Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Protecting Critical Infrastructure and Systems of National Significance

Industry Town Hall

25 November 2021

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Thank you for joining the Industry Town Hall

For today…

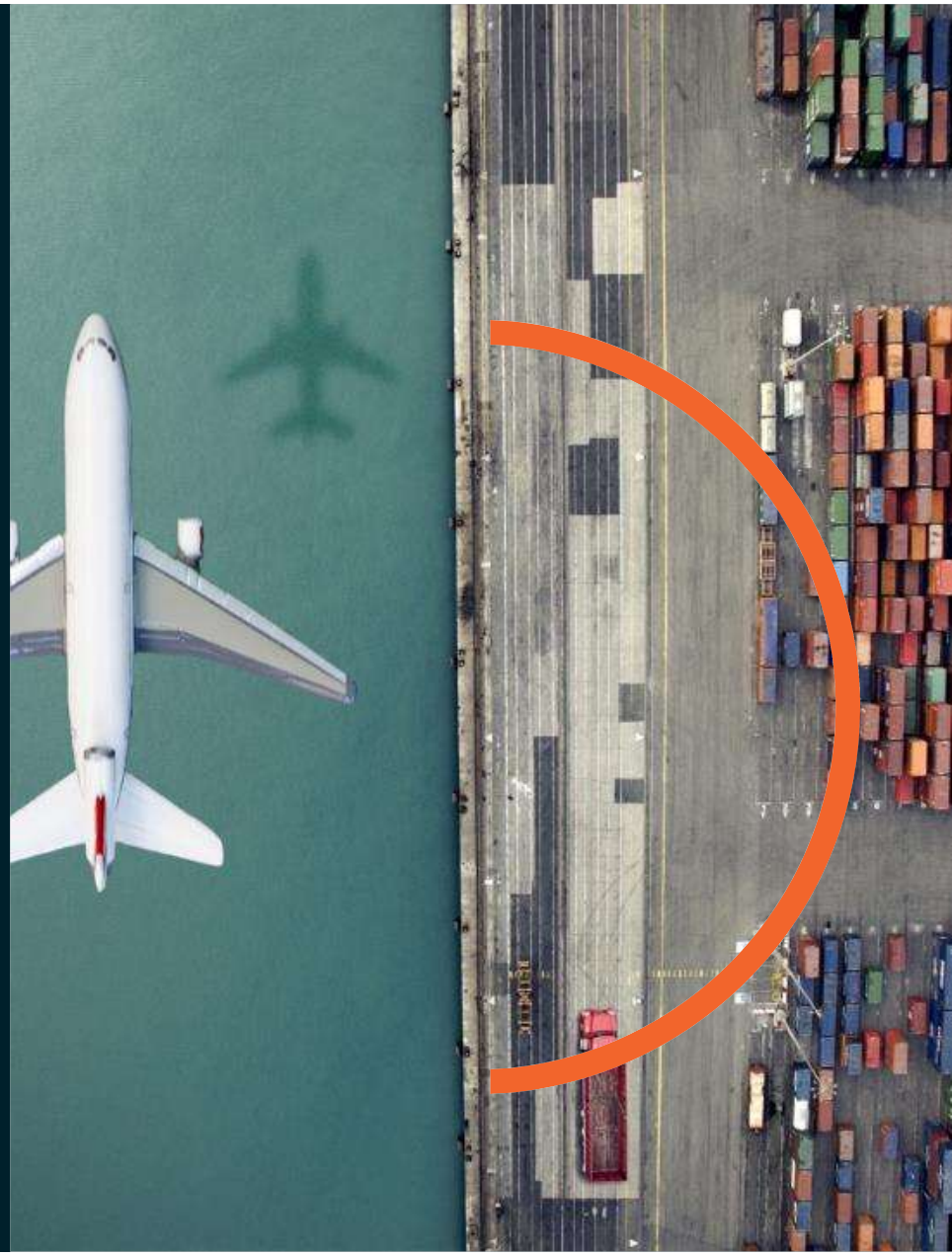
- We'll begin at 11:00am AEDT.
- When you aren't speaking, we kindly ask you keep your camera and microphone off.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Agenda

- SLACI Bill and your obligations
- RMP rules – where we landed
- Exposure Draft – next steps
- CISC website for more information



Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Two-step approach

BILL ONE - passed Senate on 22 November

- Register of Critical Infrastructure assets
- Mandatory cyber security incident reporting
- Government Assistance
- Broadening to 11 CI sectors

Fact sheets are NOW ON the CISC website explaining these elements – go to **www.cisc.gov.au**

BILL TWO – early 2022

- Risk Management Program
- Enhanced Cyber Security Obligations
- Systems of National Significance

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

BILL ONE

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Register of Critical Infrastructure Assets:

Which CI Asset classes do we propose this obligation applies to for consultation?

- Telecommunications
- Broadcasting
- Domain name system
- Data storage or processing
- Payment Systems
- Food and grocery
- Critical hospitals
- Freight infrastructure
- Freight services
- Public transport asset
- Liquid fuel
- Energy market operator
- Electricity*
- Gas *
- Water and Sewerage*
- Port*

* Obligation already applies to some assets in these asset classes under SOCI Act 2018

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Register of Critical Infrastructure Assets:
Next steps

- The Minister may commence a consultation period for a minimum of 28 days on draft rules to ‘switch on’ the Register for these asset classes.
- CISC will email all affected entities advising of the consultation process.
- Once consultation commences, CISC welcomes submissions (via the CISC website - **www.cisc.gov.au**) for the Minister’s consideration.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mandatory cyber security incident reporting:

Which CI Asset classes do we propose this obligation applies to for consultation?

- Telecommunications
- Broadcasting
- Domain name system
- Data storage or processing
- Banking
- Superannuation
- Insurance
- All financial market infrastructure – including payment systems
- Food and grocery
- Critical Hospitals
- Higher education
- Freight infrastructure
- Freight services
- Public transport
- Liquid fuel
- Energy market operator
- Electricity
- Gas
- Water and sewerage
- Aviation
- Ports

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mandatory cyber security incident reporting:
Next steps

- The Minister may commence a consultation period for a minimum of 28 days on draft rules to ‘switch on’ cyber reporting for these asset classes.
- CISC will email all affected entities advising of the consultation process.
- Once consultation commences, CISC welcomes submissions (via the CISC website – **www.cisc.gov.au**) for the Minister’s consideration.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Government Assistance

- This is available to **YOU ALL** from the **day after** Royal Assent.
- Government will be able to provide assistance immediately prior, during or following a significant cyber security incident to ensure the continued provision of essential services.
- The Minister for Home Affairs could authorise the Secretary of the Department of Home Affairs to:
  - **Gather information** to determine if another power in the *Security of Critical Infrastructure Act 2018* should be exercised; or
  - **Action Direction** - direct an entity to do, or refrain from doing, a specified act or thing; or
  - **Intervention Request** – request an authorised agency (i.e. Australian Signals Directorate) provide support (with agreement from the Prime Minister and Minister for Defence)

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Bill One – our commitment to you

- We will continue to work with you on as you to embed these obligations as ‘business as usual’.
- We will work with your Regulators (where they are not Home Affairs) to ensure this information is shared appropriately.
- We will test Government Assistance Measures to make sure our processes are clear and robust.
- We encourage you to join the Trusted Information Sharing Network to keep abreast of issues facing Australia’s critical infrastructure.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

BILL TWO

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Risk Management Program:

Who have we been engaging with on the Risk Management Program?

- Broadcasting
- Domain name systems
- Data storage or processing
- Critical hospitals
- Freight infrastructure
- Payment systems
- Freight services
- Liquid fuel
- Energy market operator
- Electricity
- Gas
- Water and sewerage
- *Defence Industry**

If your asset class is not listed above - at this time - we do not intend to recommend to the Minister to 'switch on' the RMP for you when Bill Two is passed.

** The Naval Shipbuilding area will have requirements under the RMP*

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

What we have agreed:

- Governance Rules
- Material Risk Rules
- Cybersecurity Hazards Rules
- Personnel Hazards Rule
- Supply Chain Hazards Rules
- Physical and Natural Hazards Rules

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Governance Rules

Governance rules support the substantive obligations by requiring entities to document how they will carry out a number of activities that support good risk practice within their organisation. This provides Government with assurance that risks are being managed appropriately, while allowing responsible entities the flexibility to develop and implement a risk management program that reflects sector-specific risks and hazards.

1. Responsible entities must, within six months of the commencement of this rule, ensure that their risk management program includes a reasonable risk methodology, having regard to ISO 31000 or an equivalent standard.

2. Responsible entities must, within six months of the commencement of this rule, document in their risk management program, the process by which the responsible entity has identified:

a. the components of the entity that are essential to the functioning of the critical infrastructure asset; and

b. the types of relevant impact that are most significant to the critical infrastructure asset; and

c. any critical interdependencies with other critical infrastructure assets.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Governance Rules

3. Responsible entities must, within six months of the commencement of this rule, ensure that their risk management program includes details of the individual or individuals responsible for the development and implementation of the risk management program as a whole, as well as the activities detailed within.

4. Responsible entities must, within six months of the commencement of this rule, document in their risk management program how they will take a holistic approach to risk management, outlining how the entity will consider the relevant impact of different material risks on their assets and the mitigation or minimisation of those threats or hazards across their organisation.

5. Responsible entities must, within six months of the commencement of this rule, ensure that their risk management program outlines a process for regularly reviewing the risk management program, including what circumstances would require a supplementary review.

6. Responsible entities must, within six months of the commencement of this rule, ensure that their risk management program outlines a process for updating the risk management program.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Definition of Material Risk

1. The proposed Bill Two requires responsible entities to continue to identify and mitigate **material risks** that have a substantial impact the availability, reliability and integrity of a critical infrastructure asset.

2. Responsible entities for critical infrastructure assets must consider **all** relevant **material risks** to their business.

3. Responsible entities for critical infrastructure assets are responsible for determining if a risk is a **material risk**.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Definition of Material Risk (continued)

4. Recognising the operating context differs between entities, when considering if a risk is a **material risk**, a risk management program should have regard to consideration of:

a. impairment of a critical infrastructure asset that may prejudice the social or economic stability of Australia or its people; the defence of Australia or the national security of Australia;

b. a hazard that would cause the stoppage or major slowdown of a critical infrastructure asset's functioning for an unmanageable period;

c. the substantive loss of access to or deliberate or accidental manipulation of a component of a critical infrastructure asset such as the position, navigation and timing systems impacting provision of service and/or functioning of the asset;

d. the interference with a critical infrastructure asset's operating technology or information communication technology such as a SCADA system essential to the functioning of a critical infrastructure asset;

e. the relevant impact on the critical infrastructure asset resulting from the storage, transmission or processing of sensitive operational information outside Australia;

f. the relevant impact on the critical infrastructure asset resulting from the remote access to operational control or operational monitoring systems of the asset; and

g. any other material risks as identified by the entity that go to the substance of the functioning of a critical infrastructure asset.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Rule 1 – Cyber and Information Security Hazards

1. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated.

2. Responsible entities for critical infrastructure assets **must**, within **18 months** of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks:

a. The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;

b. AS ISO/IEC 27001:2015;

c. The National Institute of Standards and Technology (NIST) Cybersecurity Framework;

d. The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1;

e. Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or

f. an equivalent standard.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Rule 2 – Personnel Hazards

1. Responsible entities for critical infrastructure assets **must**, **within 6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity identifies their critical positions and/or critical personnel and includes a list of these positions and/or personnel, as appropriate.

2. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity ensures that the suitability of critical positions and critical personnel are appropriately managed, including but not limited to:

a. assessing and managing the ongoing suitability of critical personnel and persons holding critical positions, through personnel and human resource arrangements; and

b. considering, where commensurate with the risk environment, requiring an AusCheck or an equivalent vetting check for critical personnel.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Rule 2 – Personnel Hazards (continued)

3. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity mitigates risks arising from potential negligent personnel and malicious insiders who could cause damages to the functioning of a critical infrastructure asset.

4. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity manages risks arising from the off-boarding process for outgoing personnel.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Definition of Critical Position and Personnel

The definition of *critical position* includes **but is not limited to**, a position in a responsible entity which has responsibility, access, control or management of the essential components or systems of the asset and where the absence or compromise of the position or its holder would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the responsible entity.

The definition of *critical personnel* includes, **but is not limited to**, any employee of a responsible entity with responsibility, access, control or management of the essential components or systems of the asset and whose absence or compromise would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the responsible entity. The definition of personnel includes, but is not limited to, direct employees, interns, contractors and subcontractors.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Rule 3 – Supply Chain Hazards

1. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of strategies to secure the supply of products and services to critical assets to enable continued operation.

2. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity assesses and manages:

a. unauthorised access, interference or exploitation of the critical infrastructure asset's supply chain;

b. privileged access to the critical infrastructure asset by a provider(s) in the supply chain;

c. disruption and sanctions of the critical infrastructure asset due to an issue in the supply chain;

d. threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains;

e. vulnerability disclosure for other elements within supply chains;

f. high risk vendors, as defined in the *Australian Cyber Security Centre's Cyber Supply Chain Risk Management Practitioners guide (2019)*; and

g. vendor dependency or reliance on entities inherently within supply chains.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Rule 4 – Physical and Natural Hazards

1. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity manages physical and natural hazards in their risk management program, at self-assessed critical sites.

2. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity seeks to minimise and mitigate the risk and relevant impacts of unauthorised access, interference and control of critical assets as well as the relevant impact of the natural hazards.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Rule 4 – Physical and Natural Hazards (continued)

3. Responsible entities for critical infrastructure assets **must**, within **6 months** of the commencement of this rule, ensure that their risk management program includes details of how the entity:

a. responds to incidents where unauthorised access occurs;

b. controls authorised access, including restricting access to only those persons with the appropriate approval who have an operational need to access;

c. conducts tests, as appropriate, to provide assurance that active security measures are effective and appropriate to detect, delay, and deter breaches of security; and gives consideration to how the responsible entity will respond and recover from breaches of security; and

d. minimises, mitigates and recovers from relevant impacts on their asset arising from natural hazards and disasters, including but not limited to bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis, health hazards such as pandemics.

Australian Government
Department of Home Affairs

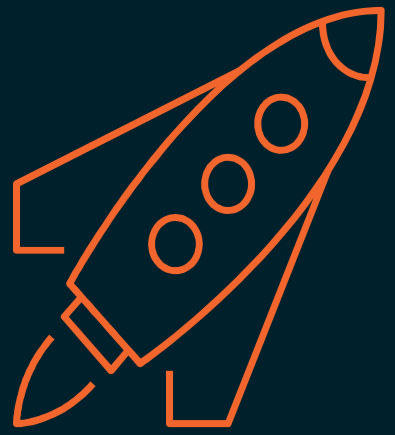
CYBER AND INFRASTRUCTURE SECURITY CENTRE

Exposure Draft - Bill Two

- The Department is hoping to release an Exposure Draft of Bill Two in the next few weeks.
- If agreed, the period of consultation will be from mid-December 2021 to the beginning of February 2022.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE



Thank you

Further information on next steps and your obligations can be found at **cisc.gov.au**

We encourage you to continue discussions internally within your organisation on these reforms.

Please send any comments or questions through to **CI.reforms@homeaffairs.gov.au**