Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

Protecting Critical Infrastructure and Systems of National Significance

Risk Management Program: Sector-Specific Rules

Discussion paper

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

Overview

The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) will introduce positive security obligations for responsible entities of critical infrastructure assets. The positive security obligations will 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 policy objective behind requiring critical infrastructure assets to adopt and maintain the Program is to drive an uplift in the security and resilience of Australia's critical infrastructure and provide Government assurance that Australia's critical services are being managed in a secure and resilient manner.

Whilst the broad objectives of a Program are set out in the Bill, under the Bill, the Minister for Home Affairs (the Minister) will have the ability to make rules that detail particular requirements for a Program. We anticipate that there will be a set of governance rules that apply generally and separate sector-specific rules made by the Minister.

The Department of Home Affairs (the Department) recently completed the first tranche of co-design with industry and government stakeholders to develop sector-agnostic governance rules. These rules will provide the overarching framework for critical infrastructure entities and set expectations about how their Programs must be developed. A summary of key findings from the co-design workshops is available here.

We are now commencing sector-specific co-design. The objectives of sector-specific co-design are to:

- assess whether there are existing regulations that meet the objectives of the Program and to reduce regulatory burden where possible;
- ensure that there are rules in place for each sector that will drive an uplift in the security and resilience of critical infrastructure assets; and
- make rules that will prescribe material risks for each sector.

Avoiding regulatory duplication

In specifying requirements in rules made for the purpose of the Program, the Minister is obliged to consider any existing regulatory system of the Commonwealth, a State or a Territory that imposes obligations on responsible entities[1]. Government's position remains that where a class of assets is already subject to a regulatory regime which comprehensively addresses (and through which entities achieve) the same outcomes as we seek through these reforms, we will not duplicate those obligations.

In some cases, entities may be subject to existing regulation that only partially addresses the outcomes that we seek through these reforms. In order to avoid a situation where an entity is required to deliver two separate Programs, we will draft principles-based rules, as appropriate, allowing responsible entities flexibility to determine how they deliver a Risk Management Program that would achieve all of the outcomes sought through the reforms.

[1] Sub-clause 30AH(6) Security Legislation Amendment (Critical Infrastructure) Bill 2020

Sector-specific rules

In developing sector-specific rules, the Department considers that there are broadly two types of inter-related rules: 1) standards rules; and 2) material risk rules.

1. Standards rules

The threat environment in which we are all operating is constantly evolving and becoming more complex over time. Government is determined to ensure that entities see security and resilience as an ongoing commitment and effort, rather than a 'check-a-box' compliance exercise. In this regard, we assess that there is merit in developing rules that would require entities responsible for a particular class of assets to meet particular standards in implementing mitigations across some or all of the hazard vectors we have discussed in previous consultation papers. We also recognise that there are many possible frameworks or standards that could be leveraged in developing such rules, including:

- Maturity models (e.g. C2M2 (or AESCSF));
- International standards (e.g. ISO27001, IEC62443); and
- Existing government frameworks (e.g. PSPF, ISM, ASD's Essential 8).

Government is also of the view that there is merit in developing rules that require responsible entities to implement mitigations in a coordinated, complementary and comprehensive manner. Rules requiring responsible entities to structure their risk mitigation activities in a particular vector or domain on a standard or framework will help ensure that an entity's Program is complementary and comprehensive.

Questions for consultation

- Do you agree that rules requiring entities in your industry sector to meet particular standards are necessary?
- What are your views on how the same outcome (a measureable uplift in the security and resilience of Australia's critical infrastructure) could be achieved in a different way?
- What is your preference for the types of standards or frameworks that would potentially be made mandatory? Should there be a specific list of standards?
- If rules were to be made for your sector requiring a particular standard to be met, how long would be required for entities to reach that standard?
- Do you agree that rules requiring an entity to align its mitigations to a framework or standard are necessary?
- What are your views on how the same outcome could be achieved (i.e. assurance for Government that mitigations are not being implemented in an ad hoc manner)?

2. Material risk rules

The Bill provides for rules to be made that that specify a risk to be a material risk. This would have the effect of requiring responsible entities to include that material risk in their Program, and therefore, require them to take steps to minimise the risk of the hazard occurring, and mitigate the consequences should it occur.

We believe there is merit in specifying some risk as material risks through the rules. Examples include:

- The loss of access to position, navigation and timing systems;
- The storage of sensitive operational information outside Australia; and
- The control and operation of assets from outside Australia.

We anticipate using the co-design workshops to discuss potential material risk rules with the sector.

It is important to note that material risks specified by Government rules are not an exclusive list of the material risks that should be considered by the responsible entity of a critical infrastructure asset. The Bill would require responsible entities to continue to identify and mitigate material risks that could have impact the availability, reliability and integrity of the critical infrastructure asset.

Questions for consultation

- Do you agree material risk rules are required for your sector?
- Do you have views as to how we should describe material risks in the rules?
- Are there material risk you believe we should consider for your sector?

Timeframes

The rules cannot be made until the Bill is passed and commences. Further, after passage of the Bill, the Minister cannot make any rules until a notice has been published on the Department's website that sets out the draft rules, and invites stakeholders to make submissions within 28 days after the notice is published. The Minister is required to consider any submissions received during the 28-day period before making the rules.

Over the next two months, the Department will work with industry to develop sector-specific rules for the electricity and gas sectors. A series of workshops will be held, commencing on 27 April. Questions raised in this paper will be discussed during the workshops.

We expect that the staggered co-design process will continue throughout 2021 and into 2022. Outcomes of this co-design will ensure that the Program obligations are tailored to the needs of each sector, and will uplift the security and resilience of Australia's critical infrastructure.

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.