BLACK
INK
LEGAL

2023–2030 Australian Cyber Security Strategy: Legislative Reforms

Response to Consultation paper

BLACK INK LEGAL
Level 14/167 Eagle Street, Brisbane, QLD, 4000

Contents

About Black Ink Legal

Black Ink Legal is a boutique provider of virtual and onsite legal, strategic sourcing, procurement and contract management services to State and Commonwealth governments and private industry. Black Ink Legal was incorporated as an Integrated Legal Practice in 2021 drawing on the founder's long-standing success providing legal, procurement and commercial services in the Commonwealth sector since 2009. We specialise in assisting our clients to develop, structure, negotiate and manage strategically important projects and procurements through to deal completion.

Black Ink Legal specialises in cyber security law, and our lawyers possess a deep understanding of the complex mosaic of the cyber and technology legal landscape. Our expertise extends to advising a diverse array of clients, ranging from emerging tech startups to established multinational corporations, on a broad spectrum of cyber-related legal issues. This includes data protection and privacy, compliance with local and international cyber security standards, breach response and notification requirements, and the management of cyber risks in contractual agreements. We are proactive in supporting and assisting our clients to navigate the intricacies of cyber law, to safeguard their digital assets and intellectual property, while ensuring their operations align with current legal frameworks. Black Ink Legal is passionate about and committed to staying at the forefront of technological advancements and legislative changes to empower our clients to achieve their business objectives with confidence, knowing their legal exposure is minimized and their innovations are protected.

Black Ink Legal extends its boutique legal and strategic services to Australian managed IT providers, emphasising support in privacy and cybersecurity with clients and partners specialising in technical cyber support and insider threat detection technology. Our advisory services are designed to address the unique challenges faced by the IT and technology sector, offering specialised guidance in navigating the complexities of data protection laws and cybersecurity threats. We understand the critical importance of safeguarding digital assets and personal information in today's interconnected world. By partnering with IT and technology firms, we aim to deliver comprehensive legal strategies that enhance their cybersecurity measures and ensure compliance with Australian privacy laws, thereby fortifying our clients' defences against cyber threats and legal vulnerabilities.

Executive Summary

Black Ink Legal welcomes the opportunity to respond to the Department of Home Affairs' Consultation Paper in relation to the *2023–2030 Australian Cyber Security Strategy* (Cyber Security Strategy) and associated *2023-2030 Australian Cyber Security Action Plan* (Action Plan). We commend the Department of Home Affairs for seeking to constructively engage with stakeholders to inform the development of the Cyber Security Strategy and associated Action Plan, and we welcome the opportunity to continue to engage with the Department as work on both progresses.

The unprecedented maturation of artificial intelligence and by extension internet connected smart technology is changing how we live, work, and do business. It is fair to say that for the foreseeable future, we will continue to embrace the lifestyle and cultural conveniences that have developed with the evolution of these modern technologies. However, the rapid evolution of technology and uptake within society has outpaced the existing legislative framework by a significant margin.

The Cyber Security Strategy addresses this evolving landscape of artificial intelligence and internet-connected smart technology, emphasising the need for robust security measures in connected Internet of Things (IoT) consumer devices. The strategy aims to establish outcome-focused provisions to guide all stakeholders in securing their products effectively. It advocates for a Shared Responsibility Model across the smart device supply chain, encompassing manufacturers, suppliers, developers, service providers, and regulatory authorities. Further, the strategy highlights the importance of aligning with standards and frameworks including the ETSI EN 303 645 as well as considering broader industry standards. It emphasises a baseline level of security, data protection considerations, and collaboration with law enforcement and intelligence agencies. The strategy also focuses on public-private partnerships, regular assessments, public awareness, collaborative response efforts, and independent oversight through the proposed Cyber Incident Review Board (CIRB).

Looking forward, the Cyber Security Strategy should seek to bring together best practice security for IoT consumer devices in a set of outcome-focused provisions that support all parties involved in the development and manufacture of consumer IoT with a robust and pragmatic guidance on securing their products. In general, the resultant legislation should seek to be outcome-focused, rather than prescriptive, to give organisations the flexibility to innovate and implement security solutions appropriate for their products.

Black Ink Legal is acutely aware that the Cyber Security Strategy, draft legislation and proposed changes to the SOCI Act will not solve all security challenges associated with IoT. There is no single standard / strategy that can protect against attacks that are prolonged or sophisticated or that require sustained physical access to a device. However, with a key focus on the technical controls and organisational policies that matter most in addressing the most significant and widespread security shortcomings, the draft legislation should consider a baseline level of security, to protect against elementary attacks on fundamental design weaknesses (for example the use of easily guessable passwords) and make the provisions applicable to all consumer IoT devices. The legislation should be complemented by other standards (for example AI, data protection etc) and standards that define more specific provisions and fully testable and/or verifiable requirements for specific devices.

Many consumer IoT devices and their associated services process and store personal data, so the draft legislation should take into consideration the interplay with data protection legislation including the *General Data Protection Regulation 2016* where Security-by-Design is an important principle. The Cyber Security Strategy presents a comprehensive framework to address cybersecurity challenges in IoT devices. By promoting secure-by-design principles, fostering collaboration across stakeholders, and establishing mechanisms like the Cyber Incident Review Board (CIRB) for incident review and policy guidance, the strategy aims to enhance national cybersecurity resilience. It underscores the importance of continuous improvement, stakeholder engagement, and adherence to best practices to create a safer digital environment for all Australians.

Response to 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?

In the smart device supply chain, responsibility and accountability for complying with a proposed mandatory cybersecurity standard should be shared among a number of key entities in the supply chain to ensure comprehensive protection at every stage of the smart device product lifecycle (Shared Responsibility Model). A Shared Responsibility Model ensures accountability and serves to address potential vulnerabilities at every stage of the product life cycle, from design to disposal. Such entities should, at a minimum, include:

a) Manufacturers and companies responsible for producing smart devices, to ensure that smart devices are designed and built according to the requirements of a mandatory cyber security standard.

b) Suppliers of components and materials used in smart devices. These component parts would need to meet the requirements of the standard.

c) Developers that create the software and firmware used to operate smart devices (including applications that can be added to smart devices to connect to the other online applications). This software and firmware should be developed in accordance with and comply with a cyber security standard.

d) Service providers such as those offering cloud services, storage services, maintenance services are responsible for the ongoing security of smart devices. Accordingly, these service providers should ensure that their services are provided in accordance with the requirements of a mandatory cybersecurity standard.

e) Regulatory Authorities, including the proposed CIRB, governing the operation and application of role setting and enforcement of cyber security standards within the smart device supply chain.

To effectively implement a Shared Responsibility Model, clear guidelines and communication channels must be established among all stakeholders – which should be included in the proposed cyber security standard. Collaboration across the supply chain, along with transparent and enforceable compliance mechanisms, are essential for upholding cybersecurity standards. Another consideration is to ensure alignment with related standards including manufacturing standards. Additionally, continuous education, awareness, and incentives for compliance can further enhance the security posture of the smart device ecosystem.

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?

The ETSI EN 303 645 standard, designed to improve the security of consumer IoT devices, includes several key principles beyond the initial three. While the first three principles focus on passwords, vulnerability management, and software updates, the remaining ones cover a wide range of security measures.

The first three principles:

a) No Universal Default Passwords
b) Implement a means to Manage Reports of Vulnerabilities
c) Keep Software Updated

are an excellent minimum starting point. However, for a minimum baseline to be effective in practice the remaining ten principles should also form part of the minimum baseline for consumer-grade IoT devices sold in Australia. These remaining principles include:

a) No Universal Default Passwords
b) Implement a means to Manage Reports of Vulnerabilities
c) Keep Software Updated
d) Securely Store Sensitive Security Parameters
e) Communicate Securely
f) Minimise Exposed Attack Surfaces
g) Ensure Software Integrity
h) Ensure that Personal Data is Protected
i) Make Systems Resilient to Outages
j) Monitor System Telemetry Data
k) Make it Easy for Users to Delete Personal Data
l) Make Installation and Maintenance of Devices Easy
m) Validate Input Data,

and collectively form a comprehensive baseline framework for securing IoT devices That should be considered by the Department. These principles address not only technical aspects but also user interaction and data protection related concerns. By implementing and adhering to these principles as a minimum baseline, manufacturers, and other entities in the IoT supply chain will be positioned effect to Secure-by-Design IoT products far more effectively than limiting the baseline to the first three principles.

3. What alternative standard, if any, should the Government consider?

As the government refines its Cyber Security Strategy, and formulates the proposed IoT standard, rather than the question what an alternative to the ETSI EN 303 645 standard is, which suggests an either / or approach, Black Ink Legal recommends the government consider how the ETSI EN 303 645 standard might intersect with other relevant industry standards, including what, if any cross-jurisdictional impact there might be.

In addition to the ETSI EN 303 645 standard, other standards that can complement and enhance the proposed Cyber Security Strategy include international standards such as ISO/IEC 27001, the GDPR and the NIST Cybersecurity Framework (NIST CSF) developed by the U.S. National Institute of Standards and Technology. A more comprehensive list of cyber related standards to consider includes:

ISO / IEC 27001 is an internationally recognized standard for managing information security. It provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). This standard outlines a risk management process involving people, processes, and IT systems, thereby ensuring the confidentiality, integrity, and availability of information. Organizations achieve ISO/IEC 27001 certification through a systematic audit process, demonstrating their commitment to information security. The standard is applicable to all sectors and sizes of organizations, offering a structured approach to securing information assets, managing risks, and enhancing trust with stakeholders.

ISO/IEC 27032: This international standard focuses on cyber security and provides guidelines for enhancing the security of digital networks and services. It emphasizes the importance of collaboration in securing cyberspace, making it particularly relevant for initiatives that require coordination across different sectors and international borders.

GDPR (General Data Protection Regulation): European in origin, however the GDPR has set an international benchmark for data protection and privacy. Australian organizations operating internationally or handling data from European citizens and organisations, can benefit (and at times it is legally necessary) from aligning with GDPR requirements, enhancing privacy protections and building trust with users.

CI DSS (Payment Card Industry Data Security Standard): For organisations that handle cardholder information, aligning with PCI DSS can help prevent payment card fraud and protect against data breaches. It provides a robust framework for securing payment systems and is essential for e-commerce and retail sectors.

Cloud Security Alliance (CSA) Security, Trust, & Assurance Registry (STAR): Cloud computing is increasingly integral to business operations. Accordingly, aligning with CSA STAR can assist organisations manage the security of their cloud services. This standard offers comprehensive security guidance for cloud service providers and users, promoting transparency and trust in cloud computing.

IEC 62443: This series of standards is designed for industrial automation and control systems security. It provides a structured approach to securing industrial operational environments, critical for protecting Australia's critical infrastructure from cyber threats.

NIST SP 800-53: This publication provides a catalog of security and privacy controls for federal information systems and organizations in the United States, but its comprehensive approach to risk management and control selection could be adapted for the Australian context, particularly in government and critical infrastructure sector.

It is important to note that there is danger in adopting standards or legislation form other jurisdictions without considering how they would apply in an Australian context. Careful consideration of the uniquely Australian context is essential as well as ensuring there isn’t excessive duplication or confusion.

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 PSTI Act in the UK?

Black Ink Legal supports the inclusion of a definition detailing what is a smart device that is subject to an Australian mandatory standard. Whether that definition should be subject to exceptions depends on what these exceptions are and how extensive. The definition should be broad enough so that it retains its currency as technology evolves.

Exceptions to this definition might include non-connectable products (by default), and products covered by other regulatory frameworks, for example, medical devices or automotive vehicles, which are subject to stringent regulatory standards, including cybersecurity measures. It will be important, when drafting the new cyber security legislation, to consider how these other regulatory frameworks might intersect with the new laws under the cyber security strategy. Consider also whether temporary exceptions would apply under the proposed legislation and in what circumstances. For example, products that are in the process of being brought into compliance with the Act's requirements.

The definition in the *Product Security and Telecommunications Infrastructure (PSTI) Act* in the UK is a useful starting point, however, there is danger in taking the definition from the UK without considering how it would apply in an Australian context. Careful consideration needs to be had of the uniquely Australian context.

Broadly, the UK PSTI Act defines smart devices subject to mandatory security standards as ‘connectable products’. Connectable products are further described in the Act as products capable of connecting to the internet or other smart devices through a network. These devices must also be capable of transmitting and receiving data. This includes a broad range of devices such as smart cameras, televisions, toys, speakers, wearable health trackers, and household appliances like fridges and washing machines. The core focus is on the security of consumer connectable products, including a wide range of IoT devices. These standards are intended to protect consumers from cyber threats by ensuring that products have a mandated baseline level of security features.

Noting the intention of the proposed new cyber security legislation, the UK definition of connectable products could work in an Australian context. However, until we see the text of the draft legislation it is only a theoretical assumption that the definition will translate to the Australia legislative context. That said, Black Ink Legal welcomes the opportunity to consider any proposed drafting when it is available.

5. What types of smart devices should not be covered by a mandatory cyber security standard?

Exemptions could include smart devices with no external connection to the internet or those which might already be governed by stringent standards. If the latter, the question becomes how those standards play into the IoT standards being contemplated by this cyber strategy.

It's important to recognise that certain types of smart devices may have specific characteristics or uses that could impact the applicability of a mandatory cyber security standard. However, it's generally recommended that all smart devices are covered by some form of cyber security standard to mitigate potential risks.

For example, critical infrastructure devices might already be subject to specific regulations, making a separate mandatory cyber security standard redundant. Additionally, some low-risk devices with limited functionality might be exempt from certain aspects of the standard.

When considering the types of smart devices that should not be covered by a mandatory cybersecurity standard, it's essential to differentiate based on the device's purpose, functionality, the data it handles, and its integration into larger systems. For example, devices considered low risk, that have smart capabilities but do not connect to the internet or other devices might be exempted. These could include simple, standalone electronic devices that use smart technology for functionality improvements but lack network connectivity, thus posing minimal cybersecurity risk. Additionally, devices used for educational purposes, such as smart devices specifically designed exclusively for educational use, especially those used in controlled environments like schools, might not require stringent cybersecurity standards if they do not handle sensitive data or connect to critical networks. Consider also smart home appliances that offer limited internet connectivity and are used for non-critical functions, such as smart toasters or coffee makers. However, this consideration must be carefully evaluated against the potential for these devices to be vulnerabilities or entry points into a broader network. Legacy devices that can no longer be updated or secured to meet new standards might be exempt (subject to stringent sunset provisions) to allow users time to transition to more secure, contemporary alternatives.

These exemptions should come with clear guidelines on usage limitations and transition to obsolescence plan. Certain industrial devices that are smart-enabled but operate within closed, highly secure networks might be exempt from broad consumer-focused cybersecurity standards. These devices often operate under industry-specific security protocols which should be aligned with the proposed new legislation where relevant and appropriate. Devices used exclusively for research and development within controlled environments might be exempt, provided they do not enter commercial markets or connect to public networks without meeting legislated cybersecurity requirements. Some smart health devices designed for personal use without the capability to connect to the internet or external devices might be considered for exemption, as is the case in the UK. However, the focus must be on devices that do not store or transmit sensitive health or personal data.

It's important to note that exemptions are, by definition, the exception not the rule. The exemption of any device from mandatory cybersecurity standards or reporting obligations should be made with caution, after all potential, foreseeable risks and evolving threats have been mitigated. The decision to exempt an IoT smart device should be based on a thorough risk assessment, considering not just the current use case but also potential future integrations and functionalities that could increase the device's risk profile. In certain circumstances consider whether the proposed Cyber Incident Review Board (CIRB) should provide an exemption monitoring and approval function. Additionally, even if devices are exempted from mandatory standards, best practices for security should still be encouraged to minimise risks to organisations, government and individuals.

Consider also the exceptions outlined in the ETSI EN 303 645 v2 (2020-06) concerning consumer IoT devices. These exceptions provide flexibility in implementing security measures in circumstances where certain provisions may not be feasible or appropriate due to device constraints or specific functionalities. For example, software components that can’t be updated due to technical limitations or design constraints (ETSI exemption 3). Another example is where the device has physical limitations that restrict its ability to process, communicate, store data or interact with users such as devices with limited battery life, memory, processing power, memory or network bandwidth (ETSI exemption 4). In total there are thirteen exemptions, but we won't enumerate them all here. However, it is worth noting that these exceptions under the ETSI are designed to provide a structured approach for organisations involved in the development and manufacturing of consumer IoT devices to effectively address security challenges while considering practical constraints. By offering flexibility in implementing security measures these exceptions serve to balance security requirements with the diverse nature of IoT devices and their ever-evolving functionalities.

6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

The appropriate timeframe for the industry to adjust to new cybersecurity requirements for smart devices varies based on several factors, including the complexity of the requirements, the current age and cybersecurity posture of the devices, and the resources available to manufacturers. However, a balanced approach that considers both the need for enhanced security and the challenges of implementation should be key in determining effective and feasible timelines.

Black Ink Legal suggests that the government consider a staged phase-in of the new requirements. For example:

- Short-term (a period of six – twelve months) for minor updates or adjustments that already largely align with extant industry practices, and which might require minimal hardware uplift or can be addressed through software updates.
- a medium-term phase in period (approximately one to two years) for more significant changes that require substantial software updates, modifications to a device's functionality or minor hardware modifications. This timeframe would allow organisations and manufacturers to plan for and integrate the changes into their product development and overall life cycle, including testing and deployment.
- Long-term (two to five years) for requirements that necessitate major hardware redesigns, development of new technologies, or substantial shifts in industry standards, a longer period is necessary. This timeline accommodates the complete product lifecycle, from design and development through to testing, certification, and market introduction.

An additional consideration could be to implement grace periods following the introduction of new requirements before any enforcement regime begins. This would help industry adjust and allow for the completion of products already in the development pipeline.

Consider also introducing key requirements in phases, starting with the most critical security features. This would provide immediate improvements to security while giving organisations time to adapt to more complex requirements.

Whatever approach the government ultimately adopts, providing manufacturers, especially SMEs, with resources, guidelines, and tools to meet new requirements will facilitate a smooth transition. This support might include technical guidelines, best practices, and financial incentives for early adoption as well as continued stakeholder engagement in the development of new cybersecurity requirements to work with industry to ensure that timelines are realistic and consider industry capabilities and constraints. Ultimately, it will be important to adopt a flexible and informed approach to setting timeframes for the new cybersecurity requirements, to ensure the enhancements are effective and sustainable and strike the right balance between the urgency of addressing cybersecurity risks with the practicalities of device manufacturing and deployment in real time.

7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?

The *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) is designed to provide a comprehensive framework for monitoring compliance and enforcement of regulatory requirements across various sectors and encompasses a broad range of regulatory powers, including:

- Issuing infringement notices
- Applying for civil penalty orders
- Seeking injunctions and
- Conducting investigations.

In principle this framework provides a robust basis for the monitoring, compliance, and enforcement of a mandatory cyber security standard for IoT devices. However, the effectiveness of the Act in the cyber security context would be contingent on how it is incorporated into the proposed new cybersecurity legislation and regulations that address the standards which IoT devices must meet. This might involve amendments to extant legislation as well as the introduction of new laws that explicitly address IoT cybersecurity, specifying how the Regulatory Powers Act's provisions would be applied in the new legislation contemplated under the 2023-2030 cyber security strategy.

Effective enforcement of cybersecurity standards will also necessitate coordination between the Regulatory Powers Act and sector-specific regulations to ensure a cohesive approach that addresses the unique risks and challenges of each sector.

International cooperation is another consideration. Given the global nature of IoT device manufacturing and supply chains, compliance and enforcement efforts under the Regulatory Powers Act may also need to be supported by international cooperation. For example, aligning Australian standards with international best practices and working with other countries to manage cross-border enforcement challenges.

In short, while the *Regulatory Powers Act* provides a flexible and comprehensive framework for enforcement and compliance, its suitability for enforcing a mandatory cybersecurity standard for IoT devices in Australia will depend on specific legislative measures that detail the application of its provisions to the cybersecurity domain. Additionally, the complexity of IoT ecosystems and the international dimension of cybersecurity challenges mean that effective enforcement will likely require a multifaceted approach, combining regulatory measures with industry and international cooperation.

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?

Reporting specific mandatory information is to help law enforcement conduct investigations, allow regulatory bodies to monitor and manage the impact of an incident, and supports the sharing of threat intelligence to prevent future attacks. Entities covered by the Notifiable Data Breaches (NDB) scheme under the *Privacy Act (Cth) 1988* (the Privacy Act) are required to report eligible data breaches, which can include ransomware incidents if they result in unauthorised access to, or disclosure of, personal information. Additionally, the Australian Cyber Security Centre (ACSC) encourages reporting cyber incidents to help understand the threat environment and assist other potential victims.

Where an entity has been the subject of a ransomware or cyber extortion incident, at a minimum, extant reporting provisions should apply, for example notifiable data breaches under the Privacy Act. Organisations covered by the Privacy Act are required to notify individuals and the Office of the Australian Information Commissioner (OAIC) when they suffer a data breach that is likely to result in serious harm to any individuals whose personal information is involved. If a cyber extortion incident involves unauthorised access, disclosure, or loss of personal information that could cause serious harm, it must be reported under this scheme.

For the financial sector, the Australian Prudential Regulation Authority (APRA) CPS 234 mandates that APRA-regulated entities must notify APRA of material information security incidents within specific timeframes. This includes incidents like cyber extortion, where the confidentiality, integrity, or availability of information assets is compromised.

Under the *Telecommunications Act (Cth) 1997*, telecommunications providers must notify the Australian Communications and Media Authority (ACMA) of details of certain security incidents, which could include cyber extortion attempts affecting their networks.

Under the *Security of Critical Infrastructure Act 2018* and its subsequent amendments under the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2021*, entities within critical infrastructure sectors are required to report significant cybersecurity incidents to the Australian Cyber Security Centre (ACSC). While this legislation primarily focuses on critical infrastructure, the inclusion of ransomware and cyber extortion incidents is implied under the broader category of cybersecurity threats.

Alignment of these extant legislative reporting obligations with the proposed new legislation will be key to ensuring any mandatory reporting regime captures all relevant information to enable mitigation and prevention of future incidents. Entities affected by cyber extortion should consider the impact of the ransomware incident on personal information and critical infrastructure, their obligations under financial regulation, and any sector-specific requirements to determine their reporting obligations.

Further, seeking legal advice and consulting with cybersecurity experts can provide guidance tailored to the specifics of the incident and ensure compliance with all applicable laws.

Specific information the government might like to consider making reportable under the new legislation could include:

- Details describing the nature of the ransomware or cyber extortion incident, including how it was identified, the extent of the systems, data, and services affected, and the duration.
- the type of ransomware used in the incident.
- A description of the compromised data, including whether any sensitive, personal or financial information was affected.
- Report on the impact of the incident on operations, including any disruptions to services, financial losses, and the cost of response and recovery efforts.
- A description of the steps taken to contain and mitigate the impact of the incident, for example whether certain systems were isolated, backups secured, whether cyber security experts have been engaged.
- Provide information on the recovery process, including the restoration of systems and data, and measures taken to prevent future incidents.
- Communication - Describe the process of internal notification and involvement of key stakeholders, including the decision-making process regarding the response to the ransomware demand.
- Detail communications with law enforcement, regulatory bodies, affected individuals, and other relevant parties.
- Note any reports made to law enforcement and regulatory bodies, including the timing of these reports and any reference numbers.
- Consider mentioning any specific legal or regulatory obligations that guided the reporting and response process, based on jurisdictional requirements.
- Future safeguards might include outlining any changes made to policies, procedures, and technical controls to prevent future incidents.

9. What additional mandatory information should be reported if a payment is made?

If a payment is made in response to a ransomware or cyber extortion incident, additional specific information becomes crucial for several reasons. It helps in understanding the financial impact of cybercrime, assists law enforcement in tracking and potentially recovering the funds, and contributes to broader efforts to combat the financing of cybercriminal activities. Information should be reported to comply with legal and regulatory requirements and to assist law enforcement and regulatory bodies in their efforts to track and combat such criminal activities. While the specifics can vary depending on the nature of the incident, consider whether the following additional information should be included in the report:

- Payment details including:
    - the total amount paid in response to an extortion demand.
    - the currency of payment, including if the payment was made using cryptocurrency.
    - the exact date and time the payment was made.
    - the manner of payment for example whether via electronic funds transfer, cryptocurrency or another method.

- The transaction details including, for cryptocurrency payments, the wallet addresses involved in the transaction, the transaction ID, and the blockchain on which the transaction occurred. For traditional payments, include transaction numbers and the financial institutions involved.
- The business case / rationale for making the payment, including details of any Board Minutes or other details of internal decision-making that led to the payment, including whether legal or other cyber expert advice was sought.
- The expected outcome of making the payment, such as the recovery of encrypted data or the prevention of data leakage.
- Any communication or negotiation that occurred with the attacker, including how they were contacted (email, dark web portal, etc.) and any instructions provided by the attacker.
- Any proof provided by the attacker that they had the means to decrypt the data or refrain from leaking it.
- Confirmation of reporting the payment to law enforcement and any regulatory bodies, including the timing of these reports and reference numbers of the reports.
- Details on the success of data recovery efforts if the ransom was paid in exchange for decryption keys.
- Any subsequent demands or communications from the attacker following the initial payment.
- Whether any post payment action was taken. For example, Steps taken to trace the payment and any legal actions initiated to recover the funds.
- Details concerning what, if any, additional security measures were implemented to prevent future incidents, including changes to policies on making ransom payments.

Organisations will also need to consider the implications of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* when making a payment related to ransomware or cyber extortion, as well as any obligations under the Notifiable Data Breaches (NDB) scheme or sector-specific regulatory requirements.

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?

Creating an effective ransomware reporting obligation that increases visibility into ransomware and cyber extortion threats while minimising regulatory burden requires a careful balance. The goal is to gather critical information to combat these threats effectively, support victims, and inform policy development, without overburdening entities, especially those with less capacity. In defining the approach, the new legislation should consider:

- Impact severity - Set clear thresholds for reporting based on the severity of the impact. For instance, incidents that lead to significant operational disruption, financial loss, or compromise of sensitive personal data should be reportable.
- Sector criticality - Consider the criticality of the sector to national security, public safety, or economic stability. Entities in critical infrastructure sectors might have more onerous reporting obligations due to the potential wider impact of ransomware incidents.

- Basic Incident details - Require reporting of basic details such as the date of the incident, type of ransomware, and method of attack. This information can be invaluable for threat intelligence without requiring extensive investigative capacity.
- Impact Description - A brief description of the operational, financial, and data privacy impacts, which can help assess the severity and prioritise responses.
- Response actions - Overview of actions taken in response, including whether law enforcement was contacted and if the ransom was paid. This helps understand decision-making processes and outcomes without necessitating detailed operational reports.
- Streamlined / simplified reporting mechanisms - Develop simplified reporting forms and processes, potentially through an online portal, making it easier for entities of all sizes to report incidents.
- Guidance and Support - Offer templates, guidelines, and even hotlines to support entities in complying with and completing their reporting obligations, especially useful for smaller organisations with limited cybersecurity expertise.
- Consider a phased reporting approach. Require an initial brief notification within a short timeframe (e.g., 24 - 48 hours) after identifying the incident, focusing on basic incident details and allow for a more detailed follow-up report once the entity has a better understanding of the incident and its impacts. This phased approach ensures timely intelligence collection without immediately burdening the entity.
- Offer incentives for voluntary reporting. Encourage voluntary reporting of smaller-scale incidents by offering incentives such as access to additional support, cybersecurity resources, or even potential immunity from certain regulatory penalties.
- Confidentiality guarantees - Ensure that sensitive information provided in reports is protected and that there are measures in place to prevent the disclosure of commercially sensitive information or personal data.
- Use of Anonymised Data - anonymise data when used for threat intelligence sharing or public reporting, to encourage openness while protecting entity interests.
- Actionable Intelligence Sharing - Develop mechanisms either through or facilitated by the CIRB, to share insights and threat intelligence with reporting entities and the broader community, demonstrating the value of reporting and fostering a collaborative cybersecurity ecosystem.

There is no silver bullet and reporting mechanisms only go so far. It's also crucial to regularly review and adjust obligations as the cyber threat landscape evolves and as entities become more mature in their cybersecurity practices. For increased efficacy, consider a tiered approach, aligned to severity thresholds, determined by severity, scale, and impact. For example:

- Operational disruption where an incident occurs those results in the shutdown or significant disruption of critical operational services for more than 24 hours.
- Financial loss where the threshold of loss exceeds $10,000 AUD, or a percentage of the entity's annual revenue, such as 1%. Or a data breach threshold, for incidents that compromise the personal or sensitive data of 100 individuals or more, or any breach involving particularly sensitive data (e.g., health records, financial information) regardless of the number of individuals affected.

- Critical infrastructure thresholds where any incident affecting entities within designated critical infrastructure sectors, regardless of the immediate visible impact, given the potential for broader implications on national security, economic stability, or public health and safety.
- A public interest threshold might apply for Incidents that attract significant public attention or concern, potentially undermining public confidence in digital services or the economy. These should be reported regardless of the direct financial or operational impact.
- Incidents where there is a high likelihood of significant further harm, such as further data breaches, fraud or threats of violence against individuals whose data was compromised, or widespread dissemination of malware.
- A breach of legal or regulatory obligations where any incident that results in a breach of specific legal or regulatory obligations related to cybersecurity and data protection, where the entity is required to maintain certain standards of data security.

Thresholds should be flexible enough to accommodate differences in the scale and capacity of entities, with possible variances for small and medium-sized enterprises (SMEs) versus large corporations or critical infrastructure sectors.

Authorities should periodically review and adjust thresholds to reflect evolving cybersecurity landscapes, technological advancements, and changes in societal norms and values around privacy and data security.

Clear guidelines and examples should be provided to entities on how to assess incidents against these thresholds, including case studies or hypothetical scenarios where reporting would be required.

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?

Limiting the scope of ransomware reporting obligations to larger businesses with an annual turnover of more than $10 million per year might seem like a straightforward way to reduce the regulatory burden on smaller entities. However, this approach risks overlooking the complex and interconnected nature of cyber threats and the role that businesses of all sizes play in the broader cybersecurity ecosystem. This might be a useful starting point or baseline position however the Department may wish to offer incentives for voluntary reporting as a measure to encourage smaller entities to report ransomware incidents. The Department could encourage voluntary reporting of ransomware incidents by offering incentives such as access to additional support, cybersecurity resources, or even potential immunity from certain regulatory penalties.

Further, the Department may wish to consider under what circumstances other entities with less annual turnover should also have reporting responsibilities. For example:

- Cyber security is a shared responsibility between government, businesses, organisations or institutions, and individuals and the risks are interconnected. SMEs are frequently players in larger, more complex supply chains and as such are obvious targets as they are vulnerable ‘entry points’. Limiting reporting obligations to larger organisations or excluding SMEs from the scope of ransomware reporting obligations, risks creating blind spots in relation to ransomware and other threats might persist across industries.

- Impact and risk are about more than just size or annual turnover. Certain SMEs might operate in sectors or supply chains that are critical to national infrastructure, public health or safety. The consequences of a ransomware attack on organisations in these sectors could well be disproportionate to the organisation's size or turnover making ransomware reporting essential regardless of an organisations size or annual turnover.
- Additionally, SMEs are common targets due to their size and inherent vulnerability including limited cybersecurity resources or expertise. SMEs are valuable sources of threat intelligence, as their experiences can provide insights into attacker Tactics, Techniques, and Procedures (TTPs) that affect a broader range of targets.

Ultimately, a complete picture of the ransomware threat landscape requires data analytics from organisations of all sizes, which in turn will help the government develop more effective defences, policies, and responses that benefit all Australians. Entities in sectors deemed critical infrastructure or essential services should have reporting obligations, regardless of size, due to the potential national security implications of an attack. Similarly, organisations that handle sensitive personal, financial, or health information should be subject to mandatory ransomware reporting obligations if they experience a ransomware attack, given the privacy, physical safety and fraud implications for individuals affected. Consider also basing the threshold for ransomware reporting on the severity and impact of the incident, rather than the size of the entity. For example, incidents that result in significant data breaches, financial loss, or operational disruption should trigger mandatory reporting obligations.

While it's important to minimise administrative and regulatory burdens, especially on SMEs, it is important to recognise that a nuanced approach, that takes into account the nature of the business, the sensitivity of the data handled, and the potential impact of an incident is critical to mitigating long term and unforeseen consequences of ransomware attacks. Tailoring reporting obligations with clear guidelines, support for compliance, and potentially phased or tiered reporting requirements is one approach that could ensure that the burden is manageable while still achieving enhanced, collective cybersecurity.

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?

The timeframe for reporting after experiencing a ransomware or cyber extortion attack, or after making a payment, must strike a balance between allowing the entity sufficient time to assess the incident and the need for timely information to combat the threat and mitigate further harm. The reporting timeframe and its associated impost can significantly impact the effectiveness of response efforts by the victim organization, law enforcement, regulatory bodies, and the broader cybersecurity community.

A preliminary report should be made not later than seventy two hours from detecting an incident. This initial notification need not contain detailed information but should inform regulatory bodies or designated authorities about the occurrence of the attack. This timeframe aligns with practices in other regulatory environments, such as the GDPR in Europe for data breaches, and is considered a reasonable period for entities to confirm they have been attacked and to initiate internal and external communication protocols.

Detailed Incident Reporting could take anywhere from seven days to several weeks depending on the nature and extent of the incident. After the initial report, entities should be given more time to understand the scope and impact of the incident fully. A detailed report, including the nature of the data compromised, the extent of the damage, the response actions taken, and any payments made, should typically be submitted within seven to thirty days. This period allows entities to conduct a thorough investigation, often with the assistance of cybersecurity professionals, and to start remediation efforts.

In circumstances where a ransomware payment is made, reporting should occur as soon as possible, and in any case, not later than twenty four hours following the payment. Prompt reporting of ransom payments is crucial for several reasons: it can aid in tracking the payment and potentially identifying the attackers, assist in efforts to recover the funds, and contribute to intelligence that helps prevent future attacks. Given the urgency and potential for financial recovery or tracking, this reporting should be expedited compared to other types of information.

Prompt reporting helps authorities gather and disseminate threat intelligence, coordinate responses, and warn of specific threat vectors or campaigns.

While rapid reporting is crucial, flexibility may be necessary for complex cases where the full extent of the attack is not immediately known. Regulatory guidelines should allow for amendments or updates to reports as more information becomes available. Especially for smaller entities, clear guidelines, templates, and support for reporting can help meet the mandated timeframes. Consider also cyber reporting hotlines or dedicated advisory services to assist entities in the reporting process.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

In the context of reporting ransomware or cyber extortion incidents, principles of no-fault and no-liability are designed to encourage organisations to come forward with information without the fear of punitive consequences. These principles can significantly increase the willingness of entities to report incidents, thereby enhancing the collective posture and ability to respond to cyber threats. However, the application of these principles must balance the encouragement of reporting with accountability and the protection of stakeholders.

The primary advantage is the likely increase in incident reporting. Entities may be more willing to disclose breaches if they are assured that doing so will not automatically result in regulatory penalties or legal liabilities, especially in cases where the entity is a victim of a sophisticated attack. It follows that increased reporting leads to increased knowledge of threat intelligence, which can be analysed to identify TTPs used by attackers. This information is crucial for improving defensive measures across the board. These principles can help foster a culture of cooperation between the private sector and government agencies, facilitating a more unified and effective response to cyber threats.

While no-fault and no-liability principles offer significant benefits, their application should not be absolute. Entities that fail to implement basic cybersecurity measures or show a pattern of negligence should not be fully shielded by no-fault principles. If an entity consistently ignores cybersecurity best practices or fails to rectify known vulnerabilities, the principles of no-fault and no-liability may not apply, especially when such negligence leads to significant harm. If an entity experiences repeated incidents due to the same unaddressed vulnerabilities, this might indicate a systemic issue with their cybersecurity posture. In such cases, the no-fault principle might be reconsidered to encourage better security practices. In situations where a breach involves highly sensitive data, such as personal health information or financial records, the principles might need to be more stringent. The minimum thresholds for what constitute adequate protection of such data should be high, and entities handling this data should be held to a higher standard of care. Entities should be required to disclose breaches in a timely and transparent manner to be eligible for no-fault protections. Failure to report in accordance with set timelines or attempts to hide the extent of a breach should negate these protections. Entities that are not in compliance with industry-specific cybersecurity frameworks or regulations at the time of the incident may not qualify for no-fault protections. This ensures that a basic level of cybersecurity hygiene is maintained.

The principles of no-fault and no-liability can significantly encourage the reporting of ransomware and cyber extortion incidents, providing critical data that enhances collective cybersecurity efforts. However, these principles should be applied judiciously, with exceptions for cases involving gross negligence, repeated incidents, mishandling of sensitive data, lack of transparency, and non-compliance with regulatory frameworks. Such a balanced approach ensures that while entities are encouraged to report incidents without fear of undue punishment, they are also motivated to maintain robust cybersecurity practices.

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?

Balancing the no-fault and no-liability principles with public expectations that businesses should take accountability for their cybersecurity is a nuanced challenge. It requires a multifaceted approach that encourages reporting and transparency while ensuring that businesses maintain robust cybersecurity practices. The government might consider where gaps exist in establishing clear cybersecurity standards and guidelines that organisations are expected to follow. This could include baseline security measures, industry-specific requirements, and best practices in cybersecurity hygiene and regularly updates of these standards to reflect evolving threats and technological advancements.

If implementing conditional no-fault protections when entities meet certain criteria, such as adherence to established cybersecurity frameworks, timely breach reporting, and evidence of due diligence in implementing cybersecurity measures it will be important to clearly specify circumstances under which no-fault protections would not apply.

Another approach is to introduce an incentive framework that establishes incentive programs for businesses that demonstrate excellence in cybersecurity practices, such as tax incentives, public recognition, or grants for cybersecurity enhancements or reduced premiums or other benefits for cyber insurance policies to businesses that adhere to high cybersecurity standards.

Education, support, and training will form core foundations to the success of the cyber strategy. Consider providing resources, training, and support to businesses, SMEs, to help them meet cybersecurity standards. This could include access to cybersecurity tools, advisory services, and educational materials. Black Ink Legal is a strong advocate for the facilitation of partnerships between government, industry, and academia to enhance cybersecurity knowledge sharing and innovation.

We also encourage regular cybersecurity assessments and audits for businesses, particularly those in critical sectors or handling sensitive data, to ensure compliance with cybersecurity standards. These assessments can provide useful feedback and recommendations for improvements, rather than be used solely for punitive measures.

Promoting transparency by requiring businesses to disclose cybersecurity practices and breaches in a manner that is accessible to the public, possibly through a centralised reporting platform would enhance public awareness of the importance of cybersecurity and the shared responsibility between businesses and consumers in protecting digital assets.

Fostering a collaborative environment for responding to cyber incidents, involving public-private partnerships will encourages information sharing about threats and vulnerabilities without placing undue blame on victim organisations. Support the development and use of collective defence mechanisms, such as threat intelligence sharing platforms and sector-specific cybersecurity organisations and tools.

Regularly reviewing and adapting no-fault and no-liability policies will ensure they effectively balance encouraging reporting with the need for accountability and consider feedback from businesses, cybersecurity experts, and the public to inform policy adjustments.

By adopting these strategies, the Department can engender a cyber security policy environment that both encourages the reporting of cybersecurity incidents and ensures that businesses take appropriate measures to protect against cyber threats. This balanced approach can help to maintain public trust and confidence in digital services and the broader cybersecurity ecosystem.

15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?

Any ransomware reporting obligation enforcement mechanism in Australia would need to balance the need for robust cybersecurity practices with the realities of business operations and the varying capacities of entities to comply. It should encourage compliance and improve the national cybersecurity posture without placing undue burdens on businesses, especially SMEs.

Consider graduated penalties that start with warnings for first time non-compliance and progress to fines for second and subsequent non-compliances. The fines could follow a scale aligned to severity of the reporting non-compliance, the potential or actual harm caused and the size of the entity. This approach allows for flexibility, recognising that not all instances of non-compliance are equally egregious.

An alternative to a graduated penalty approach is an incentive-based approach for timely and comprehensive reporting of ransomware incidents. These could include technical support in responding to incidents, reduced penalties for past non-compliance when proactive reporting is demonstrated, or public recognition for entities demonstrating leadership in cybersecurity practices. Additionally, it is important to recognise that not all entities have the same level of resources or expertise to comply with mandated reporting obligations. Accordingly, the government could consider implementing capacity-building programs that provide smaller entities with the tools, knowledge, and financial assistance they need to meet reporting standards. These programs could involve subsidised cybersecurity services, training programs, and guidance materials tailored to different industry sectors. Consider also establishing a centralised reporting system or portal that simplifies the submission of reports and allows for anonymous reporting to encourage participation.

Ultimately an effective enforcement mechanism for ransomware reporting in Australia would be multi-faceted, combining penalties for non-compliance with incentives for proactive engagement and support for entities to fulfil their obligations. By fostering a culture of cooperation and shared responsibility for cybersecurity, such a mechanism can contribute to a more resilient digital environment.

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?

Sharing anonymised information about ransomware incidents can significantly enhance the collective cybersecurity posture of Australian by enabling entities to learn from each other's experiences, identify emerging threats, and implement effective defence strategies. Examples include:

- Sharing TTPs used by attackers including detailed descriptions of how the ransomware was delivered and executed, including the initial access vectors (e.g., phishing emails, exploited vulnerabilities), any lateral movement within networks, and the encryption tactics used. Understanding TTPs helps organisations to tailor their defensive strategies more effectively.
- Sharing Indicators of Compromise (IoC) detailing specific technical indicators such as malicious IP addresses, URLs, file hashes, and email addresses associated with the ransomware incident. IoCs enable entities to update their security systems to detect and block similar attacks.
- Information on new or evolving ransomware strains, including any unique characteristics or behaviours that distinguish them from known variants. This helps in developing or updating antivirus signatures and other security measures.
- Mitigation strategies used to effectively alleviate the impact of attacks, including isolation of affected systems, use of backups for recovery, and communication with stakeholders. Also, any challenges encountered during the recovery process and how they were overcome.
- Impact analysis reports detailing the extent of operational disruption, data loss, financial cost, and recovery time. While specifics will vary, aggregate data can help in benchmarking and preparing for potential impacts.

Information sharing should be as broad and wide reaching as practicable and include CERT Australia, cybersecurity firms, industry-specific cybersecurity alliances, and international cybersecurity organisations, industry groups, the general public and SMEs to increase awareness and to improve Australia’s overall cyber security posture. Additionally, reports to regulatory bodies, including the proposed new CIRB, can help inform policy development, regulatory responses, and national cybersecurity strategies.

Frequency of information sharing, as a general rule, should be as often as practicable. Where threats are imminent, immediate sharing of IoCs and emerging TTPs can help entities defend in real time. In addition, regular, summarised reports of ransomware trends, including common vectors, targeted sectors, and effective defences, can help organisations stay informed and adjust their security posture accordingly. More comprehensive annual or quarterly reports that include detailed analyses of incidents, mitigation success stories, and policy recommendations can also provide valuable insights for strategic planning and cybersecurity.

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?

Defining the scope for 'prescribed cybersecurity purposes' under a limited use obligation is crucial for maintaining trust and collaboration between entities sharing cyber incident information and government agencies like the Australian Signals Directorate (ASD) and the Cyber Coordinator. It ensures that sensitive information shared in the context of cyber incidents is used appropriately, fostering a secure and cooperative cybersecurity environment. It should balance the need for effective cybersecurity actions with the protection of the rights and interests of reporting entities and individuals affected by cyber incidents, and should include:

- Threat Intelligence analysis for analysing and understanding the nature, methods, and sources of cyber threats. This includes identifying patterns, TTPs of threat actors, and contributing to the national threat intelligence picture.
- Prevention and mitigation by utilising the information for developing strategies, tools, and processes to prevent and mitigate future cyber threats. This can involve creating or refining cybersecurity best practices, advisories, and mitigation techniques to protect against identified threats.
- Providing direct support and guidance to entities that have reported cyber incidents, helping them to respond to and recover from incidents. This support can include technical advice, incident response services, and recovery planning.
- Leveraging shared information to strengthen Australia's overall cybersecurity posture.
- Sharing insights and intelligence with domestic and international cybersecurity partners, where appropriate, to collaborate on addressing common threats and challenges. This should be done while respecting confidentiality and the originator's control of the information.
- Informing cybersecurity research and development efforts aimed at advancing cybersecurity technologies, practices, and knowledge. This could include identifying emerging threats and developing innovative defensive technologies.

In defining the scope for 'prescribed cybersecurity purposes' under a limited use obligation it is also important to consider what limitations and safeguards might apply. For example, entities sharing information with ASD and the Cyber Coordinator should be informed about how their information will be used. Regular reporting on the use and outcomes of shared information can help maintain transparency.

18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

When cyber incident information is provided to entities like the ASD or the Cyber Coordinator, certain restrictions should be applied to its use or sharing to ensure the protection of sensitive information, maintain trust between public and private sectors, and comply with legal and ethical standards. For example:

- Purpose - information should only be used for defined cybersecurity purposes, such as threat analysis, prevention, mitigation, and improving national cybersecurity resilience. Any deviation from these purposes, especially for non-cybersecurity related activities, should be strictly prohibited.
- Privacy – it goes without saying that all handling of cyber incident information must comply with privacy laws and regulations, including the Australian Privacy Principles (APPs) and the Privacy Act 1988. Further, efforts should be made to anonymise or de-identify personally identifiable information unless it is essential for the defined cybersecurity purpose.
- Confidentiality - access to this information should be limited to individuals who require it for legitimate cybersecurity purposes, ensuring that it is shared on a need-to-know basis.
- Secure handling, storage and disposal – Cyber incident information should be stored and handled with high-security standards to prevent unauthorised access, disclosure, or loss and when no longer needed, should be destroyed.
- Consent - except in cases where sharing is mandated by law or is necessary for national security, the consent of the entity providing the information should be obtained before it is shared with other parties. When seeking consent, entities should be informed about the potential for their information to be shared with other domestic or international cybersecurity partners and under what conditions.
- Restrictions and Limitations - clear guidelines should govern the further dissemination of information to ensure that downstream entities respect the original use restrictions and privacy considerations. All use and sharing of cyber incident information must comply with relevant laws, policies, and international agreements to which Australia is a signatory.
- Reporting Obligations - where applicable, entities should comply with legal reporting obligations, such as those under the Notifiable Data Breaches (NDB) scheme.
- Independent oversight - a key function of the proposed CIRB, could be as an independent oversight body to monitor compliance and address grievances in relation 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?

Beyond establishing the proposed CIRB other possible strategies the government can adopt to encourage entities to share information and collaborate with the ASD and the Cyber Coordinator after a cyber incident which aim to build a robust cybersecurity ecosystem characterised by active participation, trust, and shared responsibility might include:

- Public-Private Partnerships (PPPs) - strengthen public-private partnerships focused on cybersecurity. These partnerships can facilitate regular information exchange, joint cybersecurity initiatives, and collaborative response efforts. PPPs can also provide a structured framework for leveraging private sector innovation and expertise in government cybersecurity strategies.
- Support the development or enhancement of sector-specific Information Sharing and Analysis Centres (ISACs). ISACs serve as central hubs for sharing threat intelligence, best practices, and security information within particular sectors, such as finance, healthcare, or energy. They can act as intermediaries between the government and private sector, ensuring that information sharing is relevant, timely, and actionable.
- Launch regular, national cybersecurity awareness campaigns to educate entities about the importance of cybersecurity, the benefits of sharing information, and how to collaborate effectively with government agencies. These campaigns can also highlight successful case studies of public-private collaboration to demonstrate tangible benefits.
- Offer technical assistance, including tools, services, and expertise, to entities that may lack the resources to effectively manage cyber incidents on their own. This support could range from incident response services to advisory services that help entities improve their cybersecurity posture.
- Provide regulatory flexibility for entities that actively participate in information sharing and collaborative efforts. This could include streamlined compliance processes or consideration in regulatory enforcement actions, recognising the entity’s proactive cybersecurity efforts.
- Introduce cybersecurity certification programs or labeling schemes that recognise entities for their cybersecurity practices and participation in information sharing initiatives. Such recognition can serve as a market differentiator, encouraging entities to adhere to best practices and actively engage in the cybersecurity community.
- Grant entities that actively share information and collaborate access to enhanced government services, such as priority access to cybersecurity advisories, briefings, and alerts. This privileged access can act as an incentive for entities to maintain active engagement with government cybersecurity efforts.
- Implement feedback mechanisms that allow entities to see the outcomes of their information sharing, including how their information contributed to mitigating cyber threats or enhancing national cybersecurity. This transparency can motivate continued participation and trust in government initiatives.

These strategies might enable the government to create a cooperative and integrated approach to cybersecurity, where entities are motivated and supported in their efforts to share information and collaborate in the aftermath of cyber incidents. A collaborative environment is essential for building a resilient national cybersecurity posture capable of addressing and adapting to the evolving cyber threat landscape.

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)?

The proposed CIRB should serve as a central mechanism for analysing cyber incidents, fostering a culture of continuous improvement, and enhancing national cybersecurity resilience. The purpose, scope, and operational parameters of the CIRB need to be carefully defined to ensure it effectively contributes to the national cybersecurity strategy. The CIRB should aim to be a dynamic and responsive entity, capable of adapting to the rapidly evolving cyber threat landscape to ensure it plays a pivotal role in strengthening Australia's cybersecurity framework, promoting a safer digital environment for all Australians.

The purpose could include:

- Incident Analysis - to conduct in-depth analyses of significant cyber incidents to understand the TTPs used by adversaries, the vulnerabilities exploited, and the impacts on affected entities.
- Lessons Learned - to extract actionable insights and lessons learned from cyber incidents to improve cybersecurity practices, policies, and defense mechanisms across all sectors.
- Recommendation Development - to develop tailored recommendations for both specific entities and broader industry sectors to mitigate vulnerabilities, enhance resilience, and prevent future incidents.
- Policy Guidance - to inform government cybersecurity policy, regulatory frameworks, and national cybersecurity strategies based on evolving threat landscapes and incident review findings.
- Stakeholder Collaboration - to facilitate collaboration among government agencies, private sector entities, and international partners for a unified approach to cybersecurity, enhancing the nation's ability to respond to and recover from cyber incidents.
- Public Awareness and Education - to raise public awareness about cybersecurity threats and promote cybersecurity best practices among citizens, businesses, and government entities.

The scope of the CIRB should include:

- Significant Cyber Incidents - the CIRB should focus on significant cyber incidents that have national security implications, potentially affect critical infrastructure, or could have widespread impacts on the economy, public safety, or public confidence.
- Cross-Sector Analysis - its scope should encompass incidents across all sectors, including government, critical infrastructure, finance, healthcare, and education, allowing for a comprehensive view of national cybersecurity challenges.
- Preventive and Reactive Measures - while the board's primary focus might be on reactive analysis post-incident, it should also proactively identify potential threats and vulnerabilities that could lead to significant incidents, recommending preventive measures.
- International Threat Intelligence - the scope should include the analysis of international cyber incidents and threats, leveraging insights from global incidents to bolster domestic cybersecurity posture.

- Technological and Policy Trends - the CIRB should consider emerging technological trends and evolving cyber threat tactics, ensuring that recommendations and policies remain relevant and effective against future threats.
- Legal and Regulatory Frameworks - the CIRB should review and recommend adjustments to legal and regulatory frameworks to support effective cybersecurity measures, ensuring that policies facilitate rather than hinder cybersecurity improvements.
- Stakeholder Engagement – the CIRB should engage a wide range of stakeholders, including industry leaders, cybersecurity experts, academic institutions, and international cybersecurity agencies, to ensure a diverse and comprehensive perspective on cybersecurity challenges and solutions.

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?

The CIRB is not a law enforcement body, however, it will play a crucial role in enhancing national cybersecurity. To ensure its operations do not interfere with law enforcement, national security, intelligence, and regulatory activities, a clear jurisdiction and mandate with a clearly defined scope must apply. For example, the CIRB's mandate should be clearly defined to focus on policy measures, information dissemination, and analysing and learning from cyber incidents rather than conducting law enforcement or intelligence activities. Its role in reviewing incidents should complement, not duplicate or interfere with, ongoing investigations or intelligence operations. Accordingly, where legal issues arise from a given cyber security incident, the CIRB should be able to refer these to the relevant law enforcement authorities. Further, formal mechanisms for collaboration and communication with law enforcement, national security, and regulatory bodies should be established to ensure that the CIRB's activities are coordinated and do not impede sensitive operations.

Information provided to the CIRB should be used strictly for the mandated purpose. Any use of information beyond this scope should be explicitly restricted. Establish protocols that govern how information is shared with the CIRB, ensuring that sharing does not compromise ongoing investigations, intelligence operations, or national security interests. This includes secure handling and storage of sensitive information. In addition, implement strict confidentiality measures to protect the identity of entities sharing information and the details of incidents that could impact ongoing operations. The CIRB should be able to anonymise data and findings as necessary to prevent unintended disclosures.

We would imagine that the CIRB will regularly engage with representatives from law enforcement, intelligence agencies, and regulatory bodies to understand their concerns and ensure the CIRB's activities are aligned with broader national security and public safety objectives.

We would further imagine that the CIRB will establish mechanisms through which law enforcement and intelligence agencies can provide feedback on the CIRB's operations and recommendations, ensuring that potential conflicts are identified and addressed promptly.

Conducting periodic reviews of the CIRB's operations, scope, and impact, especially in relation to its interaction with law enforcement, national security, and intelligence activities will be imperative. These reviews can help identify required adjustments to ensure alignment with national priorities and the protection of sensitive activities.

All things being equal, these limitations and safeguards would enable the CIRB to fulfil its mission to enhance national cybersecurity resilience while ensuring its activities do not interfere with critical law enforcement, national security, intelligence, and regulatory functions.

22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?

We query whether a no-fault approach when reviewing cyber incidents is the most effective approach? How would accountability be addressed and enforced under a no-fault regime? That said, adopting a 'no-fault' approach in the operation of CIRB may be essential for encouraging entities to share information freely about cyber incidents without fear of blame or reprisal. This would facilitate a more open, cooperative environment for understanding and learning from cyber incidents.

If a no-fault regime is adopted, we recommend that the CIRB establish a clear 'no-fault' mandate emphasising the CIRB's role in learning and improvement rather than attributing blame. This should be coupled with guidelines for all communications, reports, and publications to ensure adherence to the 'no-fault' principle, focusing on constructive insights rather than fault-finding.

Focus should be on systemic issues and solutions directing the CIRB's efforts towards identifying systemic vulnerabilities, trends, and challenges that contribute to cyber incidents, rather than focusing on individual failures and ensuring that findings and recommendations focus on broader improvements to cybersecurity practices, policies, and technologies, promoting resilience and prevention.

A collaborative review process that engages with entities that have experienced cyber incidents in a cooperative manner, ensuring they are part of the review process and can provide context and insights without fear of fault attribution is recommended.

We recommend providing entities with supportive, constructive feedback on how to improve their cybersecurity posture, emphasising learning and development opportunities underpinned by training and awareness for CIRB members and staff on avoiding bias and blame in their analysis and communications, reinforcing the importance of a constructive, 'no-fault' approach. This training should also address current cybersecurity best practices and challenges, enabling them to understand the complexities of cyber incidents and the factors that contribute to them.

Communicating the 'no-fault' approach clearly and consistently to all stakeholders, including entities that may report incidents, policymakers, and the public, will build trust and support for the CIRB's work. This could be coupled with established mechanisms for receiving feedback on the CIRB's work and approach, allowing for adjustments to ensure the 'no-fault' principle is effectively maintained.

The CIRB should conduct regular evaluations of its approach and methodologies to ensure the 'no-fault' principle is being effectively applied and to make adjustments as needed based on feedback and evolving cybersecurity landscapes.

By institutionalising these practices, the CIRB can foster a culture of openness and learning, encouraging entities to share information about cyber incidents freely and contributing to a more resilient cyber ecosystem.

Enforcing Accountability with a No-Fault Approach

While a no-fault approach focuses on systemic improvements rather than individual blame, accountability is still crucial for ensuring responsible behaviour and adherence to cybersecurity best practices. Accountability can be enforced within this framework through:

- Clear Standards and Expectations - establishing clear cybersecurity standards and expectations allows organisations to understand their responsibilities. Accountability is enforced through the expectation that these standards are met, not through punishment for failure.
- Transparency and Reporting - requiring entities to report on how they have addressed the vulnerabilities or issues identified in incident reviews promotes accountability. Public disclosure of these actions (while protecting sensitive information) can also encourage entities to follow through on commitments to improve.
- Incentives for Compliance - offering incentives for adhering to best practices and demonstrating improvements in cybersecurity posture can motivate entities to take accountability seriously. Conversely, entities that fail to meet established standards may be ineligible for certain incentives or benefits, such as cyber insurance advantages.
- Regulatory and Legal Frameworks while the no-fault approach prioritises learning and improvement, it operates within broader regulatory and legal frameworks that enforce accountability. These frameworks can include penalties for gross negligence, failure to comply with industry standards, or not reporting incidents as required by law.
- Risk Management and Insurance - encouraging or requiring cyber risk management practices and cyber insurance can also promote accountability. Insurance providers often require certain cybersecurity measures to be in place, indirectly enforcing accountability through market mechanisms.
- Sector-Specific Oversight - for critical infrastructure and sectors where cybersecurity breaches can have significant public safety implications, sector-specific oversight bodies can enforce accountability through regular audits, assessments, and feedback loops.

The no-fault approach, complemented by these mechanisms, can create a balanced environment where entities are motivated to improve their cybersecurity practices while being held accountable for maintaining a minimum standard of care and for their efforts to remediate identified vulnerabilities. This balanced approach ensures that the focus remains on enhancing overall cybersecurity resilience without stifling information sharing and cooperation.

23. What factors would make a cyber incident worth reviewing by a CIRB?

For a CIRB to function effectively, it must prioritise incidents that offer significant learning opportunities, have wide-ranging implications, or highlight systemic vulnerabilities. Not every cyber incident warrants an in-depth review by such a board, given the resource intensity and the need for focused insights that can lead to meaningful improvements in cybersecurity practices and policies. Some key factors that would make a cyber incident worth reviewing by a CIRB might include:

- Impact on Critical Infrastructure - incidents that affect critical infrastructure sectors (e.g., energy, transportation, healthcare, financial services) should be prioritised due to their potential to impact national security, economic stability, public health, or safety.
- Scale and Severity - the extent of the incident, including the number of entities affected, the volume of data compromised, or the severity of service disruptions. Large-scale incidents that indicate a significant breach of security measures are particularly worth reviewing.
- Novelty of the Attack Vector or Tactic - incidents involving new or sophisticated attack vectors, TTPs that have not been widely observed or understood. These incidents can provide valuable insights into emerging threat actor capabilities and motivations.
- Breach of Novel Defences - incidents where attackers successfully breach new or advanced cybersecurity defences, indicating a need for re-evaluation of current best practices and technological solutions.
- Legal and Regulatory Implications - incidents with significant legal or regulatory implications, such as those involving breaches of data protection laws, could warrant review to assess compliance issues and to inform future regulatory adjustments.
- Public Interest and Confidence - incidents that attract significant public attention or could affect public confidence in digital services, especially those involving popular consumer platforms or services.
- Cross-border or International Impact - incidents with cross-border implications, including those that affect international data flows, involve foreign threat actors, or have geopolitical ramifications, are important for understanding the international cybersecurity landscape.
- Repeated Incidents in a Sector - a series of similar incidents within a particular sector might indicate systemic vulnerabilities or sector-wide challenges that require a broader review to address effectively.
- Incidents with Unclear Attribution - complex incidents where attribution is unclear or contested may benefit from an independent review to dissect the available evidence and contribute to a clearer understanding of the incident.
- Lessons for National Cybersecurity Policy - incidents that could yield significant lessons or insights for national cybersecurity policy, strategy, or resilience efforts. These might include incidents that test the efficacy of existing cybersecurity frameworks or highlight gaps in national defences.

By focusing on incidents that meet these criteria, a CIRB can ensure that its reviews are both manageable and meaningful, contributing valuable insights to the cybersecurity community, informing policy development, and ultimately enhancing national and organisational cybersecurity postures.

24. Who should be a member of a CIRB? How should these members be appointed?

The effectiveness of a CIRB heavily depends on the expertise, diversity, and impartiality of its members. The composition of the CIRB should be carefully considered to include a wide range of perspectives and expertise relevant to cybersecurity, incident response, legal and regulatory issues, and sector-specific knowledge.

Who should be a member?

When considering the constitution of the CIRB, we recommend including industry experts (both local and international), industry representatives, government officials, legal and policy experts, representatives from academic and research sectors.

Individuals with extensive experience in cybersecurity practices, threat intelligence, and incident response including professionals bring a background in both offensive and defensive cybersecurity protection.

Executives or senior professionals from critical infrastructure sectors (e.g., energy, finance, healthcare, telecommunications) and other relevant industries will ensure that sector-specific insights and concerns are represented.

Representatives from relevant government agencies involved in cybersecurity, national security, and critical infrastructure protection ensures alignment with national security priorities and regulatory frameworks.

Individuals with expertise in cyber law, privacy, and regulatory issues will provide insights into legal implications and policy considerations of cyber incidents.

Scholars or researchers specialising in cybersecurity, technology policy, and related fields bring analytical and long-term perspectives to the discussion.

Where appropriate, international experts can provide a global perspective on cybersecurity challenges and solutions, especially for incidents with cross-border implications.

How should members be appointed?

We recommend establishing a nomination process that allows for potential candidates to be identified by their peers, industry groups, academic institutions, or government agencies. This process should aim to identify individuals who are not only experts in their field but also have a reputation for integrity and impartiality.

A selection committee comprising representatives from government, industry, and academia should peer review nominations and make recommendations on appointments. The committee should strive for balance in terms of expertise, sector representation, and diversity.

The Department might also consider a public consultation period where the list of nominated individuals is made public, allowing feedback and suggestions from the broader community. This can enhance transparency and public trust in the CIRB.

We recommend setting term limits for CIRB members of no more than 3 consecutive years to ensure fresh perspectives are regularly introduced. Staggering terms can help maintain continuity while allowing for periodic renewal of the board’s composition.

Ethical and security screening should be considered. Conducting thorough ethical and security screenings for all potential members will ensure there are no conflicts of interest and that members meet the highest standards of integrity and confidentiality.

Members should be officially appointed by a high-level authority, such as the head of the relevant national cybersecurity agency or a senior government official, to confer formal recognition and authority to the CIRB's activities.

We further recommend continuous evaluation via performance review of the CIRB. Implementing regular performance reviews of CIRB members will ensure they remain effective contributors and adhere to the board's ethical standards.

New members should be provided with comprehensive orientation and ongoing training to ensure they are fully prepared for their roles, including briefings on current cybersecurity threats, legal considerations, and review procedures.

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?

By carefully selecting members through a transparent and rigorous process, the CIRB will have confidence that it has the necessary expertise and credibility to fulfil its mission of improving national cybersecurity resilience through the thoughtful review of cyber incidents. This will ensure that the CIRB members bring a high level of proven, independent expertise to the reviews. The board's composition should encompass a broad spectrum of domains as outlined above, to ensure comprehensive analyses of cyber incidents and the development of actionable, informed recommendations. Key domains of expertise that we consider should be represented include:

- Cybersecurity and Information Security Technical Expertise to ensure a deep knowledge of cybersecurity principles, technologies, and practices, including threat detection, mitigation, and incident response should be accompanied by practical experience. Hands-on experience in managing and responding to cyber incidents, with insights into the challenges and best practices in real-world contexts.
- Cyber Law and Policy Expertise is critical to the Board's understanding of legal frameworks and policies related to cybersecurity, privacy, data protection, and digital governance. This should be coupled with regulatory compliance expertise for different sectors, understanding how legal and policy frameworks impact cybersecurity practices.
- Risk Management and Cyber Insurance expertise to ensure skills in identifying, assessing, and managing cyber risks, including the development of strategies to mitigate these risks. Knowledge of the cyber insurance market, including policy structures, coverage, and the role of insurance in managing cyber risks.
- Technical domains experts specific to Critical Infrastructure and sector-specific knowledge (e.g., energy, finance, healthcare), to bring a deep understanding of each of those sector's unique cybersecurity challenges and dependencies.
- Operational Technology (OT) Security expertise which is critical for reviewing incidents affecting critical infrastructure.
- Crisis Management and Business Continuity including the coordination of responses across different stakeholders. Knowledge of business continuity and disaster recovery planning, essential for understanding the broader impact of cyber incidents on operations.

- Digital Forensics and Incident Analysis will be crucial for investigating the technical details of cyber incidents and understanding the TTPs used by attackers. The ability to analyse incident trends and data to identify patterns, vulnerabilities, and emerging threats will assist the CIRB in meeting its purpose and scope.
- International Cybersecurity experts will bring an understanding of international cybersecurity standards, practices, and cooperation mechanisms, essential for addressing cross-border incidents and threats and allow comparative analysis. The ability to compare and contrast cybersecurity practices across different jurisdictions will assist in identifying emerging best practices and lessons learned globally.

Members should have:

- a proven track record of contributions to their field, such as publications, leadership roles in cybersecurity initiatives, or recognition by professional organizations.
- the ability to provide objective, unbiased analysis and recommendations, free from conflicts of interest or undue influence from specific entities or sectors is essential.
- a commitment to staying abreast of the latest developments in cybersecurity, will ensure that the CIRB's work is informed by the most current knowledge and trends.

The CIRB’s effectiveness hinges on the collective expertise of its members, spanning these diverse domains. This multidisciplinary approach ensures that reviews are thorough, insights are well-rounded, and recommendations are practical and forward-looking, contributing to the strengthening of national cybersecurity resilience.

26. How should the Government manage issues of personnel security and conflicts of interest?

The government has excellent processes in place for managing issues of personal security and conflicts of interest for example, through the AGSVA. This, together with the measures outlined below will ensure that sensitive information is handled securely, and that the board's decisions and recommendations are unbiased and in the public interest:

- Security Clearances - require all CIRB members and associated staff to undergo thorough security clearance processes appropriate to the level of classified or sensitive information they will access. This ensures that individuals have been vetted for trustworthiness and reliability.
- Regular Security Training - provide regular security awareness and protocol training, emphasizing the handling of classified and sensitive information, cybersecurity best practices, and the potential risks of insider threats.
- Secure Communication Channels - ensure that all communications, especially those involving sensitive or classified information, occur over secure, encrypted channels to prevent unauthorised access or eavesdropping.
- Access Controls- implement strict access controls to sensitive information, ensuring that CIRB members and staff can only access information relevant to their specific roles and current reviews. Use of the principle of least privilege can minimise potential security risks.

- Continuous Monitoring - employ continuous monitoring strategies for personnel and their activities related to sensitive information, including regular reviews of access logs and behaviour analysis to detect potential security concerns early.
- Declaration of Interests - require all potential and current CIRB members to declare any personal or professional interests including financial interests, affiliations with entities that may be subject to review, or personal relationships that could affect impartiality.
- Conflict of Interest Policies - develop and enforce robust conflict of interest policies that clearly outline what constitutes a conflict, the process for declaring conflicts, and the steps to be taken when a conflict is identified. These policies should also detail sanctions for non-compliance.
- Regular Updates - mandate regular updates to declarations of interest to capture any changes in CIRB members' circumstances that might introduce new conflicts of interest.
- Recusal Procedures - establish and enforce clear procedures for the recusal of board members from reviews or decisions where they have a declared conflict of interest. Ensure that these procedures are transparent and documented.
- Public Disclosure - consider the public disclosure of CIRB members' declared interests in a manner that balances transparency with privacy considerations. This can help build public trust in the board's integrity.
- Ethics Training – provide annual ethics training to CIRB members and staff, focusing on identifying and managing conflicts of interest, ethical decision-making, and the importance of transparency and integrity in their roles.
- Independent Oversight - implement mechanisms for independent oversight of conflict-of-interest declarations and management, possibly involving an external ethics committee or auditor. This can provide an additional layer of scrutiny and assurance.

By addressing personnel security and conflicts of interest through these comprehensive measures, the government can ensure that the CIRB operates securely and maintains the highest standards of integrity and impartiality. This is essential for the board to effectively fulfil its mission and maintain public confidence in its work.

27. Who should chair a CIRB?

Choosing the right chair for the CIRB is foundational to the board's success, impacting its effectiveness, the quality of its deliberations and outputs, and its overall contribution to improving national cybersecurity resilience. The chair plays a pivotal role in guiding the board's activities, ensuring effective leadership, and maintaining the board's credibility and authority. The chair should ideally have significant cybersecurity credentials, including a deep understanding of trends and best practices. This expertise will be vital in leading discussions and understanding the more technical aspects of cyber incidents in guiding the Board's recommendations. Ideally the chair or the secretary should have experience in crisis management, noting that the CIRB will deal with incidents that could have significant impact on national security, businesses and the economy. This will help to support the board effectively navigate complex situations and provide actionable guidance. Familiarity with the policy and regulatory landscape related to cybersecurity and critical infrastructure is important. The chair should have an appreciation of the implications of the board's work in policy development. Experience in governance roles might be beneficial, whether in public institutions, private sector organisations, or non-profits.

The chair must be adept at managing diverse stakeholders, facilitating constructive discussions, and driving consensus among board members. Importantly, the chair should be a person of high integrity with a strong professional reputation. This helps in establishing trust with stakeholders and enhances the board's credibility. The ability to articulate the board's findings and recommendations clearly and persuasively will be vital to the CIRB’s effectiveness.

Most importantly, the chair should be independent, without conflicts of interest that could undermine the board's impartiality and objectivity. Proper consideration should be given to ensuring diversity in selecting the chairperson, including professional background, sector experience, and demographic characteristics, to reflect the wide range of stakeholders affected by cybersecurity issues. For example, the National Cyber Security Coordinator, Michelle McGuinness or the E-safety Commissioner, Julie Inman-Grant.

28. Who should be responsible for initiating reviews to be undertaken by a CIRB?

The initiation of reviews by a CIRB is a critical process that determines which cyber incidents are scrutinised for lessons that can improve national cybersecurity resilience. To ensure that the CIRB focuses on the most significant and instructive incidents, the responsibility for initiating reviews should be strategically assigned. There are many ways this can be achieved. Consideration should be given to a multi-channelled approach to reflect that incidents are going to emanate out of different sectors in society.

Government agencies, such as the ASD, the Cyber Security Centre, or equivalent organisations could have the authority to initiate reviews. Given their comprehensive awareness of the national cybersecurity landscape, these agencies are well-positioned to identify incidents that warrant a deeper examination by the CIRB. However, not all incidents may be brought to the attention of these agencies, so it may be more appropriate for the National Security Advisor, who oversees the strategic integration of the nation's cybersecurity efforts, to initiate reviews. Their broad perspective on security and policy implications makes them well suited to recognise incidents with significant lessons or policy ramifications. Additionally, sector specific regulatory agencies overseeing critical infrastructure sectors (e.g., energy, finance, telecommunications) might initiate reviews for incidents within their domain. Their sector-specific knowledge enables them to identify incidents that could highlight systemic vulnerabilities or regulatory gaps.

The Chair of the CIRB, in consultation with board members, could have the authority to initiate reviews. This allows the board to act on its insights and concerns about emerging threats or patterns of incidents that it identifies as particularly instructive or alarming.

Legislative bodies or dedicated parliamentary committees focused on cybersecurity, national security, or critical infrastructure protection could request reviews. This would ensure that the CIRB's work remains aligned with legislative priorities and oversight.

A formal process could be established for industry, especially those within critical infrastructure sectors, to request reviews of significant incidents. This encourages collaboration and ensures that the CIRB addresses concerns from the frontline of cyber defence.

Mechanisms for triggering or initiating reviews could include:

- Criteria-Based Triggering - established by clear criteria for what constitutes a reviewable incident, ensuring consistency and focus in the CIRB's work. Criteria might include the scale of impact, novelty of the attack, or involvement of critical infrastructure.
- Review Request Portal - a secure portal where authorised entities can submit requests for incident reviews, provide relevant information and justification for the review.
- Periodic Assessment Meetings - the CIRB could hold regular meetings to assess the current threat landscape and identify incidents that merit review based on emerging trends, threat intelligence, and stakeholder input.

Ensuring the process for initiating reviews incorporates input from a diverse range of stakeholders, balancing national security concerns with the interests of private sector entities and the public will result in a more equitable approach. As well as ensuring transparency about the process for initiating reviews, including the criteria and rationale for selecting specific incidents, to build trust and accountability.

By establishing a multi-faceted approach, the CIRB can ensure that its work is timely, relevant, and responsive to the evolving cybersecurity landscape, thereby contributing effectively to national resilience efforts.

29. What powers should a CIRB be given to effectively perform its functions?

For a CIRB to effectively perform its functions within an Australian context, it would require a set of clearly defined powers, backed by legislative or regulatory support. These powers should enable the CIRB to gather necessary information, conduct thorough analyses, and make recommendations that can lead to tangible improvements in national cybersecurity resilience. Careful consideration must be given to balancing the CIRB’s powers with the need to protect individual and corporate privacy, as well as to ensure its actions do not inadvertently harm national interests or international relations. We consider several powers that essential to the effective functioning of a CIRB in Australia including:

- **Authority to Initiate Reviews:** the CIRB should have the authority to independently decide which cyber incidents to review based on established criteria, such as the impact on national security, economic stability, or public safety.
- **Investigative Powers**: The CIRB should have the authority to initiate and conduct investigations into significant cyber incidents. This includes the power to:
  - Collect evidence from relevant entities, both public and private.
  - Compel the production of documents and testimony from individuals and organizations involved in or affected by cyber incidents.
  - Access relevant cyber infrastructure with appropriate safeguards to protect privacy and sensitive information.
- **Subpoena Power:** To gather necessary information, the CIRB should have subpoena powers to require attendance for testimony or the production of documents relevant to any investigation.
- **Recommendation Authority:** The board should have the power to issue recommendations to both the public and private sectors to improve cybersecurity practices and policies. While not

necessarily binding, these recommendations should carry weight and be considered seriously by stakeholders.

- **Coordination with Other Agencies:** The CIRB should have the authority to work closely with other government agencies, such as the Australian Cyber Security Centre (ACSC), to share information and coordinate responses to cyber threats.
- **Public Awareness and Education:** The board should have the authority to publish reports and findings (while respecting confidentiality and security concerns) to raise public awareness about cyber threats and promote cybersecurity best practices.
- **Policy Development Role:** Empower the CIRB to participate in the development and review of national cybersecurity policies and strategies.
- **Funding and Resources:** Legislation should provide the CIRB with adequate funding and resources to perform its functions effectively. This includes staffing, technology, and access to expert advice.
- **International Cooperation:** Authorize the board to engage in international cooperation and information sharing to combat global cyber threats, consistent with Australia's international commitments and privacy laws.

By equipping the CIRB with these powers, Australia can enhance its ability to respond to and mitigate cyber threats, foster a culture of continuous improvement in cybersecurity practices, and protect national interests in the digital age.

30. To what extent should the CIRB be covered by a ‘limited use obligation’, similar to that proposed for ASD and the Cyber Coordinator?

The CIRB should indeed be covered by a 'limited use obligation' to ensure that sensitive information is protected and used appropriately, fostering a culture of openness and cooperation in incident reporting and response. This obligation balances the need for operational effectiveness of the CIRB with the rights and expectations of reporting entities, ultimately contributing to a more secure and resilient cyber environment in Australia.

Implementing a 'limited use obligation' for the CIRB is crucial in establishing trust and cooperation between the CIRB, entities reporting cyber incidents, and other stakeholders. This obligation would ensure that information shared with or by the CIRB is used exclusively for predefined, cybersecurity-related purposes, thereby protecting the interests of reporting entities and maintaining the integrity of sensitive information. We outline below an analysis of the extent to which the CIRB should be covered by such an obligation:

Purpose and Scope of the Limited Use Obligation

Cybersecurity Focus - information obtained by the CIRB should be used solely for enhancing cybersecurity awareness, preparedness, response, and resilience within Australia. This includes analysing trends, identifying systemic vulnerabilities, and recommending improvements. Consider also whether the CIRB might be permitted to share certain information with international partners to increase overall global cyber security posture.

This obligation should explicitly prohibit the use of shared information for purposes outside of the CIRB's mandate, such as for taking legal action against the reporting entities or for competitive advantage.

It should ensure that all shared information, especially that which could identify specific vulnerabilities or sensitive operational details of reporting entities, is kept confidential and protected from unauthorized disclosure.

Extent of the Obligation

The CIRB should be allowed to use the information to analyse cyber incidents comprehensively and to compile reports on trends, lessons learned, and recommendations for improving national cybersecurity postures. However, the details in these reports should be sufficiently anonymised to prevent the identification of specific entities or individuals, unless such disclosure is necessary and/or with the explicit consent of the entity involved.

Information should be used to inform the development of national cybersecurity policies, strategies, and regulatory frameworks. The CIRB's insights could be invaluable in shaping effective and responsive cybersecurity governance.

The CIRB might need to share specific information with government bodies, agencies, or international partners engaged in cybersecurity defence. Such sharing should be governed by strict protocols to ensure that the receiving parties adhere to similar limited use obligations.

The CIRB should use the information to engage with and educate stakeholders about emerging cyber threats and effective defence strategies. This includes conducting briefings, workshops, and awareness campaigns, where information is used to illustrate real-world challenges and best practices.

Safeguards and Accountability

The limited use obligation should be enshrined in legal or regulatory frameworks that provide clear definitions, scope, and enforcement mechanisms, ensuring that the obligations are binding and enforceable.

Implementing oversight mechanisms to regularly review the CIRB's adherence to the limited use obligation can help ensure compliance and address any concerns or breaches of the obligation.

While maintaining the confidentiality of sensitive information, the CIRB should operate transparently, providing stakeholders with insights into its operations, methodologies, and use of information to foster trust and accountability.

31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?

Enforcement mechanisms for failure to comply with the information gathering powers of the CIRB should be carefully designed to encourage cooperation and compliance while respecting the rights and concerns of entities involved. These mechanisms must balance the need for effective cybersecurity oversight with the potential burden on business, especially considering the sensitive nature of cyber incident information. Potential enforcement mechanisms might include:

Graduated Response System

A graduated response system for non-compliance, could start with informal resolutions such as reminders and consultations. This approach affords organisations a chance to comply before facing more severe consequences, acknowledging that non-compliance might sometimes result from misunderstandings or capacity issues.

Formal Notices and Orders

Issue of formal notices requiring compliance within a specified timeframe, followed by binding orders if initial notices are ignored. These documents should clearly state the nature of the non-compliance, the information required, and the timeframe for compliance, providing a clear legal basis for the requirement.

Fines and Penalties

A system of fines and penalties for continued non-compliance, scaled according to the severity of the non-compliance and the entity's size would ensure that penalties are both a deterrent and fair. The imposition of fines should be subject to review and appeal to ensure continuing fairness and accuracy.

Reputational Incentives

Use of reputational incentives, highlighting compliance in public reports or offering recognition for entities that consistently cooperate with the CIRB could supplement the above mechanisms. Conversely, public disclosure of non-compliance could serve as a reputational deterrent for entities considering withholding information.

Referral to Regulatory or Legal Authorities

For serious cases of non-compliance, we consider that the CIRB should be able to refer the matter to relevant regulatory or legal authorities who have broader enforcement powers. This could include industry-specific regulators or the courts. Referral should be considered a last resort and used in cases where non-compliance poses a significant risk to national cybersecurity.

The above mechanisms should be underpinned by support and assistance to entities that may struggle to comply due to resource or knowledge constraints. This can include providing templates, guidance documents, or direct assistance. Supporting compliance in this way can reduce instances of non-compliance due to capacity issues.

A clear process for review and appeals should be established to ensure recourse if an organisation believes enforcement actions are unjust or based on misunderstandings.

Any enforcement mechanism should be clearly defined within the legal or regulatory framework establishing the CIRB's powers. This includes specifying the limits of the CIRB's powers, due process for enforcement actions, and the protections for organisation's rights and confidential information.

In designing these enforcement mechanisms, it is crucial to ensure that they are applied fairly, consistently, and with due regard for the principle of minimising harm. This approach will help maintain the cooperative and collaborative spirit that is essential for effective cybersecurity governance.

32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?

For a CIRB to remain impartial and credible its design must incorporate transparency, accountability, and fairness. These are essential design features, critical in ensuring that the CIRB can conduct thorough, unbiased reviews of cyber incidents and contribute meaningful improvements to cybersecurity practices.

The CIRB must have a clearly defined mandate and scope, detailing its responsibilities, the types of incidents it will review, and its limitations. This is essential to prevent mission creep and ensure the CIRB remains focused on its core objectives.

It's also important that the CIRB is comprised of members with a diverse range of expertise and backgrounds (see our response against questions 24 and 25). Diversity among the CIRB members will mitigate bias and promote a comprehensive understanding of issues affecting all sectors of society, from government, private enterprise and individuals.

The CIRB should be established as an independent entity, within the cyber strategy framework but with independent, arm's length operational autonomy. The CIRB's funding, oversight, and reporting structures should support its ability to function independently from undue influence by government, industry, or individual stakeholder interests.

Publicly available Terms of Reference for the CIRB should include transparent processes and procedures for conducting reviews, including how incidents are selected for review, how information is gathered and analysed, and how findings and recommendations are developed and disseminated. These Terms of Reference should also detail the CIRB's own approach to confidentiality, data protection and handling of classified or proprietary information. Ensuring the security of data and confidential information shared with the CIRB is essential for maintaining public trust. Strict confidentiality and data protection measures need to be implemented to safeguard sensitive information obtained during reviews.

The Terms of Reference should also include mechanisms for holding the CIRB accountable for its actions and decisions, for example, this could be through parliamentary oversight as well as providing avenues for review or appeal of the CIRB's findings or recommendations by affected entities.

Establishing mechanisms for feedback and consultation with stakeholders to inform the CIRB's work, and recommendations will further ensure that the CIRB remains impartial and maintains credibility.

By incorporating these design features, the CIRB can establish itself as a trusted, impartial entity capable of making significant contributions to improving national cybersecurity through thoughtful review of cyber incidents.

33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

The CIRB should apply above the minimum standards of protection it expects of Australian businesses. The follow, non-exhaustive list of design features would ensure a CIRB can maintain the integrity of and protection over sensitive information.

- Develop and implement stringent data handling protocols that outline procedures for collecting, storing, processing, and disposing of sensitive information. These protocols should comply with national data protection laws and international best practices. Adopt a data minimisation approach, ensuring that only the necessary amount of sensitive information is collected and retained for the specific purposes of the CIRB's reviews.
- Use strong encryption for storing and transmitting sensitive data to protect against unauthorised access and breaches.
- Implement strict access controls, ensuring that only authorised personnel with a legitimate need can access sensitive information. This includes using multi-factor authentication, role-based access controls, and logging and monitoring access to sensitive data.
- Establish secure, encrypted communication channels for receiving incident reports and sharing information with stakeholders.
- Require all CIRB members and staff to sign confidentiality agreements that legally bind them to protect any sensitive information they access as part of their duties. Regularly remind and train members on their confidentiality obligations.
- Where possible, anonymise or pseudonymise sensitive information to reduce the risk of identifying individuals or organisations from data processed by the CIRB. Ensure that such techniques are applied in a way that the data's utility for review purposes is not significantly compromised.
- Develop a comprehensive incident response plan specifically for data breaches or unauthorised access to the sensitive information the CIRB holds. This plan should include procedures for containment, assessment, notification, and remediation, as well as communication strategies for stakeholders.
- Conduct regular security audits and vulnerability assessments of the CIRB’s information systems and processes to identify and mitigate potential risks to sensitive data. This should include both internal and external audits by reputable cybersecurity firms.
- Provide ongoing training and awareness programs for CIRB members and staff on the importance of data protection, recognising and responding to security incidents, and adhering to data handling protocols.
- Ensure that all activities related to the handling of sensitive information are in full compliance with relevant legal and regulatory frameworks, including privacy laws and regulations specific to the sectors from which the data originates.
- If third-party vendors are used for processing or storing sensitive information, conduct thorough security assessments of these vendors and establish contractual obligations that require them to adhere to the same high standards of data protection.

These design features establish a robust framework for maintaining the integrity of and protection over sensitive information, enabling the CIRB to fulfil its mandate while ensuring the confidentiality and security of the data it handles.

Response to Part 2 – Amendments to the SOCI Act

Note: Black Ink Legal is not directly subject to the provisions of the *The Security of Critical Infrastructure Act 2018* (SOCI Act). However, we represent clients who may find the provisions of the SOCI Act apply to their business. Accordingly, we offer our views and recommendations on those questions in this Part 2 – Amendments to the SOCI Act most applicable to our client base. Where the question does not apply, we have not provided a response. However for ease of reference we have kept the numbering consistent with the numbering in the Consultation Paper.

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?

Black Ink Legal is a virtual law firm with minimal critical infrastructure and while our core business is not directly connected to the provision of essential infrastructure, we nevertheless take managing our firm's cyber security very seriously. Measures we take to protect our network and systems include:

- All corporate laptops have managed antivirus and ransomware monitoring;
- Windows updates and 3rd party patching are regularly applied;
- Multi-Factor Authentication (MFA) is enforced for users accessing Microsoft 365 services including Sharepoint.

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?

The SOCI Act aims to protect critical infrastructure from threats, including cyber threats, by establishing a regulatory framework for entities operating within key sectors. However, it currently doesn't explicitly detail measures applicable to data storage systems. Proposed amendments could mandate the development and implementation of risk management programs tailored to the specific risks associated with data storage systems. These programs could require entities to identify, assess, and mitigate risks, including cyber threats, physical security threats, and insider threats. In addition, they could require critical infrastructure entities to ensure that their supply chain partners adhere to certain security standards, particularly those providing data storage solutions. This could involve conducting security assessments of third-party vendors and requiring them to meet established cybersecurity standards and the timely reporting of significant cyber incidents affecting data storage systems. This ensures that relevant authorities are informed and can assist in coordinating a response, if necessary, while also contributing to a broader understanding of the threat landscape.

A further recommendation is to establish enhanced cybersecurity standards for data storage systems, including encryption requirements, access controls, and regular security assessments. These standards should be developed in consultation with industry experts to ensure they are effective. By taking these recommendations into account, the government can enhance the protection of data storage systems within Australia's critical infrastructure, mitigating risks that could have significant national security, economic, or public safety implications. Simultaneously, by incorporating measures to balance the regulatory burden, the amendments can ensure that critical infrastructure entities are able to comply effectively without undue strain on their operations.

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?

The proposed amendments to the SOCI Act, particularly those focusing on enhancing the protection of data storage systems within critical infrastructure sectors, will have both financial and non-financial impacts on affected entities. Additionally, these amendments may influence how data is utilised for business purposes. Understanding these impacts is essential for balancing security needs with operational and economic realities.

Financial Impacts can be measured as compliance costs, operational costs, costs associated with training and insurance related costs. Specifically, organisations may incur significant costs related to upgrading their data storage and cybersecurity systems to meet new standards. This includes investments in technology, software, and infrastructure to ensure compliance with enhanced cybersecurity requirements. The need for ongoing risk assessments, security audits, incident reporting, and supply chain management could lead to increased operational costs. Entities may need to hire additional staff or engage external consultants to manage these requirements. Investing in employee training and awareness programs to ensure staff understand and can effectively implement the new security measures will also have a financial impact. Entities that demonstrate compliance with the SOCI Act's heightened standards may benefit from reduced cyber insurance premiums over time, as insurers recognise the lower risk profile of compliant organisations.

Non-financial impacts include reputational benefits. For example, an organisation’s compliance with stringent cybersecurity standards can enhance their reputation and credibility, fostering trust among customers, partners, and regulators, which in turn could lead to competitive advantages in the market. The proposed amendments will lead to strengthened cybersecurity defences, reducing the likelihood and impact of cyber incidents and will enhance the overall resilience of critical infrastructure sectors. By extending security requirements to supply chain partners, entities can benefit from a more secure and reliable supply chain, reducing the risks associated with third-party vendors and service providers. Another non-financial impact is enhanced regulatory alignment, which could facilitate compliance with similar regulations in other jurisdictions, streamlining regulatory compliance efforts. By extending security requirements to supply chain partners, organisations can benefit from a more secure and reliable supply chain, reducing the risks associated with third-party vendors and service providers.

While the proposed SOCI Act amendments aim to secure data, they also necessitate the implementation of robust data governance frameworks to support robust, data-driven decision-making, ensuring that data is accurate, available, and secure. Enhanced security measures, particularly those involving encryption and access controls, could impact the ease of access to and the speed of processing data for legitimate business purposes. Organisations will need to balance security with accessibility to ensure operational efficiency and effectiveness. To mitigate potential negative impacts, organisations should adopt a strategic approach to compliance, leveraging technology and processes that enhance security without unduly hindering operational capabilities. Engaging in dialogue with regulators to clarify expectations and seek flexibility where necessary can help ensure that the amendments support, rather than inhibit, the effective use of data for business purposes.

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

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?

The introduction of consequence management powers within the context of the SOCI Act in Australia necessitates careful consideration of existing legislation and policy frameworks not just at the federal but at state and territory levels. For example, State and territory Emergency Management, Critical Infrastructure and Public Health Legislation may intersect with the SOCI Act's proposed consequence management powers, particularly those related to emergency management, public safety, and public health.

39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

Key principles, safeguards and oversight mechanisms in the establishment of consequence management powers within Australia's national security and critical infrastructure protection framework include:

- Necessity and Proportionality - actions taken under consequence management powers should be necessary for the protection of national security and the public interest, and proportional to the threat or incident being addressed.
- Transparency and Accountability - these powers should be subject to transparent processes and decision-making, with clear accountability for actions taken.
- Privacy - safeguarding privacy and personal data must be a priority principle, with measures taken to minimise impact on individual rights.
- Rule of Law - all actions must comply with the rule of law, including adherence to existing legal frameworks and international obligations.
- Collaboration and Stakeholder Engagement - efforts should involve close coordination with relevant stakeholders, including state and territory governments, industry partners, and international allies, to ensure a unified and effective response.

Safeguarding these principles would be robust judicial oversight, within a clear legislative framework, data protection measures and provisions for the regular review of the powers and their use, including sunset clauses that require legislative renewal. For example, to prevent the indefinite or inappropriate extension of extraordinary powers. Establishing an independent review body (potentially the CIRB or an off shoot of the CIRB) to monitor and evaluate the use of these powers, investigating complaints and recommending improvements.

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?

Improving the information sharing regime under the SOCI Act is essential for enhancing Australia's ability to mitigate the effects of cyber threats and other security risks. Effective information sharing can facilitate timely and coordinated responses, enabling both the public and private sectors to better protect critical assets. Our suggestions for improving the current information sharing regime under the SOCI Act include:

- Streamlining information sharing tools and mechanisms through the implementation of automated tools and systems that facilitate the real-time exchange of threat intelligence and incident data, reducing delays in information sharing. This could take the form of a government centralised, secure platform for information sharing that allows for real-time alerts, threat intelligence feeds, and secure communication channels between government agencies and critical infrastructure entities.
- In certain circumstances, expanded legal protections against liability for sharing information in accordance with the SOCI Act, could be provided to entities to encourage more open and timely sharing of threat data.
- Consider broadening the definitions of critical infrastructure and relevant information to ensure comprehensive coverage of all sectors and types of data that are essential for security. To keep pace with evolving technology and threats, this could mean including additional sectors to the definition of critical to national security.
- Additional incentives could involve strengthening public-private partnerships to foster a collaborative environment where proactive information sharing is part of the collective effort to protect critical infrastructure, with recognition programs, access to additional government resources, or regulatory benefits.
- Implement mechanisms to provide feedback to entities that share information on how their data contributes to national security efforts, enhancing the value proposition of participation. Conduct frequent awareness campaigns highlighting the importance of information sharing for national security and the benefits for participating organisations.

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?

Moving towards a 'harm-based' threshold for information disclosure represents a significant shift in how decisions about information sharing are made, particularly in the context of critical infrastructure and cybersecurity. This approach requires entities to evaluate the potential harm that could arise from not disclosing certain information, rather than simply adhering to predefined criteria or categories of information that must be disclosed.

This approach would require organisation leaders to have a deeper understanding of the vulnerabilities, threat landscapes, and potential impact on stakeholders, necessitating more sophisticated risk analysis capabilities to enable a harm-based threshold assessment to take place. In addition, organisations would need to closely monitor legal and regulatory frameworks to ensure their decisions align with current requirements regarding harm and disclosure. This might involve additional legal consultations to interpret harm thresholds in the context of specific incidents.

This has the potential to impact decision making at the enterprise level as harm-based thresholds provide entities with greater discretion in determining whether to disclose information. While this flexibility can be beneficial, it also places a greater burden on entities to make judicious decisions based on the potential for harm. It also risks organisations deliberately choosing not to share information for reputational or other economic / business related reasons.

Assessing potential harm can be highly subjective and may vary significantly between entities, sectors, and even within organisations. This variability could lead to inconsistent disclosure practices, potentially impacting the overall efficacy of information sharing for cybersecurity purposes. Entities may face an increased burden in making disclosure decisions, as they must now consider the nuanced potential for harm, which requires detailed analysis and potentially complex judgment calls. There is a risk that entities, erring on the side of caution regarding privacy concerns or fearing reputational damage, might choose not to disclose information unless the potential for harm is unequivocally clear, leading to underreporting of significant incidents.

That said, a harm-based approach allows entities to adapt more dynamically to evolving threats and vulnerabilities, as the decision to disclose is based on the current context and understanding of potential harm rather than static criteria. Overall, a move towards a harm-based threshold for information disclosure emphasises the importance of context, risk assessment, and the potential impact on stakeholders in decision-making processes. While it offers flexibility and the potential for more meaningful information sharing, it also requires entities to enhance their analytical capabilities and carefully navigate the challenges of subjectivity and variability in assessing cyber risks.

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

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?

The most relevant security standards for developing an RMP include:

ISO/IEC 27001:2013 - Information Security Management

Provides a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It helps organisations assess and treat information security risks tailored to their needs.

NIST Cybersecurity Framework (CSF)

Developed by the National Institute of Standards and Technology (NIST), the CSF offers a comprehensive approach to managing cybersecurity risk, encompassing five key functions: Identify, Protect, Detect, Respond, and Recover. It's widely applicable across sectors and organisational sizes.

CIS Controls

The Centre for Internet Security Critical Security Controls (CIS Controls) outlines a prioritized set of actions to protect organisations and data from known cyber-attack vectors. It focuses on practical, actionable steps that can significantly reduce risk.

ISO/IEC 27005:2018 - Information Security Risk Management

Provides guidelines for information security risk management in an organisation, complementing the broader ISO/IEC 27001 standard. It offers a systematic approach to risk assessment and risk treatment.

NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations

Provides a comprehensive set of security and privacy controls for federal organisations and systems. While U.S. federal-centric, its principles are broadly applicable and provide detailed measures for mitigating a wide range of cyber risks.

NIST SP 800-30 - Guide for Conducting Risk Assessments

Offers guidance on conducting risk assessments, including preparing for the assessment, conducting the assessment, communicating the results, and maintaining the assessment. It helps organisations understand their vulnerabilities, threat sources, and the potential impacts of cyber incidents.

Australian Government Information Security Manual (ISM)

For organisations in Australia, the ISM issued by the Australian Cyber Security Centre (ACSC) provides a framework for choosing effective security controls for information systems and managing risk. It's particularly relevant for government entities and contractors.

GDPR (General Data Protection Regulation)

While not a cybersecurity standard per se, the GDPR imposes significant security requirements regarding the protection of personal data for organizations operating in or dealing with individuals in the European Union. It emphasizes the importance of risk assessment and mitigation in the context of data privacy.

Considerations for Adopting Security Standards in an RMP

Contextual Relevance - choose standards that align with your organization’s industry, regulatory environment, and specific risk profile.

Integration - an effective RMP should integrate elements from various standards to cover all aspects of cybersecurity risk comprehensively.

Adaptability - be prepared to adapt the guidelines and controls specified in these standards to fit the unique needs and circumstances of your organization.

Continuous Improvement - security standards evolve, and so do cyber threats. Regularly review and update your RMP in line with the latest standards and threat intelligence.

By leveraging these security standards, organizations can develop a robust RMP that not only addresses current cybersecurity challenges but also is adaptable to future changes in the cyber threat landscape.

44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?

In Australia, the development of a Risk Management Plan (RMP) for cybersecurity within critical infrastructure and other sectors is influenced by a range of legislative requirements and guidelines at the Commonwealth, state, and territory levels. These requirements often serve complementary roles but can also introduce specific obligations that need to be harmonised within an RMP. Understanding how these various requirements interact is crucial for ensuring comprehensive and compliant risk management practices.

Commonwealth Requirements

Security of Critical Infrastructure (SOCI) Act 2018 - this Act and its amendments introduce obligations for entities in critical sectors to report on security risks and incidents. It emphasises the need for RMPs to address risks that could affect Australia's national security.

Privacy Act 1988 (Cth) - for organisations handling personal information, the Australian Privacy Principles (APPs) outline requirements for managing privacy risks in RMPs, including obligations for security of personal information.

Australian Cyber Security Centre (ACSC) Guidance - provides frameworks and guidelines, such as the Essential Eight mitigation strategies, which organisations can incorporate into their RMPs to address cybersecurity risks effectively.

State and Territory Requirements

While Commonwealth laws provide a broad framework for cybersecurity and risk management, state and territory legislation and guidelines can introduce additional requirements, particularly in sectors like healthcare, education, and utilities, which may be regulated at the state level. Examples include:

State-Based Privacy Laws - states like Victoria and New South Wales have their own privacy laws and principles that apply to state government agencies, necessitating specific privacy risk management measures in RMPs.

Emergency Services Legislation - states and territories have legislation governing emergency management, which may require critical infrastructure providers to prepare RMPs that align with state emergency management frameworks.

Health Records Legislation - states such as Victoria (*Health Records Act 2001*) and New South Wales (*Health Records and Information Privacy Act 2002*) have specific laws governing the management of health records, impacting RMPs in the healthcare sector.

Interaction and Harmonisation

In many cases, Commonwealth and state/territory requirements can complement each other, providing a layered approach to risk management. For example, Commonwealth cybersecurity guidelines can be integrated with state-specific privacy protections to create a comprehensive RMP.

Organisations operating across multiple jurisdictions may face challenges in harmonising different requirements. It’s crucial to identify and address any conflicting obligations, possibly by adhering to the most stringent standards or seeking exemptions where appropriate.

Certain sectors may be subject to additional regulations at both the Commonwealth and state/territory levels, necessitating sector-specific approaches within RMPs to ensure compliance across all relevant frameworks.

Best practice suggests conducting a thorough assessment of all applicable Commonwealth, state, and territory requirements relevant to your organisation’s operations. Engaging with legal experts, regulatory bodies, and industry groups to understand the nuances of applicable requirements and best practices for compliance is recommended but costly and time consuming.

Regularly reviewing and updating RMPs to reflect changes in the legal and regulatory landscape, ensuring ongoing compliance and effective risk management is required to ensure ongoing harmonisation.

By considering the interaction between Commonwealth, state, and territory requirements, organisations can develop RMPs that not only comply with all applicable laws and guidelines but also effectively mitigate cybersecurity risks

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?

Improving the alignment of procurement and network change management processes with the notification arrangements under the SOCI Act would involve several strategic adjustments which could enhance cybersecurity resilience, ensure compliance, and facilitate effective risk management across Australian government operations and critical infrastructure sectors. For example:

- Integration of key SOCI Act provisions into the Procurement Process could include specific risk assessment criteria related to the SOCI Act in the procurement processes for technology and services and evaluating potential suppliers' compliance with the SOCI Act and their ability to manage risks to critical infrastructure. In addition, the explicit inclusion of security obligations in contracts with suppliers, would require them to notify the procuring entity of any changes that might affect the security of critical infrastructure, in line with SOCI Act notification requirements.

- At a strategic level, these inclusions could be made at a government department policy level and / or amendments to the Commonwealth Procurement Rules. By implementing these, the Australian government and critical infrastructure entities can better align their procurement and network change management processes with the SOCI Act's notification arrangements. This alignment is essential for enhancing the security and resilience of Australia's critical infrastructure against evolving threats.

Summary

The Cyber Security Strategy presents a comprehensive framework to address cybersecurity challenges in IoT devices. By promoting secure-by-design principles, fostering collaboration across stakeholders, and establishing mechanisms like the CIRB for incident review and policy guidance, the strategy aims to enhance national cybersecurity resilience. It underscores the importance of continuous improvement, stakeholder engagement, and adherence to best practices to create a safer digital environment for all Australians.

While the 2023–2030 Australian Cyber Security Strategy and the forthcoming legislation aim to address critical cybersecurity challenges in IoT devices, it is essential to acknowledge that there is no silver bullet solution to all security issues associated with IoT. The focus on technical controls and organisational policies is crucial in addressing significant security shortcomings, but it is imperative to recognise that sophisticated attacks and evolving threats may require continuous adaptation and vigilance. As the proposed legislation is yet to be drafted, the devil will indeed be in the detail of the draft Bill when it is ultimately released. It will be crucial to carefully analyse the specifics of the legislation to ensure that it effectively addresses the complexities of securing IoT devices and aligns with best practices and industry standards. The interplay with data protection legislation, alignment with related standards, and considerations for evolving technologies will be key factors in shaping a robust legal framework for cybersecurity in IoT devices.

Black Ink Legal commend the Department of Home Affairs for seeking to constructively engage with stakeholders to inform the development of the Cyber Security Strategy and associated Action Plan, and we welcome the opportunity to discuss any of the topics raised in this submission. We look forward with anticipation to the next round of consultation and the release of the draft legislation.

BLACK
INK
LEGAL