Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

ACTION ALERT
Risk Management
implementation and uplift

In light of the global situation, the Cyber and Infrastructure Security Centre **strongly recommends** that responsible entities for critical infrastructure assets consider your risk management measures at this time, particularly cyber and information security risk. If you don't have an adequate risk management program in place, then the CISC strongly advises that you develop one. If you do have one, then now is a good time to consider reviewing it. Such actions will provide you with an improved posture to protect your critical infrastructure assets.

Why is this alert being made?

The CISC recommends Australian organisations assess and improve their critical infrastructure resilience as good practice. While the CISC is not aware of any specific threats to Australian critical infrastructure organisations, adopting an enhanced risk posture will help to reduce the likelihood and impact of any risks that may be realised.

This alert draws on information derived from CISC partner agencies and industry sources.

What should I be doing now?

It is **strongly recommended** that responsible entities for critical infrastructure assets commence voluntarily implementing the obligations proposed in the draft risk management program rules under the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 that is currently before the Parliament.

It is **strongly recommended** that entities make themselves familiar with the 23 February 2022 ACSC advisory notice and secure their systems. Further information that is regularly updated is available at cyber.gov.au.

Entities should, where **possible**, work to identify, minimise and mitigate **material risks** which could affect their business and the continued delivery of goods and services. Entities should **urgently** work to identify and resolve risks that may affect the availability, integrity, reliability and confidentiality of their asset.

Cyber and information

- Where appropriate, the CISC **recommends** organisations commence implementation of the ACSC Essential Eight Maturity Model at level one or higher, or a similar cyber-security standard.
- Ensure your cybersecurity plan is up to date and actionable.
- If you have an incident response plan, initiate it – work to see if your systems have been compromised.
- Responsible entities for critical infrastructure assets should report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal.
- Follow **cyber.gov.au** for more information.

Personnel

- Work to identify your critical workers and positions, and commence a review to ensure that appropriate and suitable persons hold these positions.
- Review your planning around malicious insiders, negligent workers and off-boarding of staff.

Supply chain

- Initiate a review of your supply chain arrangements – are you still able to function should one of your suppliers cease to be available or there is a disruption to supply of your critical inputs?

Physical and natural

- Check to ensure your physical premises are secure.
- If possible, initiate an organisation wide reset of swipe or tap access cards or keys.

What if my asset won't be captured by the risk management program rules?

It is **strongly recommended** that all critical infrastructure assets undertake an **urgent** review and uplift of all security measures, particularly cyber security, regardless of if they would be required to implement a risk management program.

CONTACT US | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au