Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

# Protecting Critical Infrastructure and Systems of National Significance

## Co-design of Governance Rules: Critical Infrastructure Risk Management Program

## Summary of consultation

**1300 27 25 24**
ci.reforms@homeaffairs.gov.au

# Contents


Co-design consultation 3

Governance Rules - Objective 3

Governance Rules Framework 3

Structure of consultation 3

Summary of key issues 4

Context identification process 4

Siloes & Accountability 5

Risk methodology & Reviews 6

Next steps 7

# Co-design consultation

## Governance Rules - Objective

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) introduces:

- an expansion of critical infrastructure assets and sectors;
- additional positive security obligations for responsible entities of critical infrastructure assets;
- enhanced cyber security obligations for responsible entities of those assets most important to the nation, described as systems of national significance; and
- government assistance in response to significant cyber attacks that impact on Australia's critical infrastructure assets.

The positive security obligations require responsible entities to manage the security and resilience of their critical infrastructure assets, including through delivering a Critical Infrastructure Risk Management Program (the Program). The objective of the Governance Rules is to provide further specificity to the Program requirements in the Bill.

Working closely with industry to co-design rules ensures that the reforms will be implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burden.

## Structure of consultation

In March 2021, the Department of Home Affairs (the Department) has undertaken a period of co-design on prospective cross-sectoral Governance Rules to underpin the Program, comprising of:

1. Two virtual town hall sessions were held on 2 and 4 March 2021, attended by approximately 850 participants. The purpose of these sessions was to introduce the key concepts that would be discussed in the workshops on Governance Rules, with an emphasis on providing clarity to industry on what the Program obligations would require.

2. Seven workshops were held over a two-week period from 8 March 2021, with over 500 industry and government stakeholders in attendance. Discussions in the workshops focused on three inter-related areas that, in Government's view, should be codified through rules – context identification processes, siloes and accountability, and risk methodology and reviews.

3. Two further town hall sessions **will be held** on 29 and 30 March 2021 to present key findings from the workshops and introductory town halls.

# Summary of key findings

## Common themes

### What we heard

- Industry collectively suggested that their current business practices broadly achieve many of the objectives of the Program already. Many participants advised that they have already implemented risk management plans in their businesses either for business continuity purposes or as a requirement of existing regulation.
- Many industry participants expressed concern with apparent overlap of requirements for the Program and pre-existing regulation/sector requirements.
- There was general agreement that the Governance Rules must not be overly prescriptive. Participants advised that each industry sector manages risks in a unique way. Broadly applied prescriptive rules may disrupt industry's ability to respond to unique challenges. By following a more principles-based approach, each business could continue to manage their own risks in the way that works best for its context.

### What we will do

- The Department will ensure that minimising regulatory duplication remains a top priority.
- In developing rules the Department will strive for clarity whilst avoiding prescriptiveness where appropriate, providing industry with sufficient flexibility to recognise the unique circumstances of their business.
- The Department will also provide guidance material to industry to ensure smooth implementation of the requirements under the Program.
- Rules will be designed so as not to disrupt existing good practices in mature entities, but to uplift practices within less mature entities.

## Context identification processes

### Objectives

- The Program provisions of the Bill focus on the entity identifying threats or hazards to their critical infrastructure asset and managing material risks.
- Government's view is that good risk management practice would require an entity to understand its context in order to effectively identify threats and hazards to their assets.
- Requiring entities to identify their context as part of preparing and updating their Program will help to ensure it is developed in a holistic and coherent fashion.

### What we heard

- There was general agreement that rules requiring entities to carry out context identification as part of preparing the Program would be beneficial.

- Participants broadly accepted that responsible entities should be required to have a **principles-based risk identification process** outlined in their risk management program. Avoiding a prescriptive approach will enable businesses to identify material risks that are relevant to their context. Discussions focused on the importance of balancing the development of principles-based rules for assurance that security outcomes were being achieved, whilst enabling sufficient flexibility for industry to leverage existing risk management processes.
- Industry stakeholders supported the need to avoid duplication, including by cross-referencing **existing risk frameworks**. Further suggestions were made that risk frameworks should be aligned with ISO31000, an international standard widely adopted across sectors in Australia. While broadly comfortable with this approach, some industry stakeholders emphasised the importance of leveraging other risk frameworks that were already informing risk management, including FARE, NIST, HB167:2006 Security Risk Management, and C2M2. Other stakeholders noted similarities in risk management practices included in the 'three lines of defence' model.
- Emphasising that risks are constantly evolving and that they are not linear, **strong information sharing** is needed to ensure that context identification is accurate and meaningful. This would be particularly relevant to some sectors due to their different levels of maturity in risk management. A number of industry representatives stressed that in their view, Government has a significant role to take on in this space to ensure that entities have the best information available to them to inform their Programs.

## What we will do

- The Department will draft Governance Rules that will require responsible entities to document in their Program:
    a. how they will identify context as part of their risk management process; and
    b. the outcome of the context identification process.
- The Department will continue to look for opportunities to improve mechanisms to encourage information sharing between industry or between industry and government.
- The Department notes that the Trusted Information Sharing Network (TISN) will remain a helpful mechanism for delivering threat and other information and will continue to engage with industry on how to better utilise and broaden this network.

## Siloes and Accountability

### Objectives

- Government's view is that good risk management practice entails both identifying and mitigating material risks that may have a significant relevant impact on their critical infrastructure assets. Requiring entities to demonstrate that they are thinking about risk management holistically in their business will help to ensure that risk processes are robust.
- Government's view is that in order to be effective, the Program provisions of the Bill must be underpinned by appropriate responsibilities and accountabilities within the business for the Program. Requiring entities to document in their Program who is accountable for the Program as a whole and for each activity described in the Program will help to ensure that coordinated risk practices are adopted within different parts of a business.

### What we heard

- Industry expressed that, in some sectors, '**siloes**' may serve a purpose by ensuring that appropriate subject matter expertise was engaged when mitigating specific types of risk. For example, it would be appropriate that the cyber security expert would take the lead on designing and implementing cyber security controls. Sometimes, 'siloes' would be created for other reasons. For example, personnel security was often treated separately due to privacy obligations.
- Concerns were raised about the threat vector of **supply chains**, noting that most businesses had little or no control over their suppliers who may be located both domestically and overseas.
- In relation to **accountability**, there was broad support for the Bill's requirement for the Board or equivalent authority to certify the Program. When asked about accountability for specific risk processes within the Program, industry advised that different levels of maturity and capability across sectors and entities meant that there was not a 'one size fits all' organisational structure for accountability.
- Strong feedback was received to indicate that rules **should not overly prescribe** how responsible entities determine appropriate responsibilities and accountabilities as it could undermine more proactive risk management approaches and place an unreasonable burden on entities operating within complex regulatory environments. Instead, rules should support those entities in providing the Government assurance that obligations were being met. Industry also requested more examples of what would be required in practice.

### What we will do

- The Department will draft rules requiring entities to document in their Program **how** they will take a holistic approach to risk management by outlining how the entity will consider the relevant impact of material risks on their assets, and the mitigation or minimisation of those threats or hazards across their organisation.

- The Department will draft rules requiring entities to document in their Program who is responsible and accountable for both the Program as a whole, and each individual activity within the Program.
- The Department will consider existing regulatory frameworks, including State and Territory legislation to avoid unnecessary regulatory duplication.
- The Department will draft rules that give responsible entities sufficient flexibility and to avoid arbitrarily designating roles or individuals with accountability, as there needs to be assurance that those who certify the Program have the knowledge and expertise to do so.

## Risk methodology and Reviews

### Objectives

- Government's view is that while industry is best placed to identify, assess and manage risks to their business, there is merit in a rule that requires the entity to **identify** a risk management framework that will underpin the development of the Program.
- The Bill currently requires the Program to be reviewed on a regular basis and kept up to date. Government's view is that there is value in a rule requiring the Program to **outline** the process by which the Program will be reviewed regularly and kept up to date.

### What we heard

- Discussions highlighted sectoral variance in **existing risk management practices**. Stakeholders in the finance sector indicated that their key risks were primarily related to supply chain (e.g. third-party risk through contractual arrangements) and cyber security. Stakeholders in the energy sector highlighted that their key priorities were to ensure business continuity and safety. Stakeholders in the higher education and research sector advised that they had standard risk process in place through business impact analysis and disaster recovery planning.
- Industry stressed the importance of existing regulatory frameworks being taken into account so that entities would have the flexibility to maintain their security in the way most suited to achieving their security objectives.
- Suggestions were made that rules include **safe harbour provisions** to help minimise regulatory burden and duplication. For example, entities that demonstrated that they reviewed their Programs in accordance with an industry standard could be considered to have met the requirements under the Program.
- Rules should not prescribe **the frequency of reviews**, as good risk management frameworks already included adequate review processes. Industry advised that different frequency of reporting requirements was implemented based on different risk elements.

### What we will do

- The Department will draft rules that will require responsible entities to **document appropriate and acceptable risk methodologies** to underpin the Program. Efforts will be taken to avoid rules being too prescriptive.
- The Department will use existing frameworks and avoid duplication where it can be clearly evidenced that such a framework can adequately meet the requirements of the Program.
- The Department will consider the concept of safe harbour provisions during the co-designing of sector-specific rules.
- The Department will draft rules that will avoid a 'one size fits all' approach to review of the Program.

# Next steps

Following the final two town hall sessions on 29 and 30 March 2021, the Department will finalise the schedule and dates for the sector-specific co-design and have that information available to industry as soon as possible.

Engagement with industry has been essential throughout the development of the Bill. The Department will provide further advice on how industry stakeholders can participate in the co-design process.

In early April the Department will publish draft threshold definitions, finalising the development of asset definitions, on the Home Affairs website for a three week period. The department welcomes submissions on these threshold definitions during this period.

## Additional support for industry

- In addition to our regulatory reforms, the Australian Government is committed to a range of non-regulatory reforms to assist the critical infrastructure community to improve the security and resilience of critical infrastructure. These non-regulatory reforms also aim to support industry to meet their regulatory obligations.

- The Department is updating the Critical Infrastructure Resilience Strategy, which sets out how the Australian Government will work with critical infrastructure entities of all levels of maturity to enhance the security and resilience of critical infrastructure.

- The Department is also enhancing the Trusted Information Sharing Network (TISN), which will help deliver the objectives of the Critical Infrastructure Resilience Strategy, and enhance and better coordinate our education and engagement activity.

- The TISN is a trusted, non-competitive environment for the critical infrastructure community to better plan, prepare, respond and recover in the face of all hazards. We are enhancing this network to more closely reflect the needs that industry and government identify as critical to ensuring a more secure and resilient critical infrastructure community, including greater engagement with government at all levels and greater cross-sector engagement.

- Organisations that are interested in joining the Trusted Information Sharing Network may contact the Critical Infrastructure Centre at CIR@cicentre.gov.au. More information about the network can be found on the CIC website, www.cicentre.gov.au.