class	 Defence industry	 Designated hospitals	

The SOCI Act now provides the following key measures for the owners and operators of certain critical infrastructure assets:

- the requirement to report information to the register of critical infrastructure assets, ensuring we have an understanding of our critical infrastructure ecosystem, risks and interdependencies;
- mandatory cyber incident reporting requirements, ensuring that we have a better aggregate understanding of how cyber attacks are impacting our critical infrastructure;
- the requirement to implement and comply with an all-hazards critical infrastructure risk management program (CIRMP), creating a baseline for security across the critical infrastructure ecosystem;
- the requirement for owners and operators of our most interconnected systems of national significance to comply with enhanced cyber security obligations – working in a close partnership with Government to ensure they are sufficiently prepared and positioned to defend and respond in the event of a significant cyber attack on their systems; and
- responsive government assistance measures to help industry respond to significant cyber incidents as a last resort.

The information we collect under the SOCI Act is analysed and shared with industry to help critical infrastructure owners and operators be better prepared for cyber incidents. Information sharing between government and industry, and across industry, has proven to be an effective mechanism to build organisational and sectoral resilience, with minimal regulatory intervention.

An independent review under section 60A of the SOCI Act will commence after the CIRMP obligation is in full effect. This will more holistically address reforms to the SOCI Act that are less time-critical. We also propose to leverage this review as an opportunity to evaluate the effectiveness of the amendments proposed in this Consultation Paper.

Why we need further reform

Following recent cyber incidents, stakeholders across industry and the broader Australian community have expressed a strong desire for the Government to have the right tools to respond quickly to cyber incidents. Recent incidents impacting critical infrastructure highlighted that there are a number of gaps in the SOCI Act that limit our ability to prepare, prevent and respond to cyber incidents. We cannot delay implementing lessons learned from recent incidents.

In 2022–23, the Mandatory Cyber Incident Reporting (MCIR) regime for critical infrastructure assets identified that there were 188 significant or relevant incidents impacting Australia. This means that these incidents impacted the confidentiality, integrity or reliability of Australian critical infrastructure. The response to these incidents revealed a number of gaps in our existing legislative mechanisms and policy frameworks for critical infrastructure that will be addressed in this Consultation Paper.

Several key themes have been identified for legislative reform to the SOCI Act:

- **Clarity:** The security standards of critical infrastructure need to be clarified and enhanced, particularly within the telecommunications sector;
- **Consistency:** The application of the SOCI Act needs to consistently capture the secondary systems where vulnerabilities could have a relevant impact¹⁴ on critical infrastructure; and
- **Coordination:** The SOCI Act needs to enable an agile, industry-led response to incidents with appropriate support from government when necessary.

Proposed reforms outlined in this Consultation Paper will form an important step in the implementation of the Strategy and help Australia become a world leader in cyber security by 2030.

¹⁴ As defined in s8G of the SOCI Act, a 'relevant impact' is an impact to the availability, integrity, reliability, or confidentiality of a critical infrastructure asset.

Measure 5

Protecting critical infrastructure – Data storage systems and business critical data

The issue

Over the last 18 months, Australia has seen a growing number of cyber incidents impacting non-operational data storage systems held by critical infrastructure entities. Critical infrastructure entities are a natural target for cyber attacks given their size, function and value. These incidents, which include the 2022 Optus and Medibank attacks, did not directly impact the essential functions of critical infrastructure, but rather the non-operational systems that hold large quantities of data. This includes both personal information and other 'business critical data'¹⁵.

There are two primary reasons why attacks on data storage systems that hold business critical data can cause significant disruptions to critical infrastructure.

Firstly, critical infrastructure entities often hold valuable non-personal data, such as operational or research data. Operational data can include network blueprints, encryption keys, algorithms, operational system code, and tactics, techniques and procedures. Theft of this data can cause significant damage to the operation of critical infrastructure. For example, malicious actors could use this data to expose other vulnerabilities in infrastructure networks or install malware on operational technology.

Secondly, data storage systems can often be a point of entry for malicious actors to attack other systems related to critical infrastructure. Ransomware actors and cybercriminals often start by attacking corporate data systems, seeking to use these networks as entry points for 'lateral transfer' to higher value targets. Cybercriminals could exploit vulnerabilities in the corporate network of a critical infrastructure entity to gain access to their operational technology and network control systems. Malicious actors continue to develop sophisticated mechanisms to exploit these vulnerabilities in peripheral systems.

This risk of lateral transfer is being realised globally. For example, in the US, the Colonial Pipeline incident began as a ransomware attack on a corporate system. This resulted in the company shutting down its operational systems to mitigate the risk of cross-system compromise, which caused cascading supply chain impacts to the distribution of gasoline and jet fuel to the Eastern United States.

15. Under s5 of the SOCI Act, business critical data means:

- (a) personal information (within the meaning of the Privacy Act 1988) that relates to at least 20,000 individuals; or
- (b) information relating to any research and development in relation to a critical infrastructure asset; or
- (c) information relating to any systems needed to operate a critical infrastructure asset; or
- (d) information needed to operate a critical infrastructure asset; or
- (e) information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

Currently, the SOCI Act does not explicitly require critical infrastructure entities to protect data storage systems that hold business critical data, even if vulnerabilities in these systems could cause significant disruption or damage to critical infrastructure. The current definitions of 'asset' and 'material risk' in the SOCI Act do not explicitly call out these data storage systems. As a result, many entities are not including these systems in their CIRMP or reporting significant data breaches when they affect these systems.

What we have heard so far

During consultation on the Strategy, stakeholders were broadly supportive of expanding critical asset definitions to include secondary systems, such as those that hold large volumes of data. However, regulatory duplication was a key concern raised by industry. Stakeholders cautioned against reforms that would extend the scope of the SOCI Act to capture data storage systems that are already sufficiently regulated by other regulatory frameworks, such as the Australian Prudential Regulatory Authority's Consumer Prudential Standard (CPS) 234. Stakeholders also supported the role of the *Privacy Act 1988* (Privacy Act) as the primary legislative framework regulating personal information.

Other industry feedback highlighted the importance of ensuring that any amendments to the scope of the SOCI Act were targeted and proportionate. The proposal in this Consultation Paper focuses on a targeted amendment that limits the application of the SOCI Act to data storage systems that hold business critical data, and limits regulation to those systems where vulnerabilities would have a relevant impact on critical infrastructure.

What we have committed to in the Action Plan

Under Initiative 13 of the Strategy, we committed to:

Protect the critical data held, used and processed by critical infrastructure in 'business-critical' data storage systems. Government, in consultation with industry, will consider clarifying the application of the SOCI Act to ensure critical infrastructure entities are protecting their data storage systems where vulnerabilities to those systems could impact the availability, integrity, reliability or confidentiality of critical infrastructure.

The Government response to the Privacy Act Review

The Privacy Act regulates Australian Privacy Principle (APP) entities, which can include both critical infrastructure and non-critical infrastructure entities. While various sector specific frameworks may also regulate personal information, the Privacy Act remains the primary lever for the protection of personal information.

Through the implementation of the Government response to the Privacy Act Review, the Government is taking action to strengthen the protection of personal information. The Government has outlined a number of measures to enhance the compliance with, and enforcement of, the Privacy Act. These measures recognise the vast amount of data, including personal information, which is collected by entities and has been involved in recent large-scale data breaches.

Proposed amendments to the SOCI Act

We are aware of the critical role of data in Australia's economy, and recognise the importance of entities having the ability to access, utilise and share data. Better access to data can elevate business performance, and improve the delivery of goods and services to Australians. In particular, we are conscious of the potential impacts of measures to enhance the security of data storage systems on the productivity of 'data-intensive' sectors including telecommunications and finance. Stricter security requirements could affect the ability of these entities to innovate and utilise emergent technologies, including artificial intelligence.

While the SOCI Act currently imposes positive security obligations on data storage and processing assets, this does not adequately protect secondary systems operated by existing critical infrastructure entities outside the data storage and processing sector, where vulnerabilities to those systems could have a relevant impact on critical infrastructure.

Asset definition

Firstly, we propose to include data storage systems holding 'business critical data' in the definition of 'asset' under section 5 of the SOCI Act. This amendment would:

- Ensure that all asset classes must consider data storage systems holding 'business critical data' as part of their broader critical infrastructure asset, where vulnerabilities in these systems could have a 'relevant impact' on critical infrastructure;
- Enable 'business critical' data storage systems to be considered as an asset by other relevant definitions in the SOCI Act, including the definition of an explicit material risk under the CIRMP; and
- Only take effect on critical infrastructure assets captured by existing asset class definitions under the SOCI Act.

Material risk definition

We also propose an amendment to the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules* (CIRMP Rules), to include risks to data storage systems holding 'business critical data' and the systems that access the data as 'material risks' (section 6 of the CIRMP Rules). Under this amendment:

- There would be no change to existing requirements for critical infrastructure entities to consider cyber and information hazards or other hazard domains.
- Protection of data storage systems holding 'business critical data' would need to be considered as part of all-hazard risk mitigation, which may include consideration of physical infrastructure security.
- The CIRMP would remain as a principles-based obligation. This means that the CIRMP can be acquitted by industry as suits them best (for example, using a single document or a suite of documents) while taking other federal, state and territory regulations into consideration, provided attestation and the document/s used to comply with the obligation can be produced on request.

The proposed amendments are intended to complement obligations under other legislation, such as those obligations in the Privacy Act that apply to personal and sensitive information.

Implication for risk management obligations

By covering data storage systems that hold business critical data under the SOCI Act, critical infrastructure entities that are currently captured by the SOCI Act would be required to:

- consider how threat actors could exploit vulnerabilities in these systems;
- implement controls to mitigate or eliminate risk, prior to risks being realised;
- proactively identify and control against risks to their data storage assets as part of their CIRMP obligation;
- provide operational and ownership information regarding these systems to the Cyber and Infrastructure Security Centre (CISC);
- report under their MCIR obligation when a cyber incident impacts these systems; and
- comply with directions under the SOCI Act when an attack on business critical data systems is having a relevant impact on their asset (for example, under Part 3A).

Scope of application

This measure would apply to systems that hold large volumes of personal and non-personal information, where this information has a relevant impact on the operation of the critical infrastructure asset – such as operational and research data. This amendment aims to reduce the likelihood and severity of cyber attacks on these systems, and help mitigate the consequences of these incidents on critical infrastructure.

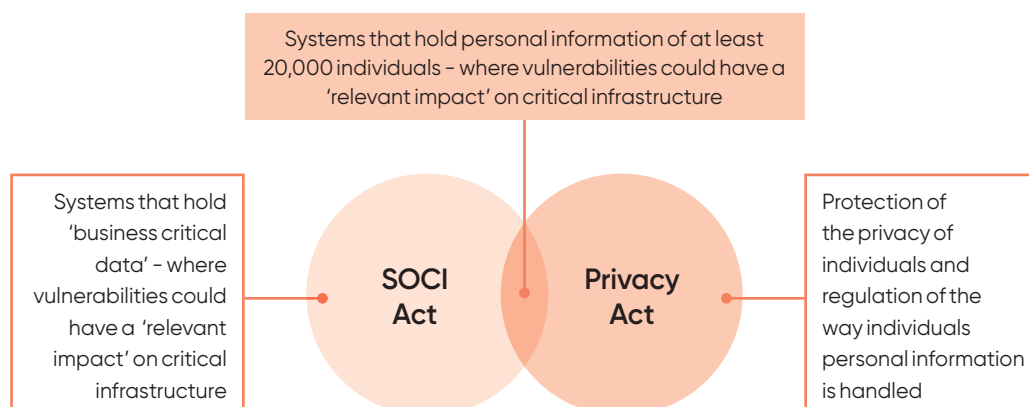
Consistent with our current regulatory approach, the Government remains committed to limiting regulatory duplication. The implementation of these reforms will be done in close consultation with other agencies and regulators to ensure security outcomes are achieved with minimal regulatory burden.

Relationship with the Privacy Act

The Department of Home Affairs will work closely with the Attorney-General's Department to ensure amendments to the SOCI Act are complementary to existing and proposed obligations under the Privacy Act. The relationship between the SOCI Act and the Privacy Act will also be supported by appropriate guidance material. To manage the burden on industry of overlapping consultation processes, the Department of Home Affairs and the Attorney-General's Department will seek to coordinate consultation on reforms to the SOCI Act and the Privacy Act to the extent possible.

The figure on the next page outlines how data protection would be managed across the SOCI Act and the Privacy Act under the proposed reforms. While the scope and purpose of the SOCI Act and Privacy Act vary, both would play a complementary role in regulating systems that hold personal information of at least 20,000 individuals, where vulnerabilities could have a relevant impact on critical infrastructure.

Figure 2: Management of data protection under the proposed reforms



Hypothetical scenarios

Clarification of data protection obligations under the SOCI Act will help avoid inconsistent application of regulations. Consider the following scenarios, where protections for data storage systems are inconsistent and subject to interpretation:

- **Scenario 1:** A major port has operational data stored with a third-party data storage or processing provider (which is regulated under the SOCI Act). Under current legislative obligations, the data storage and processing entity contracted by the major port has obligations under the SOCI Act to protect the system that holds business critical data. If a breach occurred in this system, the data storage and processing entity has an existing obligation to report any data breaches under the MCIR in the SOCI Act.
- **Scenario 2:** A telecommunications asset has customer data stored within a data storage system connected to their network (which forms part of their existing critical infrastructure asset). If the telecommunications asset was subject to an eligible data breach,¹⁶ the telecommunications provider would have an obligation under the Privacy Act to report the breach to affected persons and the Australian Information Commissioner. However, it is unclear whether the telecommunications asset should consider business critical data as part of their existing risk management obligations.
- **Scenario 3:** A water asset has research and development data stored within a data storage system connected to their operational technology (which forms part of their existing critical asset). As per the telecommunications asset, it is unclear whether the water asset should consider business critical data as part of their existing risk management obligations. Under current regulations, the water asset would not be obligated to report a compromise in their research data if the breach did not impact the confidentiality, availability or reliability of their asset.

16. An eligible data breach is where there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by a telecommunications company which is likely to result in serious harm to individual or individuals to whom the information relates.

There is no compelling argument to justify why business critical data is subject to more rigorous protection when its storage is outsourced under Scenario 1. It is a reasonable expectation that all critical infrastructure entities take extra steps to manage the risk and protect the security of their data storage systems, including those that hold large volumes of personal data. This is not only because of the value of this data, but the potential for further compromise of the asset's function and downstream impacts on Australian communities.

The proposed amendments would set a consistent standard

Under the proposed amendments to the SOCI Act, all three entities described in the scenarios above would need to take positive steps to protect data storage systems that hold business critical data where vulnerabilities in these systems could cause a disruption to critical infrastructure. In practice, this may involve the responsible entity taking measures such as:

- generally increasing the cyber maturity of its data storage assets;
- introducing more stringent security controls for credentials belonging to third-party service providers;
- implementing tighter access controls on sensitive research and operational data;
- vetting prospective employees whose roles require access to large amounts of operational data;
- educating staff and third-party service providers about the risks of phishing;
- eliminating risks in the physical environment for key storage assets; and
- having all the above measures signed off on by the company's board.

Your input

With an increased focus on the value of data held by industry and government, including operational and customer data, the Department seeks to understand your current approach to data protection, management, and risk mitigation. You are encouraged to discuss how you currently manage potential risks from third parties and managed service providers that may have access to your business critical data.

34. How are you currently managing risks to your corporate networks and systems holding business critical data?

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

Measure 6

Improving our national response to the consequences of significant incidents – Consequence management powers

The issue

Recent incidents have demonstrated that businesses often face difficulties responding effectively to the aftermath of cyber attacks. Beyond the technical incident, attacks on critical infrastructure can have long-lasting and cascading effects on Australian services, lives and business. This can include harms to our citizens (such as fraud or scams), organisations (such as theft of data and financial loss), and the wider economy (such as disruption of essential services). Consequences of significant incidents can often lead to reputational damage and loss of confidence in a system, market, entity or nation.

Most critical infrastructure entities are willing to act to address the consequences of incidents impacting their assets. However, in some cases, they may have legal or other restrictions preventing them from doing so. Reviews of the response and consequence management framework in the wake of the 2022 Optus and Medibank incidents showed that there were no clear powers available to support a fast and effective response without legal risk. For example, entities were unable to share data about affected customers with banks to prevent financial fraud. Existing legal restrictions prevented entities from sharing this information, and Government did not have sufficient powers to direct them to take action.

Currently, the Government does not have powers to support industry with post-incident consequence management. Existing government assistance powers under Part 3A of the SOCI Act are designed to assist with the immediate response to serious cyber security incidents that pose a material risk to Australia's national interests. The powers cannot be used for consequence management because they are limited in scope to the event of the technical cyber incident, and do not cover the consequences following an incident. This means that Government can help defend critical infrastructure from incidents impacting the delivery of essential services, but it has limited ability to assist with managing consequences after an incident. The powers are not designed to manage secondary consequences, no matter the severity or scale of impact.

It is the responsibility of critical infrastructure owners and operators to consider and plan for these risks and implement appropriate strategies to manage incidents impacting their assets. However, the public also expects that the Government will be able to step in as a last resort. Enabling the Government to directly manage consequences to the Australian economy and population would ensure that the SOCI Act better achieves its objective, which is to help manage national security risks with the potential to disrupt the functioning of Australia's society and economy. Should the consequences of an attack on critical infrastructure go beyond the initial incident, the Government has a responsibility to continue working with industry to reduce these impacts.

The *National Emergency Declaration Act 2020* (NED Act) enables the Governor-General to make a national emergency declaration on the advice of the Prime Minister. It also allows a responsible Commonwealth Minister to streamline the exercise of existing national emergency powers listed in the NED Act. It is designed to cut red tape in existing laws to relieve the administrative burden of people affected by a disaster. Part 3A of the SOCI Act is listed as a national emergency law in section 10 of the NED Act.

What we have heard so far

Consumer groups and community stakeholders have identified the need for government to help manage the consequences of cyber incidents. The Australian public expects the Government to work with industry to mitigate harm following a cyber incident and move quickly to help our communities recover. This indicates a need for legislative levers that will allow Government to seamlessly coordinate incident response, from both the technical incident to broader consequence management under the [Australian Government Crisis Management Framework \(AGCMF\)](#) and [Cyber Incident Management Arrangements](#).

Consultation has also highlighted the rapidly evolving nature of cyber risk, with incidents increasing in scale and severity. Across the next five years, we will see new and unanticipated challenges emerging in cyber space. Through consultation on the Cyber Security Strategy Discussion Paper, industry and individual respondents flagged that the risk environment will evolve rapidly in the next decade. It is likely that cybercrime will be assisted by emerging technologies such as generative artificial intelligence. We must be flexible in meeting these evolving threats and acknowledge the potential for the outcomes of cybercrime to significantly impact the Australian economy and our community.

What we have committed to in the Action Plan

Under Initiative 14 of the Strategy, we committed to:

Expand crisis response arrangements to ensure they capture secondary consequences from significant incidents. Government will consult with industry on introducing an all-hazards consequence management power that will allow it to direct an entity to take specific actions to manage the consequences of a national significant incident. This is a last-resort power, used where no other powers are available and where it does not interfere with or impede a law enforcement action or regulatory action.

The Government proposes to establish last resort powers that would seek to help critical infrastructure entities manage the consequences of significant incidents. This includes preventing or mitigating serious or long-term harm to Australians or critical infrastructure or address consequences that prejudice the socioeconomic stability, national security or the defence of Australia.

Proposed amendment to the SOCI Act

We propose to legislate an all-hazards power of last resort, which may only be authorised by the Minister for Home Affairs (the Minister) if there is no existing power available to support a fast and effective response.

Scope of directions power

Subject to industry views, it is proposed that the directions power may be used to:

- Direct a critical infrastructure entity to do or prohibit from doing a certain thing to prevent or mitigate the consequences of an incident, such as a direction to address issues onsite or suspend operation;
- Provide a direction to a critical infrastructure entity to replace documents of individuals or businesses impacted by the incident (where this is not duplicative with other legislative levers);
- Authorise the disclosure of protected information as defined in the SOCI Act to allow for the sharing of information between government entities (including states and territories), between government and industry, or between the affected entity and a third party; and
- Gather information for the purpose of consequence management, if this does not interfere with or impede any other law enforcement action or regulatory action.

The Department seeks your views on the proposed scope of this directions power, and what costs would be incurred in complying with these powers.

Last resort power

By its nature as a last resort power, the proposed consequence management power cannot be exercised if there are existing powers that would be effective and achieve the same outcome. In these circumstances, other relevant powers need to be exhausted before using the consequence management power.

The last resort power may extend into places where an existing or future power may take precedence. This may include future consequence management regimes or instances where personal information is compromised in a data breach and information sharing with third parties is required. In this scenario, if any other minister held a power that would be effective and achieve the same outcome at that point in time, the Minister for Home Affairs would not be able to exercise the proposed consequence management power.

For example, to support a coordinated response to future data breaches, the Government has agreed to amend the Privacy Act to enable the Attorney-General to authorise the sharing of personal information with appropriate entities where this may reduce the risk of harm in the event of an eligible data breach for specified purposes and for a limited time. The Privacy Act power would take precedence over the SOCI Act directions power in relation to sharing personal information. The proposed directions power might be used as a 'last resort' to direct an entity to share personal information (for example, where the Minister for Home Affairs is satisfied that the responsible entity is unwilling or unable to address the consequences that prejudice the socioeconomic stability, national security or defence of Australia) and the Attorney-General has authorised this under the Privacy Act.

Interaction with other policy frameworks

The last resort directions power would be integrated into the current government assistance regime in the SOCI Act and work in tandem with existing policy frameworks to assist in the aftermath of a crisis that impacts critical infrastructure. For example, it would not impede the use of any powers under the NED Act and would be subject to relevant Privacy Act requirements and safeguards relevant to personal information.

If the Government considers using this power, whole-of-Australian-government coordination mechanisms would be convened or mechanisms under the AGCMF would be activated. These mechanisms would inform the overall response to the incident and ensure all relevant consequence management levers are considered. This would include consultation with other government agencies, regulators and law enforcement bodies (including across the Commonwealth, states and territories). This approach would ensure that government has a comprehensive appreciation for the incident, consequences, regulatory levers and available law enforcement actions.

Where a cyber incident results in a data breach involving personal information, entities need to comply with obligations under the Notifiable Data Breaches Scheme. Government has agreed or agreed in principle to further reforms to this scheme, such as establishing the power to permit personal information sharing by the Attorney-General as described above. The use of the directions power will not interfere with or impede regulatory action by the Office of the Australian Information Commissioner (OAIC), and a direction should not duplicate or be inconsistent with obligations under the Notifiable Data Breaches scheme.

Safeguards and oversight mechanisms

The power would be integrated into the existing government assistance powers under Part 3A of the SOCI Act. They will have the following principles and safeguards:

- There will be no change to the duration of a ministerial authorisation (as set out in section 35AG).
- A direction can only be given to a critical infrastructure entity.
- A direction can only be given where it is to address a consequence of an event that has occurred, is occurring or is imminent, and has had, is having or is likely to have, a relevant impact on critical infrastructure.
 - To be considered for use, the consequence/s this power seeks to address must have a causal link to an incident impacting a critical infrastructure asset.
 - The incident must have a 'relevant impact', whether direct or indirect, on the availability, integrity, reliability, or confidentiality of critical infrastructure.
 - In this instance, 'imminent' relates to other critical infrastructure entities (or the affected entity) that may be compromised, or further compromised, by the inciting incident. This will assist in preventing the compounding of incident consequences and limiting potential contagion effects.
- A direction must not interfere with or impede a law enforcement action or regulatory action.
- The purpose of the direction is limited to preventing or mitigating serious or long-term harm to Australians or critical infrastructure or address consequences that prejudice the socioeconomic stability, national security or the defence of Australia.
- Informed by advice based on consultation with Commonwealth, state and territory agencies and regulators, the Minister must be satisfied that no existing regulatory system of the Commonwealth, a state or a territory could be used to provide a practical and effective response to the incident.
- If the power is being considered to direct the sharing of personal information, the minister responsible for the Privacy Act must authorise its use, and subsequent use or disclosure of such information would be subject to the Privacy Act.
- Prior to exercising the power, the Minister must consult with the affected entity.
- The Minister must be satisfied that the responsible entity is unwilling or unable to address the consequences that prejudice the socioeconomic stability, national security or defence of Australia.

- Prior to exercising the power, the Minister must consult with the relevant Commonwealth minister, or first minister of the relevant state or territory.
- In determining whether to exercise the power, the Minister must consider the public interest – for example, whether issuing the direction is in the interest of public health and safety and is proportionate to the risk of inaction.
- Immunities would be provided in the SOCI Act to ensure that entities would not be subject to civil liability when acting lawfully in response to a compulsory legal direction.
- The periodic report under section 60 of the SOCI Act must include the number of directions issued under this power.

The Department seeks your input on whether these principles and safeguards will provide sufficient oversight for the use of this power.

Hypothetical scenarios

Data breaches are not limited to personal information

Non-personal data, such as confidential research data, can be a valuable target for cybercriminals and nation-state actors. The theft of intellectual property and national security research data from our university system has been called out by a number of government agencies as a particular issue of concern. For instance, as part of ongoing efforts to utilise Australian expertise for socioeconomic coercion, confidential research data could be stolen by compromising university research databases. Once stolen, this data could be used by state-based attackers to undermine other critical infrastructure systems. Malicious actors could use the stolen data to plan widespread attacks on critical services and cause disruption to functions of other critical infrastructure assets.

While the university could investigate the incident and upgrade their cyber defences, the Government is uniquely placed to address the consequences for other critical infrastructure entities whose security could be impacted by the stolen data. The university may be unable to act as it does not have access to national communication channels or the asset register.

In this scenario, current government assistance powers would only allow the Government to issue directions to the university. A new consequence management power would be needed to issue directions to other critical infrastructure entities whose systems and critical functions could be disrupted due to the data breach. These directions could include directing entities to upgrade information technology (IT) and operational technology (OT) security to address system vulnerabilities. Critical infrastructure entities breaching existing contracts with IT and OT service providers would be able to rely on the immunity provisions to enable compliance with the direction and avoid civil liability.

A cyber incident may have complex non-cyber consequences

Cyber incidents often result in cascading consequences that have a wide-reaching impact on society. Consider the scenario of an issue-motivated group exploiting controls at Australia's only chlorine gas manufacturer, disrupting the national supply of chlorine. As critical infrastructure entities, water utilities are critically reliant on chlorine gas to produce drinking water in urban environments. These entities can only store limited amounts of chlorine gas onsite due to industrial safety standards and regulations. As a result, there is a national shortage of chlorine gas for water treatment within one to three weeks of the cyber incident.

International supplies will take months to arrive, and cannot be easily relied upon due to Australia's unique chlorine handling infrastructure, with any use of internationally supplied drums requiring major re-engineering of water utility infrastructure or significant compromise of work health and safety legislation. This leads to intense competition between jurisdictions and industry, with a corresponding loss of public confidence in government infrastructure and the potential to create public unrest.

In this scenario, the Government may need to direct entities to take preventative actions or suspend their operations. This could include triaging the remaining national chlorine supplies to prioritise entities and communities with the greatest need. Commonwealth health agencies would complement state and territory emergency management efforts. The Government may also need to direct entities to truck water from treated sources to critical infrastructure such as hospitals.

Non-cyber hazards can cause severe consequences for critical infrastructure

Non-cyber hazards can also cause major disruption and damage to critical infrastructure. Suppose that it is the middle of summer and energy generation is already operating near peak capacity. A malicious insider and issues-motivated actor sabotages a gas pipeline near agricultural land, causing an uncontrolled release of gas and liquid fuels that results in cessation of gas to a large population. The critical infrastructure gas supplier is willing to cease the flow of gas to reduce physical hazards but cannot coordinate the delivery of gas from other sources, nor can it adequately address all health hazards caused by land contamination.

In this scenario, the Government may need to issue a 'do not disturb'/quarantine order for the contaminated area and direct the entity to engage in remediation to avoid groundwater contamination and human health issues. Concurrently, the Government may need to coordinate alternate transport of critical liquid fuels to support the operation of other critical infrastructure sectors. Finally, the Government may need to redirect resources and issue prioritisation orders for electricity supply to households and hospitals if energy demand outstrips generation supply that may otherwise be supplemented by gas-powered redundancy.

Your input

How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?

37. How would a directions power assist you in taking action to address the consequences of an incident?
38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?
39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

Measure 7

Simplifying how government and industry shares information in crisis situations – Protected information provisions

The issue

The SOCI Act currently captures a wide range of documents that are “obtained by a person in the course of exercising powers, or performing duties or functions, under this Act”. Both government and industry stakeholders have raised concerns regarding how they should approach the capture of information under the Act. Unclear provisions for sharing information limit the ability of responsible entities and government departments to manage crisis situations.

The protection and disclosure of information relating to the operation, structure, and location of critical infrastructure assets is vital to preventing and mitigating the impact of those seeking to do harm to Australia. Due to issues limiting the sharing of information during an attack on critical infrastructure (as evidenced in recent incidents), we propose to amend the protected information framework to better support industry and enable a more agile response to attacks.

What we have heard so far

Through our series of town halls during the CIRMP grace period, we have reiterated that the protected information provisions are not intended to limit or impede the sharing of information with government or with regulators. These provisions should not interfere with the ability of other regulators to carry out their functions, or an organisation’s ability to respond to an incident. We continue to provide case-by-case advice and have held a number of bilateral meetings to provide more tailored assistance to entities in navigating the provisions. Drawing on this engagement, we have also published additional guidance on the CISC website clarifying the protected information provisions, including guidance on the most frequently asked questions.

While this guidance and engagement has been well received, industry continues to express that the current protected information regime limits effective information sharing. We have heard that current provisions are overly complex, impeding the response to high risk, time sensitive events and potentially exacerbating the consequences of an attack.

What we have committed to

On 21 November 2023, the Attorney-General announced the completion of a review of secrecy provisions across Commonwealth laws conducted by the Attorney-General's Department¹⁷. As part of these reforms, Government accepted the establishment of principles for the framing of secrecy offences to ensure consistency of secrecy provisions across Commonwealth laws. These included:

- removal of criminal liability from approximately 168 secrecy offences out of the 875 total secrecy offences;
- further reductions in the number of offences through the enactment of a new general secrecy offence in the *Criminal Code Act 1995* that will ensure Commonwealth officers and others with confidentiality obligations can be held to account for harm caused by breaching those obligations;
- improved protections for press freedom and individuals providing information to Royal Commissions; and
- establishment of principles for the framing of secrecy offences that will guide the future development and consistency of secrecy laws across Commonwealth laws.

The proposed changes to the protected information network under the SOCI Act outlined below have been developed to align with these principles.

Proposed amendment to the SOCI Act

Revision of the 'protected information' definition: A harms-based approach

The current definition of protected information is broad and has led to varying interpretations by industry and Government. To ensure there is consistent understanding and application of the protected information framework, we propose that the definition be given greater clarity and specificity. This will make it easier for entities to protect and share information relating to major incidents.

We propose to clarify that entities should take a harms-based approach when disclosing information under the SOCI Act. This means that when considering whether to disclose information, individuals must consider the potential harm or risk to the security of their asset, commercial interests, the Australian public, the socioeconomic stability, national security and defence of Australia. Clarifying that entities must consider the potential harm of releasing information addresses the underlying intent of these provisions, provides boundaries for disclosure, and is in line with the principles of the final report of the Secrecy Review. This step will provide more clarity for both industry and government. It also addresses previous concerns that all information shared by industry could be captured under the SOCI Act, impacting community trust. Adopting this principle would achieve flexibility, while maintaining boundaries between information that may be shared in the interest of transparency and information that must remain protected to prevent or mitigate harm.

17. AGD (2023). *Review of secrecy provisions: Final report*

Clarification of disclosure provisions

Current provisions authorise the use and disclosure of information by entities if they are ensuring compliance with a provision of the SOCI Act. However, this requirement does not clearly apply in the case where an entity may seek to disclose information for the purposes relevant to the continued operation or mitigation of risk to an asset. This limits the ability of responsible entities to be agile in complying with their obligations.

We propose to clarify this authorisation to allow entities to disclose information for the purpose of the continued operation of, or mitigation of risks to, an asset. This approach will make information disclosure easier for business and help entities achieve broader security uplift across critical infrastructure. This authorisation will be balanced with security considerations through the application of the harm-based approach to disclosing information under the SOCI Act, as outlined above.

While the Secretary of Home Affairs may disclose protected information to ministers and their departments, there is a requirement that ministers and agencies fall into certain categories in order to receive this information. In practice, gaps in these categories can cause implementation issues. For example:

- These categories do not include emergency management agencies (either Commonwealth, state or territory), thereby limiting the scope of incident response coordination between departments.
- The categories do not include regulatory agencies who may have responsibility for responding to the incident, such as the OAIC for a cyber incident that is also a notifiable data breach.
- For state and territory agencies, there are limits on the ability for the Commonwealth to disclose information relating to data storage and processing assets to a relevant jurisdiction, if the physical infrastructure is not located in that jurisdiction.

We propose that provisions relating to government entities should be broadened to allow disclosure of protected information to all Commonwealth, state and territory government entities regardless of policy responsibility, where disclosure is necessary for the purpose of upholding the security and resilience of critical infrastructure or protecting national security. This threshold limits disclosure to circumstances relating to the defence of Australia, national security and the socioeconomic stability of Australia or its people.

Additionally, while information may be disclosed to the Inspector-General of Intelligence and Security (IGIS) by the Secretary for Home Affairs, and information may be disclosed by the IGIS to an Ombudsman official, there is no authorised disclosure provision to allow industry, government officials, or individuals to voluntarily disclose information to the IGIS. Unintended capture and criminalisation of this form of disclosure impedes the agency in performing its functions and adversely impacts Australia's overall security apparatus by dis-incentivising potential respondents from engaging with the IGIS. Amendment to existing sections concerning authorised disclosure to the IGIS (s43A, s43C) to include voluntary disclosures to the agency would alleviate this issue.

Your input

The Department seeks your views and feedback on the proposed changes to the secrecy provisions under the SOCI Act:

- 40. How can the current information sharing regime under the SOCI Act be improved?
- 41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

Measure 8

Enforcing critical infrastructure risk management obligations – Review and remedy powers

The issue

There is currently no legislative framework which allows the regulator to issue a direction to an entity to remedy a deficient risk management program (RMP) when a regulator assesses it as such and when the entity is unwilling to comply with the regulator's recommendations. Without this ability, the CIRMP obligation may not achieve its intent of embedding preparation, prevention, and mitigation activities into the business-as-usual operations of critical infrastructure assets.

The CISC recognises that both educative and enforcement mechanisms are necessary to provide an effective and flexible regulatory system that does not unnecessarily impede the efficient and effective operations of regulated entities. A range of regulatory options are available to address non-compliance – including, but not limited to, education and engagement, information gathering powers, corrective action plans, infringement notices, directions and enforceable undertakings.

The Secretary of Home Affairs may require an entity to produce its CIRMP under s37 of the SOCI Act, and provide a corrective action plan where the CIRMP is assessed as deficient. However, the entity cannot be directed to take specific actions to improve the maturity of their CIRMP without seeking an enforceable undertaking. This represents a gap in the graduated regulatory powers available to the regulator.

What we have heard so far

Ahead of the expiry of a six month grace period on 17 August 2023, we hosted three interactive town halls on the CIRMP obligation. We also held a number of bilateral meetings to provide deeper engagement with entities to discuss their specific circumstances and obligations. We held a series of webinars focused on all-hazards risk management. We also launched our first podcast series, the Trusted Insider, which examines the risk of insider espionage, sabotage and how unauthorised access to information can cause harm to Australia's critical infrastructure.

Importantly, we continue to receive positive feedback from stakeholders on this program of engagement. Anecdotally, owners and operators who have engaged with us on SOCI Act reforms for some time have remarked on substantive improvements in outreach and engagements. The uplift in engagement has also proactively attracted new stakeholders, who are keen to learn more about SOCI Act reforms.

The majority of critical infrastructure entities are taking a proactive approach to implementing their CIRMPs or keeping the CISC informed on the development of their CIRMPs. Even though responsible entities are not obligated to provide an annual report for the 2022-2023 financial year, the CISC has encouraged voluntary reporting so we can work in partnership with entities on implementing their CIRMPs.

To date, the CISC has received 54 voluntary annual reports. There has been a good level of detail in the annual reports outlining the approaches that entities are taking to protect their assets against the four main types of hazard. This includes identifying the risk management framework adopted by the entity to mitigate these risks.

While our overall posture will begin to move towards compliance in 2024, we remain committed to the continued education and engagement of responsible entities. It is hoped that the continuance of an educative approach will encourage compliance from responsible entities without requiring further sanction. Compliance and enforcement levers remain a last resort.

Proposed amendment to the SOCI Act

We propose to introduce a formal, written directions power in Part 2A of the SOCI Act to address seriously deficient elements of a CIRMPs, when:

- The Secretary of Home Affairs or relevant Commonwealth regulator¹⁸ has, following consideration of the facts and the entity's obligations under the SOCI Act and delegated legislation, formed a reasonable belief that an entities' CIRMP is seriously deficient; and
- The deficiency carries a material risk to the socioeconomic stability, defence, or national security of Australia; or
- There is a severe and credible threat to national security; and
- The Secretary or relevant Commonwealth regulator is satisfied that the direction is likely to compel an effective response to address that risk.

This directions power would be managed by appropriate oversight mechanisms. Before making the decision to issue a direction, the Secretary/regulator must give the entity a written notice that states the intended decision to issue a direction, reasons for the direction and invite the entity to respond. When deciding whether to issue the direction, the Secretary/regulator must consider relevant matters including the entity's response, any action taken, or proposed to be taken, by the entity to prevent or remedy the non-compliance, as well as the extent and degree of non-compliance.

Wherever possible, the CISC seeks to work in partnership with industry to ensure regulated entities understand and effectively manage their risks. Deficiencies will be assessed and directions issued in accordance with the CISC Compliance and Enforcement Strategy. For example, a key principle of the Compliance and Enforcement Strategy is proportionality – that is, taking into account the security implications of the non-compliance, the seriousness of the non-compliance, the compliance history and regulatory posture of the entity, the need for deterrence, the facts of the matter at hand, and the impact on Australia's reputation or Australian interests overseas.

18. Defined in section 5 of the SOCI Act to mean a Department or body that is specified in the rules. For example, the 'relevant Commonwealth regulator' for payment systems is prescribed in the CIRMP Rules as the Reserve Bank of Australia. For certain defence industry assets, the Department of Defence is prescribed as the relevant Commonwealth regulator. For all other entities, the regulator is the Department of Home Affairs' Cyber and Infrastructure Security Centre.

Examples of circumstances where the Secretary may direct a responsible entity to rectify seriously deficient elements of a CIRMP include:

- Where the entity is not meeting or taking reasonable steps to meet required maturity levels of prescribed cyber security frameworks, the Secretary may direct the entity to enhance its cyber controls to mitigate risks to the asset.
- Where an entity does not have a process in place to assess the suitability of critical workers that have access to critical components of a critical infrastructure asset, the Secretary may direct the entity to implement a process to address the risk of trusted insiders using their position to cause harm or undermine Australia's national security.
- Where the entity has failed to consider and minimise risks in the threat landscape that pose a potential risk to their asset, the Secretary may direct the entity to consider those risks. For example, if an electricity distributor has failed to minimise the threat posed by cyber attacks on their operational technology, the Secretary can direct them to consider those risks.

Depending on the deficiency, the entity would still have some discretion in how they integrated a direction to redress a seriously deficient CIRMP. For example, the entity would retain the discretion to comply with their chosen cyber security framework. This is in line with the principles-based nature of the obligation and keeps the onus on the responsibility entity to mitigate the risks facing their critical infrastructure asset.

No mechanism currently exists in the civil penalty regime to effectively address wilful non-compliance with CIRMP requirements. In accordance with the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, we propose the penalty for the proposed power should align with the existing penalty in the SOCI Act for failure to comply with a direction given under subsection 32(2) – that is, a penalty of 250 penalty units.

Your input

The Department seeks your feedback and advice on how this legislative change may impact you and your business, particularly for responsible entities with an asset already captured by the CIRMP obligation:

42. How would the proposed review and remedy power impact your approach to preventative risk?

Measure 9

Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

The issue

Security regulation for the telecommunications sector currently spans across Part 14 of the *Telecommunications Act 1997* (Telecommunications Act) and the SOCI Act. Industry has expressed confusion about the multiple regulatory frameworks that address security obligations in the telecommunications sector. The current framework also limits the ability for the Minister for Home Affairs and the Department of Home Affairs to ensure compliance with the security obligations outlined under the Telecommunications Act.

Telecommunications assets are an integral and interconnected component of the broader critical infrastructure ecosystem. To ensure that we have a clear regulatory framework for these assets, we need to address legislative complexities in security and risk mitigation for the sector.

What we have heard so far

In its Review of Part 14 of the Telecommunications Act, finalised on 7 February 2022, the Parliamentary Joint Committee on Intelligence and Security (PJClS) made six recommendations to uplift the security of the telecommunications sector. The six recommendations are largely consistent with our expectations from our ongoing engagement with the sector.

In May 2023, the Government established the Australian Telecommunications Security Reference Group (Reference Group). The Reference Group is chaired by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) in close collaboration with the Department of Home Affairs, and comprises of members from the telecommunications industry and peak bodies. During the first phase, the Group considered options to achieve better regulatory alignment for security regulation across the sector.

Throughout these meetings, members called for reduced complexity, minimised duplication and scalable obligations. In July 2023, the Reference Group finalised a report to Government. Industry members supported the proposed approach of consolidating security regulation for the telecommunications sector under the SOCI Act.

What we have committed to in the Action Plan

Under Initiative 13 of the Strategy, we committed to:

Align telecommunication providers to the same standards as other critical infrastructure entities, commensurate with the criticality and risk profile of the sector by moving security regulation of the telecommunications sector from the Telecommunications Sector Security Reforms (TSSR) in the Telecommunications Act 1997 to the SOCI Act.

Proposed amendment to the SOCI Act

The Government is committed to engaging industry to achieve best practice security regulation for the telecommunications sector.

Based on advice from the Reference Group, we propose to consolidate security regulation for the telecommunications sector under the SOCI Act. Security obligations from Part 14 of the Telecommunications Act, including the security obligation and the notification obligation, will move to the SOCI Act. Additionally, any 'SOCI-like' obligations currently applied under the Telecommunications Act will be repealed and activated under the SOCI Act. The new framework will harmonise the current security obligation and notification obligation, into a new Telecommunications Security and Risk Management Program (TSRMP) within the SOCI Act. Ensuring no loss of cyber maturity and maintaining security standards will be a key consideration when harmonising these frameworks.

The TSRMP will be co-designed with the sector and the Reference Group to ensure we meet industry's calls for reduced complexity, minimised duplication and scalable obligations. By consolidating security regulation for the telecommunications sector under the SOCI Act, we will align obligations for telecommunications entities with other critical infrastructure sectors (e.g., data storage and processing, financial services). These reforms will also promote continued uplift and overall enhancement of the critical infrastructure ecosystem.

Your input

The Department seeks your feedback and advice on how this legislative change may impact you and your business. We are particularly interested in the impacts of changes to the following obligations:

- TSRMP obligation
- Notification obligation

In evaluating the impact, we ask you to consider the following questions:

43. What security standards are most relevant for the development of an RMP?
44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?
45. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?
46. How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?
47. How can outlining material risks help you adopt a more uniform approach to the notification obligation?



Next steps

The Department welcomes your views on the proposals in this Consultation Paper. We want to ensure that proposed legislation reform benefits from your expertise, learnings and experiences.

How to make a written submission

The Australian Government invites written submissions on the detailed questions in this Consultation Paper. For your reference, the full list of questions is extracted at Attachment A.

Written submissions will close at **5.00 PM AEDT, Friday 1 March 2024**.

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

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

Evaluating impacts

For the proposals to achieve their goals, we are committed to ensuring that the benefits outweigh any regulatory impact. We aim to build a full picture of the impacts and will need your detailed input to develop a comprehensive assessment. In addition to the financial impacts, we welcome views on the impacts of measures on affected entities' ability to utilise and share data.

We will shortly release a schedule of sector-specific impact analysis sessions, which we also encourage you to attend. These sessions will include time for questions and answers to discuss the details of the proposals and any other concerns. We will provide you with costing templates before or during these sessions and guide you through them. This will allow us to allow us to fully appreciate the impacts of the proposed reforms.

Face-to-face consultation

We will run a series of general town hall meetings, sector-specific meetings, and be available for bilateral discussions during the consultation period.

We will continue to engage with stakeholders through existing engagement mechanisms, including the Trusted Information Sharing Network (TISN). The links to town halls, sector-specific meetings and TISN sessions will be made available on our website: www.cisc.gov.au.

What we will do with your feedback

Feedback from written submissions and face-to-face engagement will be used by the Department to refine the legislative proposals described in this Consultation Paper. Your feedback will help us fully understand the costs and benefits of options to inform the policy development process and advice to Government. Any regulatory burden will be carefully considered alongside the benefit from proposed changes to strengthen our cyber resilience and posture.

After reviewing your feedback on the proposals in this Consultation Paper, the Department will provide advice to Government on new legislation implementing the proposals to be considered in 2024.

Privacy collection notice

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

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

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

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

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

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

Attachment A: Consultation Paper questions

Part 1 – New cyber security legislation

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?
2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?
3. What alternative standard, if any, should the Government consider?
4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?
5. What types of smart devices should not be covered by a mandatory cyber security standard?
6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?
7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?
9. What additional mandatory information should be reported if a payment is made?
10. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?
11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than \$10 million per year?
12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?
13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?
14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?
16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?
18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?
19. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?
21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?
22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?
23. What factors would make a cyber incident worth reviewing by a CIRB?
24. Who should be a member of a CIRB? How should these members be appointed?
25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?
26. How should the Government manage issues of personnel security and conflicts of interest?
27. Who should chair a CIRB?
28. Who should be responsible for initiating reviews to be undertaken by a CIRB?
29. What powers should a CIRB be given to effectively perform its functions?
30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?
31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?
32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?
33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

Part 2 – Amendments to the SOCI Act

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

- 34. How are you currently managing risks to your corporate networks and systems holding business critical data?
- 35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?
- 36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

- 37. How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?
- 38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?
- 39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

- 40. How can the current information sharing regime under the SOCI Act be improved?
- 41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

- 42. How would the proposed review and remedy power impact your approach to preventative risk?

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

- 43. What security standards are most relevant for the development of an RMP?
- 44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?
- 45. How can outlining material risks help you adopt a more uniform approach to the notification obligation?
- 46. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?
- 47. How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?

