Risk Management Program Rules

Questions, comments or concerns can be emailed to CI.Reforms@homeaffairs.gov.au

These draft rules are provided for the purpose of information. They should not be considered final drafted legal instruments.

Risk Management Program Rules

26 November 2021

Contents

Context Statement

1. On 29 September 2021 the Parliamentary Joint Committee on Intelligence and Security (the Committee) released its report and supporting recommendations regarding the Security Legislation Amendment (Critical Infrastructure) Bill 2020.
2. The Committee made 14 recommendations in relation to the Bill, including proposing a split into two amended bills:
    a. Bill One was introduced to parliament on 20 October 2021 and includes expanding the critical infrastructure sectors covered by the Security of Critical Infrastructure Act 2018, introducing government assistance to be used as a last resort measure as well as mandatory reporting obligations. The Bill as amended was passed by the Senate on 22 November 2021.
    b. Bill Two will include the declarations of systems of national significance, enhanced cyber security obligations and positive security obligations, which are to be defined in delegated legislation and will require responsible entities for one or more critical infrastructure assets to have, and comply with, a risk management program.
3. Before making or amending a rule, the Minister for Home Affairs must, among other things, have regard to any existing regulatory system of the Commonwealth, State or a Territory that imposes obligations on responsible entities. Many critical infrastructure sectors already have regulatory systems in place to sufficiently mitigate against threats sufficient to not warrant the development of a risk management program.
4. Where an existing regulatory system is not in place, there is a requirement to develop a risk management program.
5. A risk management program is designed to:
    - Identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset.
    - So far as it is reasonably possible to do so, minimise or eliminate any material risk of such a hazard occurring or mitigate the relevant impact of such a hazard on the asset.
6. At its core, a risk management program is designed to mitigate risks/hazards that can cause an impact on the functioning of critical infrastructure. For example:
    - a cyber attack resulting in prolonged outages of an electricity provider, a hospital ICU or a payments system;
    - a terrorist attack on a major liquid fuel pipeline or data centre;
    - infiltration and sabotage of a major water plant or taking down Australia's domain name systems, or
    - catastrophic failures in food and groceries and freight distribution chains due to a supplier with super user access to systems causing months long outage.

7. Obligations in Bill Two will require responsible entities to have a written risk management program would be switched on via rules which would include a grace period of at least six months from the making of the rules or 1 July 2022 whatever is latest.
8. These rules are structured by hazard vector only for the purposes of consultation, ease of discussion and costing.
9. Guidance material will be developed to support the implementation of these rules.

Data Hosting Certification

1. If a critical data storage or processing asset is 'Certified Strategic' under the Digital Transformation Agency's Hosting Certification Framework, then, for the purposes of storage of government data and data owned by critical infrastructure clients, that asset is taken to comply with all data storage or processing sector specific rules. Responsible entities for critical data storage or processing assets are still required to comply with data storage or processing sector-specific rules for facilities that are not 'Certified Strategic' under the Hosting Certification Framework, and are still required to comply with risk management program obligations under Bill Two.

Definition of Material Risk

1. Bill Two will require responsible entities to continue to identify and mitigate **material risks** that have a substantial impact on 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**.
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 information1 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.

[1] Sensitive operational information is information about the asset that includes **but is not limited to**:
a. layout diagrams;
b. schematics;
c. geospatial information;
d. configuration information;
e. operational constraints or tolerances information; and
f. data that a reasonable person would consider confidential or sensitive about the asset.

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.

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*[2] and/or *critical personnel*[3] 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[4] or an equivalent vetting check for *critical personnel*.
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 manages 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.

[2] 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.
[3] 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.
[4] Attachment A provides further information on the AusCheck scheme

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 how the entity seeks 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.

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 seeks to minimise and mitigate the relevant impact of physical and natural hazards for 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.
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.

Attachment A – AusCheck explanatory information

A background check under the AusCheck scheme can currently include some or all of the following:

- a security assessment conducted by the Australian Security Intelligence Organisation (ASIO);
- a criminal intelligence assessment undertaken by the Australian Criminal Intelligence Commission (ACIC) (note this is not authorised for any scheme other than the aviation and maritime security identification card (ASIC and MSIC) schemes);
- a criminal history check undertaken by the ACIC with results assessed by the Department of Home Affairs (the Department);
- an immigration and right to work check undertaken by the Department; and
- an identity verification check undertaken by the Department.

A review of an applicant's internet browsing history is never included in an AusCheck background check.

The level of assurance required under each check is yet to be determined, but it is likely that each critical infrastructure sector will be held to levels of assurance relevant to each sector. For example, there are different security relevant offences and assessment methodologies in the ASIC/MSIC schemes and the Major National Event scheme. Under the critical infrastructure scheme, critical infrastructure sectors will be able to co-design relevant background checks to treat their trusted-insider risks (criminal history check, security assessment, right to work check and verification of identity check) as part of their risk management program.

The Commonwealth Spent Convictions Scheme allows an individual not to disclose certain criminal convictions in particular circumstances (such as less serious offences), and prohibits unauthorised use or disclosure of information about the conviction. A conviction is considered spent if:

- it is old—it is 10 years since the date of your conviction (or 5 years if you were a child at the time of your conviction);
- it was minor—you were sentenced to no more than 30 months (2½ years) imprisonment (or you were not imprisoned at all);
- you have not re-offended during the 10 year waiting period (or 5 years if you were a child at the time of your last conviction); and/or
- an exclusion does not apply (for example, a scheme may mandate that a particular offence cannot be count as spent).

If an AusCheck background check determines a person to be ineligible to work in a security-sensitive role, the specific details of their criminal history will not be shared with their employer.

If a preliminary AusCheck assessment indicates an applicant is likely to be ineligible to work in a security-sensitive role, the applicant is always given all of the information supporting such a decision. The applicant always has an opportunity to make representations regarding the preliminary assessment, and AusCheck is required to consider any such representation prior to making any final assessment.

If an AusCheck background check determines a person to be ineligible to work in a security-sensitive role, the employer has the option of offering them employment in a role not requiring a background check.

An AusCheck background check is currently valid for two years. Consideration is being given to extending the duration of that validity period.

It is likely that any AusCheck scheme will require responsible entities, as well as any person holding an 'eligible' AusCheck background check, to inform the Department of any information which may adversely impact the AusCheck assessment. This would allow checks to be ongoing, rather than point in time. For example, should a person be convicted of a security-relevant offence they would be required to inform the Department of this, which could result in a reassessment of their background check.

Responsible entities do not collect information to provide to AusCheck. The employee will provide their own information to AusCheck, and the responsible entity will verify the employee has an operational need for a background check.

The Department is investigating the possibility of recognising both Australian and other government security clearances as part of this process. It is likely this will be developed as part of the AusCheck Regulations, rather than these risk management program rules.

An AusCheck background check for two-year ASICs and MSICs costs $92.50 per application. Actual costs for new critical infrastructure sectors will be confirmed through scheme design.

In the financial quarter leading up to 1 October 2021, AusCheck completed 61% of all background checks in 5 business days and 71% in 10 business days. Background checks which took longer than 10 business days were typically due to complexities in applicants' backgrounds, which needed to be resolved by ASIO and/or the ACIC.

Decisions made in the AusCheck scheme may be subject to review or appeal under the *Administrative Decisions (Judicial Review) Act 1997*, or by the Administrative Appeals Tribunal.