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

In response to the worsening threat environment in which critical infrastructure operates, the Australian Government has proposed the Protecting Critical Infrastructure and Systems of National Significance reforms. As part of the reforms, 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 written Critical Infrastructure Risk Management Program (the Program).

The Program will require responsible entities of specified critical infrastructure assets to take an all-hazards approach when identifying, understanding, managing and mitigating risks. 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.

The Department of Home Affairs (the Department), with industry and government stakeholders, has completed co-designing sector-agnostic governance rules in March 2021. These rules will supplement the risk management program framework outlined in the Bill, setting out further requirements for responsible entities. A summary of key findings from the co-design workshops is available here.

We have now commenced co-designing sector-specific rules. The objectives of this process are to:

- ensure that there are rules in place for each sector that will drive an uplift in the security and resilience of critical infrastructure assets;
- consider making rules that will prescribe material risks for each sector.
- work with stakeholders to ensure that proposed rules are fit for purpose in their sectors; and
- assess whether there are existing regulations that meet the objectives of the Program and to reduce regulatory burden where possible.

Sector-specific rules

Government is determined to ensure that entities see security and resilience as an ongoing commitment, rather than a 'check-a-box' compliance exercise. In this regard, we assess that there is merit in developing sector-specific rules that will require responsible entities to implement mitigations in response to a range of hazards, including cyber, physical, natural, personnel and supply chain vectors.

Standards and principles-based rules

Sector-specific rules may be constructed by referring to existing standards or other regulations as appropriate. We recognise that there are many possible standards that industry use and follow as part of existing risk management processes. The sector-specific rules may leverage **standards** such as:

- maturity models (e.g. C2M2, AESCSF);
- international standards (e.g. ISO27001, IEC62443); and
- existing government frameworks (e.g. PSPF, ISM, ASD's Essential Eight).

We also recognise that there are sector and entity-specific differences in human and financial resources, technology, threats, existing standards and maturity, to name a few. In this regard, we also intend to draft rules around principles that will be underpinned by guidance and advice, proportionate to the risks and circumstances faced by each sector.

Principles-based rules will require responsible entities to achieve goals in a less-prescribed manner. This offers flexibility by providing a framework that guides responsible entities to identify key outcomes and objectives in their Program. Examples of principles-based rules are:

- ensuring active security measures are effective and appropriate to detect, deter, respond to and recover from breaches of security; and
- ensuring that the risk management program includes details of how the responsible entity manages risks arising from the off-boarding process for staff, contractors and subcontractors.

Rules may also reflect certain **outcomes** that responsible entities will be required to achieve as part of the Program. Examples of outcomes-driven rules are:

- minimising and mitigating relevant impact to assets arising from the supply chain;
- managing the risk of insider threats to the asset; and
- ensuring that critical employees undertake and pass a background check under the AusCheck scheme.

In specifying requirements in rules, the Minister of Home Affairs 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 intended through these reforms, we will seek to incorporate these regulations into the sector-specific rules where appropriate. Where entities are subject to a regulatory regime that partially addresses the outcomes being sought through these reforms, we intend to write rules in such a way as to allow entities to provide artefacts that have been developed or are used to satisfy those other regulatory obligations to satisfy the requirements of their Program.

Rules requiring responsible entities to mitigate risks in accordance with a standard or principle-based obligation will help ensure that an entity's Program is complementary and comprehensive.

Other examples of sector-specific rules can be found in Table 1 below.

Material risks

The Bill further provides for rules to be made that specify a risk to be a material risk. This would have the effect of requiring responsible entities to include that particular material risk in their Program, take steps to minimise the risk of the hazard occurring, and mitigate the

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

consequences should it occur. Examples of material risks that responsible entities may wish to consider as part of their risk management program include, but are not limited to:

- the loss of access to, or deliberate or accidental manipulation of position, navigation and timing systems;
- the storage, transmission or processing of sensitive operational information outside Australia;
- remote access to operational control or operational monitoring systems of the asset, in particular from outside Australia; and
- any action, including interception, alteration, deletion or sabotage, of data hosted, stored, processed or provided by the asset that may result in compromise of its confidentiality, integrity or availability.

We will use the co-design workshops to discuss potential material risk rules with each of the critical infrastructure sectors. The Department is seeking views from relevant stakeholders on what should be considered a material risk for the purpose of the Program.

It is important to note that specified material risks in the sector-specific rules will not be 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.

Table 1: Examples of standards rules and principles rules

Vector	Rule type	Examples rules
Cyber	Standards rules	Responsible entities for critical XX assets must, within YY months of the commencement of this rule, ensure that their risk management program includes mitigations that comply with Standard ZZ.
	Principles or outcomes-based rules	Responsible entities for critical XX assets must, within YY months of the commencement of this rule, ensure that their risk management program sets out how cyber hazards are being mitigated in a comprehensive and coordinated fashion.
Personnel	Standards rules	Responsible entities for XX assets must, within YY months of the commencement of this rule, ensure that their risk management program includes details of how the entity implements appropriate background checking of new and ongoing employees, contractors and subcontractors, having regard to Standard ZZ or an equivalent standard.
	Principles or outcomes-based rules	Responsible entities for critical XX assets must, within YY months of the commencement of this rule, ensure that their risk management program includes details of how the entity assesses and manages the ongoing suitability of its self-assessed critical employees, contractors and subcontractors.
Supply chain	Standards rules	Responsible entities for critical XX assets must, within YY months of the commencement of this rule, ensure that their risk management program includes details of how the entity complies with the business continuity components of Standard ZZ.
	Principles or outcomes-based rules	Responsible entities for critical XX assets must, with YY months of the commencement of this rule, demonstrate how their risk management program, as far as is reasonably practical, minimises and mitigates relevant impacts to the asset arising from the supply chain, including but not limited to:

		• unauthorised access, interference or exploitation; • privileged access; • disruption and sanctions; • threats to people, assets, equipment, products, services, distribution and intellectual property within supply chains; • high risk vendors; and • vendor dependency or reliance on entities inherently within supply chains.
Physical and Natural	Standards rules	Responsible entities for critical XX assets must, within YY months of the commencement of this rule, ensure that their risk management program includes details of how the entity: • detect and deters unauthorised access; • restrict, control and monitor access by unauthorised persons; and • control authorised access, including restricting access to only those persons with the appropriate approval who have an operational need to access, having regard to ZZ or an equivalent standard.
	Principles or outcomes-based rules	Responsible entities for critical XX assets must, within YY months of the commencement of this rule, demonstrate in its risk management program how it conducts tests, as appropriate, to ensure active security measures are effective and appropriate to detect, deter, delay, respond to and recover from breaches of security as self-assessed critical sites. Responsible entities for critical XX assets must, within YY months of the commencement of this rule, ensure that their risk management program sets out how the entity will, as far as is reasonably practicable, minimise or eliminate any material risk of and mitigate the relevant impact from a natural hazard or disaster on the asset,

		including but not limited to bushfires, floods, cyclones, storms, heatwaves, earthquakes, tsunamis and health hazards such as pandemics.

Questions for consultation

- What is your preference for the types of standards 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 or principles-based obligation 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 standard/principles-based obligations 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)?

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.

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 assistance 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.