

File/Our Ref:
Your Ref:
Please quote in reply



By your side

18 November 2022

Minister for Home Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

By email: ci.reforms@homeaffairs.gov.au

Re: Risk Management Program consultation

The Australian Services Union (ASU) welcomes the opportunity to make a submission on the *Security of Critical Infrastructure Act 2018* Reforms – Draft Risk Management Program Guidance and Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022.

The ASU is one of Australia's largest Unions, representing approximately 135,000 employees. The ASU is the union for energy and water workers in Australia. The responsibility of providing electricity & gas (energy), and water/sewerage in our society falls on ASU members across the country. Their professionalism ensures continuity of services and in times of crises like natural disasters, they are often amongst the first responders.

The ASU participated in consultations and the inquiry into the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) which came into force on 3 December 2021, followed by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth) which came into force on 1 April 2022.

We support the principle that a responsible entity for an applicable critical infrastructure asset must have and comply with (unless an exemption applies) a Risk Management Program (RMP). We understand an RMP must identify material risks; minimise risks to prevent incidences; mitigate the impact of realised incidents and ensure effective governance.

Personnel hazards

Subsection 9(2) of the Rules provides that an entity must establish and maintain a process of system to identify critical workers and the suitability of a critical worker to have access to the critical components of an asset.

Subsection 9(3) of the Rules provides the process to consider the suitability of a critical worker may be a background check under the AusCheck scheme.

The Rules do not provide direct guidance for when and how often a background check is required. Nor do the Rules provide guidance on what a responsible entity must do with the data obtained from these extensive background checks.

There are also no protections in place to prevent employers from misusing workers' private information. Further guidance material is required in relation to these matters.

The ASU continues to be extremely concerned about the AusCheck scheme background check. The AusCheck scheme goes far beyond what is necessary to protect our critical infrastructure. It is a direct attack on our member's right to privacy. The AusCheck scheme puts too much power in the hands of employers to collect personal information about our members, without offering proper safeguards to prevent discrimination or to protect our members' personal information.

Case study - Powerlink

In Early 2021, Powerlink advised its workforce that it intended to conduct a 'digital footprint check' on employees. The purpose of this investigation was to find employees they deemed to have conducted 'adverse online behaviour' in preparation for the implementation of the AusCheck system.

The employer proposed a very broad definition of adverse online behaviour that went beyond the employee-employer relationship. Notably, Powerlink stated that it would seek out activity that suggested the employee was '*susceptible to, or easily succumbs to, groupthink or other conformity pressures*'. The only reason that Powerlink did not implement its proposal was as a result of a successful dispute by the Industry.

Case study - TransGrid

TransGrid is an electrical company operating in NSW. In 2021, Transgrid engaged an agency called My Verification Services in preparation of the Bill passing parliament. My Verification Services conducted highly invasive investigations of employees without their consent. This involved employees receiving phone calls at home on their private telephone numbers with regard to complying with the engagement of My Verification Services. Often, these phone calls were after-hours. Members reported significant distress at this level of harassment.

TransGrid told the ASU that it intended to apply the same standard to each cohort in the business. That would mean that an administrative officer would be subject to the same level of scrutiny as a frontline operator with access to secure or sensitive operational areas.


Further guidance material is required to limit and confine the list of critical workers so that the definition of who is a critical worker effects the least number of workers as possible and limits the relevant entity from adopting an expansive or a broad view of the definition, as highlighted in the above case studies.

Consistent guidelines

The Draft Risk Management Program Guidance states there is no template for developing an RPM with each critical infrastructure asset able to develop a program that is suitable to their business and operational needs.

A structured and consistent approach for recognising, understanding, and responding to risk is essential. An RPM framework should be developed by stakeholders of each sector (including unions) to assist critical infrastructure assets to identify, analyse and manage risks. The framework would establish an appropriate personnel and physical hazard risk management program for each sector.

Yours faithfully



Robert Potter
NATIONAL SECRETARY