Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Protecting Critical Infrastructure and Systems of National Significance

Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Industry Town Hall

4 February 2022

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Thank you for joining the Industry Town Hall

For today…

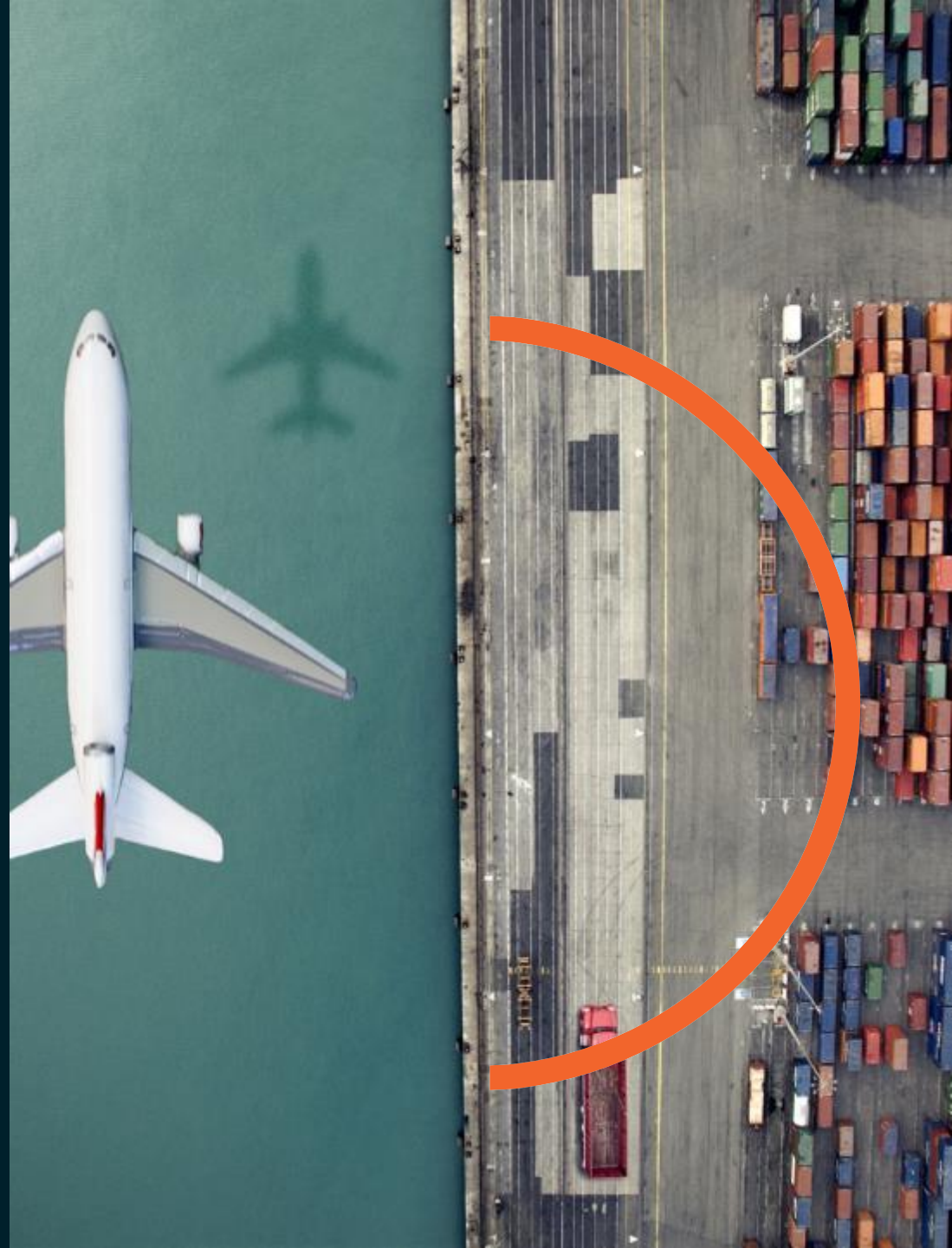
- When you are not speaking, we kindly ask you keep your camera and microphone off to assist in managing bandwidth and connectivity.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Agenda

- The process up until now
- Key themes from your submissions
- Key amendments to the Bill
- Next steps
- Recap on Bill One



Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

We would like to open up Mentimeter for commentary

The Department is seeking feedback to inform our guidance material and education activities for these reforms moving forward.

Are there any topics or formats that you or your organisation may find most valuable?

On your phone – go to www.menti.com
and enter code 2434 8084

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

The journey so far…

The Department thanks you for your contributions to the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 to date.

- Department held 3 townhalls on the exposure draft
- Engaged in **9** roundtable discussions with the Minister
- Continued bilateral engagements, and ad-hoc discussions
- Received **66** submissions on the exposure draft

All your engagements continue to shape the development of the SLACIP Bill, through an iterative drafting process.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Key themes from submissions – General themes

- Requirement for detailed guidance and ongoing engagement consultation to implement reforms
- Note regulatory duplication with existing regulatory frameworks
- Requirement to refine certain sector and asset definitions
- Acknowledge there are circumstances where the use and disclosure of protected information is not contemplated by the proposed framework

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Key themes from submissions – Risk Management Program

- Note the cost to industry of the Risk Management Program
- Increase timeframes for compliance with the Risk Management Program
- Require recognition of existing regulatory frameworks which achieve the intent of the Risk Management Program

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Key themes from submissions – Systems of National Significance and Enhanced Cyber Security Obligations

- Require increased clarity over which assets will be declared systems of national significance
- Seek further consultation both before and after a declaration is made

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Key Proposed Amendments

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Key proposed amendments from the Exposure Draft – Definitions

- Education asset and higher education and research sector
- Data storage or processing service asset and sector
- Critical telecommunications asset
- Critical superannuation asset
- Critical domain name system
- Critical food and grocery asset
- Gas transmission pipeline
- Direct interest holders (moneylenders)

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Key proposed amendments from the Exposure Draft – Risk Management Program

- Rule making power to determine which existing frameworks and standards will meet the Risk Management Program obligations

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Key proposed amendments from the 2020 Bill – Protected Information

- The SLACIP Bill will expand the circumstances in which entities may make a record of, use or disclose protected information which relates to that entity
  - An entity may share information with relevant Commonwealth, State or Territory Government entities for relevant purposes
  - The new Secretary content provision will cover ALL other appropriate circumstances, balancing its national security significance with its utility.

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Mentimeter

The Department is seeking feedback to inform our guidance material and education activities for these reforms moving forward.

Are there any topics or formats that you or your organisation may find most valuable?

On your phone – go to www.menti.com
and enter code 2434 8084

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Next Steps

- The Cyber and Infrastructure Security Centre will finalise its review of all your submissions and feedback, and finalise legal drafting of any further amendments to the Bill

- The Parliament will debate the Bill

- Risk Management Program, Enhanced Cyber Security Obligations and Systems of National Significance would become available, if Parliament pass the Bill.

- We will work with you on the development of guidance, including via the Trusted Information Sharing Network, to assist in the implementation of the reforms

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Bill One – Security Legislation Amendment (Critical Infrastructure) Act 2021

- The Security Legislation Amendment (Critical Infrastructure) Act 2021 commenced in December
- The Department has concluded consultation with industry on the proposed 'turning on' of Positive Security Obligations
  - Register of Critical Infrastructure Assets
  - Notification of Cyber Security Incidents
- The Minister may seek to make the Rules

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

The TISN will be the key forum for the uplift of Australia's critical infrastructure into the future, and can be contacted at **CIR@homeaffairs.gov.au**