Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Overview of Cyber Security Obligations for Corporate Leaders

Leadership in cyber security governance

Contact us

Enquiries regarding the licence and any use of this document are welcome to enquiries@CISC.gov.au, or:

Industry Partnerships Branch,
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Contents

Minister's Foreword

Australia's critical infrastructure is under constant threat from cyber attacks. We need to act now to strengthen our defences.

The Australian Signals Directorate's Annual Cyber Threat Report lays out the problem in stark terms; in the 2022–2023 Financial Year nearly 94,000 reports were made to law enforcement through ReportCyber – around one every 6 minutes.

The threat is real, and it's growing. The stakes in protecting our people and businesses have never been higher. That's why I launched the 2023–2030 Australian Cyber Security Strategy in November 2023.

The Strategy sets out our vision for Australia to be a world leader in cyber security by 2030. The Government envisions a future where stronger cyber protections enable our citizens and businesses to prosper, and to bounce back quickly following a cyber attack.

Our Strategy is game-changing for Australia's cyber security; it defines six 'cyber shields' that we will build to defend our nation from cyber threats. Critical infrastructure is one of these essential shields.

Every day, Australians rely on critical infrastructure to live their lives – including our national electricity, water, health, transport, logistics and telecommunication networks. A large-scale cyber attack on one of these systems would be devastating for life and business in Australia. Cyber security needs to be a top priority for critical infrastructure.

Boards, Directors, and other business leaders play a vital role in shaping the cyber security posture for Australia's critical infrastructure. By providing strategic direction and oversight, they set the tone for a strong cyber security culture – before, during, and after an incident.

Industry leaders should be commended for the steps that they have already taken to enhance the security of Australia's critical infrastructure. Many leaders have made major investments to harden their systems and secure their data – but as always, more can be done.

Through our consultation on the Strategy, we have consistently heard that business leaders face a complex regulatory environment. Directors, Boards and business operators told us that many expectations of cyber governance are unclear. We've heard your call for clarity.

That's why I am pleased to commend this booklet to critical infrastructure owners and operators across the country. This document is our first step to clarify cyber obligations for corporate leaders. Next, we will explore options to provide additional information on cyber governance obligations under current regulation. We've also started a dedicated consultation process to explore amendments to existing cyber security legislation and regulation, including the *Security of Critical Infrastructure Act 2018*.

Cyber security obligations are important, and we expect leaders to take them seriously. By upholding these obligations, government and industry can build our national cyber shields. Together, we can reach our vision of becoming a world leader in cyber security by 2030.

The Hon. Clare O'Neil MP

Minister for Home Affairs
Minister for Cyber Security

Introduction

The complex and evolving risk of cyber incidents presents serious security challenges for owners and operators of Australia's critical infrastructure assets. Cyber security risk management is an imperative for all levels of management from the Board down. An organisation's Board, Directors and senior management play a pivotal role in developing frameworks to adequately identify and manage cyber risks.

Australia's cyber security regulatory framework is designed to support the security and prosperity of our critical infrastructure. Cyber governance obligations are intended to help organisations manage risks and respond to cyber security incidents. This includes obligations under the *Security of Critical Infrastructure Act 2018* (SOCI Act), the *Privacy Act 1988* and the *Corporations Act 2001*. These obligations help businesses prepare for cyber incidents, report incidents when they occur, and respond to the consequences of an incident.

Through our consultation on the *2023–2030 Australian Cyber Security Strategy* (the Strategy), we heard that there is a need for better clarity on cyber governance obligations. Directors, Boards and business operators feel that they face a complex regulatory environment. Many expectations of cyber governance are unclear. Industry feedback has flagged that more could be done to help businesses understand what good cyber security looks like.

Clarifying public regulatory guidance is a commitment from Government in the Strategy, and this document is a first step on that road. Under Initiative 5 of the Strategy, the Australian Government committed to provide clear cyber guidance for businesses. As a first step, this document provides an overview of corporate obligations for critical infrastructure owners and operators. Next, the Government will consider how best to collaborate with industry to guide good cyber governance.

Government systems are also a critical part of the nation's digital infrastructure. As part of our Strategy, the Government has committed to hold ourselves to the same standards we impose on industry. In parallel to clarifying obligations on industry, we will do the same for government departments and agencies as part of a broader plan to uplift Commonwealth cyber security.

How to use this document

This booklet is designed to support Boards, Company Directors, Chief Executive Officers, and other corporate leaders navigate important obligations and requirements that should be considered in developing cyber security frameworks for critical infrastructure assets. While the booklet is primarily aimed at senior leaders, it will be equally informative for relevant officers at all levels within an organisation. The intention is for this document to be read in conjunction with other domestic and international guidance as part of a best practice framework – including the 'Cyber Security Principles' published by the Australian Institute of Company Directors and the Cyber Security Cooperative Research Centre.

The document acts as a stepping off point for Australia's cyber security regulatory landscape, but it is not the final destination. It will continue to be updated, including following the conclusion of ongoing consultation on proposed amendments to cyber security obligations and the regulation of critical infrastructure through the SOCI Act. We also intend to explore options to provide further information to industry beyond critical infrastructure sectors.

The reporting obligations listed here are not exhaustive, and this guide does not constitute legal advice. We encourage you to seek your own professional advice to find out how applicable laws might apply to you, as it is your responsibility to determine your obligations. The booklet provides a quick reference guide to some of the most important obligations and provides senior leaders with a reference point to start assessing their organisation's exposure to cyber risk and regulatory compliance. The compiled list of obligations should also provide assurance to the general public that Australia's critical infrastructure benefits from coherent and appropriate regulation.

Prepare, Report, Respond

The obligations listed in this booklet have been grouped into three themes:

- **Preparing** for a cyber incident;
- **Reporting** to regulators before, during, or after a cyber incident; and
- **Responding** to the consequences of a cyber incident.

We hope that this framework assists entities consider how they might prepare for, and work through, the implications of a cyber security incident.

Each of the obligations outlined in this document help to improve cyber governance, transparency and accountability. Strong governance is essential when responding to and recovering from a cyber incident. Transparency and accountability builds trust among stakeholders, protects an organisation's reputation, and contributes to the quick resolution of an incident. By adhering to these obligations, corporate leaders can better protect their company, shareholders, customers and the broader public from cyber threats.

Preparedness Obligations

Australian Privacy Principle (APP) 11 – Security of Personal Information

Who this applies to:	**The Australian Privacy Principles (APPs) apply to APP entities.** An 'APP entity' is an "agency" or "organisation" within the meaning of the *Privacy Act 1988* (Cth).
Obligation:	APP 11 requires entities to take reasonable steps to ensure the security of personal information held, and to actively consider whether it is permitted to retain personal information. The 'reasonable steps' are circumstance dependent and include: the amount and sensitivity of the information held; the nature of the APP entity; possible adverse consequences in the case of a breach, and; whether a security measure itself is privacy invasive. Entities also have obligations to destroy or de-identify personal information in certain circumstances.
Intent:	To protect the personal information held by entities from misuse, interference and loss, as well as unauthorised access, modification and disclosures.
Enabling legislation:	*Privacy Act 1988*
Administering body:	Office of the Australian Information Commissioner
More information:	Australian Privacy Principles

Australian Prudential Regulation Authority Prudential Standard – CPS 234

Who this applies to:	**Australian Prudential Regulation Authority (APRA) regulated entities.** (APRA oversees banks, credit unions, building societies, general insurance and reinsurance companies, life insurers, private health insurers, friendly societies, and a large part of the superannuation industry. Each of these financial institutions – each bank, each insurance company, each superannuation fund – is an APRA-regulated entity)
Obligation:	To ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.
Intent:	To minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including those managed by related or third parties.
Enabling legislation:	*Australian Prudential Regulation Authority Act 1998* *Banking Act 1959* *Superannuation Industry (Supervision) Act 1993* *Insurance Act 1973* *Life Insurance Act 1995* *Private Health Insurance (Prudential Supervision) Act 2015*
Administering body:	Australian Prudential Regulation Authority
More information:	*Prudential Standard CPS 234*

Critical Infrastructure Risk Management Program Obligation

Who this applies to:	**Responsible entities for critical infrastructure assets in the asset classes specified in section 4 of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.**
Obligation:	Entities must submit an Annual Report regarding their Critical Infrastructure Risk Management Program (CIRMP) approved by the entity's Board, council or other governing body, in the approved form, to the relevant Regulator within 90 days of the end of the relevant Australian financial year. The report must state whether the risk management program was up to date, any variations to the program, and details of how the program was effective in mitigating any relevant impacts that hazards may have had on that asset during that year.
Intent:	To uplift core security practices relating to the management of critical infrastructure assets.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	*Guidance for the Critical Infrastructure Risk Management Program*

Enhanced Cyber Security Obligations – Cyber Security Incident Response Plan

Who this applies to:	**Responsible entities for a System of National Significance (SoNS) as declared under the SOCI Act. Systems of National Significance are a significantly smaller subset of assets which are considered to be of the highest criticality by virtue of their interdependencies across sectors and potential for cascading consequences to other critical infrastructure assets and sectors if disrupted. The Minister may only declare an asset as a SoNS if is a critical infrastructure asset and the Minister is satisfied that the asset is of national significance.**
Obligation:	Relevant entities for SoNS are required to have a written Cyber Security Incident Response Plan detailing how the entity will respond to cyber security incidents that affect its systems.
Intent:	To assist entities articulate 'what to do' and 'who to call' in the event of a cyber incident, thereby reducing the risks of a significant cyber attack against Australia's most critical assets.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	The Enhanced Cyber Security Obligations Framework

Enhanced Cyber Security Obligations – Cyber Security Exercises

Who this applies to:	Responsible entities for a SoNS as declared under the SOCI Act.
Obligation:	Requirement for SoNS to undertake cyber security exercises.
Intent:	To test preparedness, mitigation and response capabilities to reveal whether existing resources, processes and capabilities on an entity sufficiently safeguard being impacted by a cyber security incident.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	The Enhanced Cyber Security Obligations Framework

Hosting Certification Framework Obligations

Who this applies to:	Service providers / hosting providers who provide or seek to provide hosting arrangements of Australian Government data, whole of Government systems and systems rated to the classification level of PROTECTED.
Obligation:	Requirement for all data held by Commonwealth Government agencies to be hosted with the appropriate level of privacy, sovereignty, and security controls.
Intent:	To support the secure management of Government systems and data.
Enabling legislation:	No overarching legislation
Administering body:	Department of Home Affairs
More information:	Hosting Certification Framework

Reporting Obligations

Notifiable Data Breaches Scheme Obligations

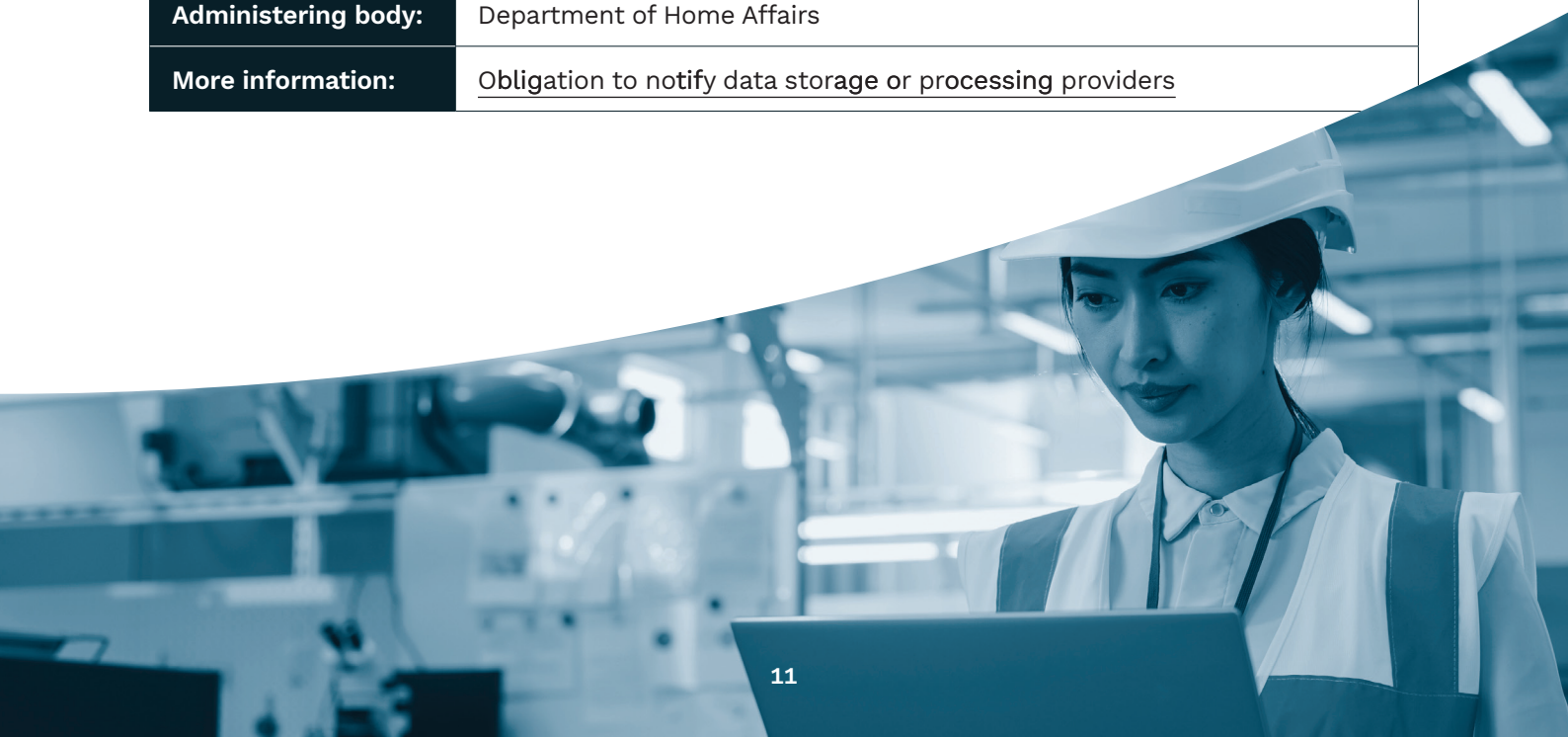
Who this applies to:	Any APP or Privacy Act regulated entity.
Obligation:	To notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved. Conduct a reasonable and expeditious assessment of a suspected eligible data breach, taking all reasonable steps to ensure that this assessment is completed within 30 days.
Intent:	To ensure entities are prepared to respond to data breaches should they occur, and to reduce the risk of harm to affected individuals by ensuring they are notified when their personal information has been compromised.
Enabling legislation:	*Privacy Act 1988*
Administering body:	OAIC
More information:	About the Notifiable Data Breaches scheme Rights and responsibilities

Obligation to report Cyber Security Incidents

Who this applies to:	**Responsible entities for critical infrastructure assets specified in section 5 of the *Security of Critical Infrastructure (Application) Rules 2021*.**
Obligation:	Relevant responsible entities are required to report a cyber security incident to the Australian Signals Directorate.
Intent:	To provide the Australian Government enhanced visibility of emerging cyber threats and risks. This supports Government industry partnerships in mitigating against and responding to cyber incidents.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	Mandatory Cyber Incident Reporting Initial guidance for Critical Infrastructure Sectors

Critical Infrastructure Assets Obliged to Notify Third Party Data Storage or Processing Providers About Sensitive Information

Who this applies to:	**Responsible entities for critical infrastructure assets (as defined in section 12L of the SOCI Act) that utilise third party data storage or processing providers to store or process business critical data for a critical infrastructure asset.**
Obligation:	Responsible entities for critical infrastructure assets are required to notify third party data storage and processing providers that the provider is storing or processing critical business data for a critical infrastructure asset.
Intent:	Ensures third party data storage and processing providers are aware of the sensitivities associated with the data they are handling and can implement appropriate protections.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	Obligation to notify data storage or processing providers



Obligation to Provide Information to Register of Critical Infrastructure Assets

Who this applies to:	**Responsible entities and direct interest holders for critical infrastructure assets specified in section 4 of the *Security of Critical Infrastructure (Application) Rules 2021*.**
Obligation:	Reporting entities must provide operational, interest and control information relating to those assets to the Register and have an ongoing obligation to update the Register if information relating to the asset changes.
Intent:	Ensures the Government can identify and manage risks to critical infrastructure assets.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	Register of Critical Infrastructure Asset Guidance

Obligation to Report to Australian Securities and Investments Commission

Who this applies to:	**Australian Financial Services Licensees and Australian Credit Licensees.**
Obligation:	Requirement to submit notifications about 'reportable situations' (which may include among other matters significant data breaches) to the Australian Securities and Investments Commission (ASIC) within 30 calendar days via the ASIC Regulatory Portal.
Intent:	To ensure financial services are provided efficiently and fairly, and that entities have adequate risk management systems in place.
Enabling legislation:	*Corporations Act 2001*
Administering body:	Australian Securities and Investments Commission
More information:	Reportable situations (previously breach reporting)

Obligation to report to Australian Prudential Regulation Authority

Who this applies to:	APRA regulated institutions.
Obligation:	An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or has been notified to other regulators, either in Australia or other jurisdictions. An entity must notify APRA as soon as possible, and in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.
Intent:	To minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including those managed by related or third parties.
Enabling legislation:	*Australian Prudential Regulation Authority Act 1998* *Banking Act 1959* *Superannuation Industry (Supervision) Act 1993* *Insurance Act 1973* *Life Insurance Act 1995* *Private Health Insurance (Prudential Supervision) Act 2015*
Administering body:	Australian Prudential Regulation Authority
More information:	Prudential Standard CPS 234 Information Security Prudential Practice Guide CPS 234 Information Security Notifications – Information security incident notification, and Material information security control weakness notification

Obligation to Report to ASX Limited

Who this applies to:	ASX listed entities
Obligation:	If you are an ASX-listed listed entity, you must comply with Listing Rule 3.1 that if you become aware of information that a reasonable person would expect to have a material effect on the price or value of your securities, you must immediately tell the ASX. Immediate disclosure is not required if the information falls within the exception in Listing Rule 3.1A.
Intent:	To maintain the integrity and efficiency of Australian markets that trade in ASX quoted securities or derivatives of those securities by ensuring that the market is properly informed.
Enabling legislation:	Nil
Administering body:	ASX Limited
More information:	ASX Listing Rules Chapter 3 – Continuous Disclosure

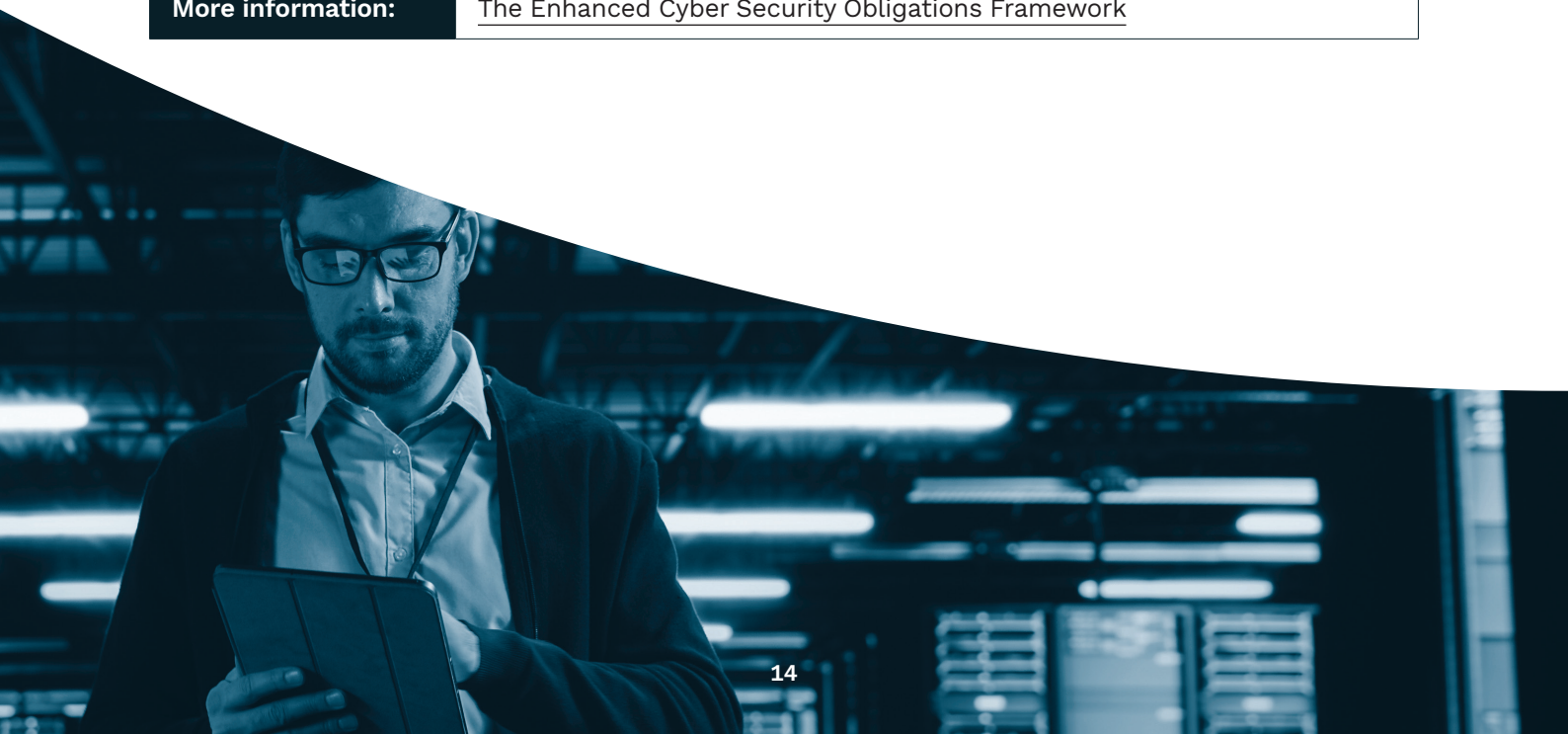
Response Obligations

Enhanced Cyber Security Obligations – Vulnerability Assessments

Who this applies to:	Responsible entities for a SoNS as declared under the *Security of Critical Infrastructure Act 2018.*
Obligation:	The Secretary of the Department of Home Affairs may give a notice requiring the responsible entity of a SoNS to undertake a vulnerability assessment within a specified period.
Intent:	To identify 'gaps' or risks in systems for remediation, including where further resources and capabilities can be deployed to improve preparedness for, and resilience to, cyber incidents.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	The Enhanced Cyber Security Obligations Framework

Enhanced Cyber Security Obligations – Provision of System Information

Who this applies to:	Relevant entities for a SoNS as declared under the SOCI Act.
Obligation:	The Secretary of the Department of Home Affairs may give a notice requiring a responsible entity of a SoNS to provide systems information. This notice can be in relation to periodic reporting of system information or in response to a specific event.
Intent:	To build situational awareness and a near-real time threat picture, allowing the Government to share actionable and anonymised information to assist all entities to improve their cyber resilience.
Enabling legislation:	*Security of Critical Infrastructure Act 2018*
Administering body:	Department of Home Affairs
More information:	The Enhanced Cyber Security Obligations Framework



Australian Prudential Regulation Authority Prudential Standard – CPS 234 Information Security

Who this applies to:	APRA regulated entities.
Obligation:	Information security response plans must include mechanisms for managing all relevant stages of an incident. This includes having robust mechanisms in place to detect and respond to actual or potential compromises of information security in a timely manner and maintaining plans in line with information security incidents experienced, both internally and externally. An APRA-regulated entity would typically have clear accountability and communication strategies to limit the impact of information security incidents. Incident response plans would also typically assist in compliance with regulatory notification requirements.
Intent:	To minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including those managed by related or third parties.
Enabling legislation:	*Australian Prudential Regulation Authority Act 1998* *Banking Act 1959* *Superannuation Industry (Supervision) Act 1993* *Insurance Act 1973* *Life Insurance Act 1995* *Private Health Insurance (Prudential Supervision) Act 2015*
Administering body:	Australian Prudential Regulation Authority
More information:	Prudential Standard CPS 234 Information Security Prudential Practice Guide CPS 234 Information Security

Guidance material – domestic

The following material has been prepared to aid understanding, support general compliance and foster good risk management practices. Senior leaders and their officials may find it useful when developing their approach to upholding cyber governance obligations.

Cyber and Infrastructure Security Centre (CISC)

- Guidance material on the SOCI Act, CIRMP obligation, mandatory cyber reporting and other obligations for critical infrastructure entities and SoNS.

Australian Institute of Company Directors (AICD)

- Cyber Security Governance Principles published by the AICD and the Cyber Security Cooperative Research Centre.

The Australian Signals Directorate

- Resources for governance and user education in cyber security by the Australian Signals Directorate.
- Guidelines for Cyber Security Incidents by the Australian Signals Directorate.
- Cyber security exercise guidance by the Australian Signals Directorate.

Australian Prudential Regulation Authority (APRA)

- Information about how Boards can improve cyber resilience within organisations including the importance of Board engagement in overseeing cyber security risk management and ensuring appropriate strategies are in place.
- A cyber security stocktake report highlighting potential gaps in organisations' cyber resilience.
- Information about the use of multi-factor authentication as a cyber security measure to enhance security and protect sensitive data.
- Information Security Guide, providing comprehensive guidance on cyber security for Boards and Directors including insights into best practices for managing information security risks.

Australian Securities and Investments Commission (ASIC)

- Key cyber resilience considerations for an organisation's Board and Directors to offer valuable guidance on how to approach cyber security matters.
- Good practices in cyber resilience for Boards and Directors, including actionable insights to enhance cyber security measures.
- Spotlight on cyber: Findings and insights from the cyber pulse survey 2023, summarises important trends in cyber security, identifies areas for improvement and highlights better practices with practical examples.

Australian Security Intelligence Organisation (ASIO)

- ASIO Outreach provides advice to Government, industry and academia on current and emerging security threats, and the design and application of security policy. The Outreach portal is a secure website for security professionals. The website is accessible to approved subscribers and contains intelligence reporting on domestic and international security, and protective security advice in relation to espionage, foreign interference, and terrorism.

Office of the Australian Information Commissioner (OAIC)

- Overview of the OAIC's Notifiable Data Breaches scheme.
- Information on when organisations are required to report a data breach under the Notifiable Data Breaches Scheme.
- Guidance on how to report a data breach when required.
- Privacy guidance for organisations and government agencies.
- Guidelines to Australian Privacy Principles.

Reserve Bank of Australia (RBA)

- RBA report highlighting the importance of building resilience to cyber risks including the need for Boards to proactively address cyber threats in the financial sector.
- RBA report offering additional insights on addressing cyber risks in the financial sector.

Tertiary Education Quality and Standards Agency (TEQSA)

- Guidance note on corporate governance by TEQSA, which includes considerations for cyber security.

Guidance material – international

Please note: These links are provided for reference only. Australian business leaders should follow domestic laws in the first instance. That notwithstanding, international partners have prepared a range of guidance material that may be relevant to senior leaders in Australia.

In the United Kingdom:

- The National Cyber Security Centre has produced a Cyber Security Toolkit to help Boards ensure that cyber resilience and risk management are embedded throughout an organisation, including its people, systems, processes and technologies.
- The National Protective Security Authority has produced a Leadership and Governance pack to support positive and visible Board level support for protective security.

In the United States:

- The Cybersecurity and Infrastructure Security Agency has produced guidance for corporate leaders and CEOs.

In Canada:

- The Canadian Centre for Cyber Security has produced cyber security guidance.
- Public Safety Canada has produced a range of materials to support critical infrastructure enhance resilience and manage risk.

Conclusion

Strong organisational leadership has never been more important for addressing cyber security risks to Australia's critical infrastructure.

Boards, Directors, and other corporate leaders must embrace their roles in promoting cyber resilience and complying with regulatory frameworks. Awareness of cyber governance obligations is essential for corporate leaders to make informed decisions to manage cyber risk. These obligations help us safeguard our critical infrastructure and protect the broader Australian economy from rapidly evolving cyber threats.

This guide is an initial step to provide further clarity on Australia's cyber security regulatory landscape, but it is not the final destination. This document will continue to be updated to reflect changes in the cyber security landscape. We are also exploring further options to provide additional information to corporate leaders beyond the critical infrastructure sector.

The Government is commencing a targeted consultation process to seek industry feedback on proposed amendments to cyber security obligations and the regulation of critical infrastructure under the SOCI Act. We invite corporate leaders across all sectors to engage in this process and help shape the next iteration of cyber obligations in Australia.

For further information please contact us at
enquiries@cisc.gov.au

Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE