



152 Miller Street, West Melbourne  
Victoria 3003, Australia

GPO Box 1272,  
Melbourne, Victoria 3001.  
[professionalsaustralia.org.au](http://professionalsaustralia.org.au)

1 February 2022

Department of Home Affairs

Email: [CI.Reforms@homeaffairs.gov.au](mailto:CI.Reforms@homeaffairs.gov.au)

### **Submission to Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022**

Professionals Australia is a registered union which represents over 20,000 professional employees across Australia, including engineers, managers, information technology professionals, architects, scientists, and pharmacists.

We believe many of our members will be impacted by the proposed changes in the Critical Infrastructure Protection (CIP) Bill, as they work across a diverse range of industries in both the public and private sectors including Roads, Rail, Water, Electricity, Information Technology, Cybersecurity, Healthcare, Aviation, Telecommunications, Laboratories, Research, Mining, Oil, Construction and Manufacturing.

While Professionals Australia is committed to protecting the security and resilience of critical infrastructure and systems of national significance, we also need to ensure the interests of professional employees working in these areas are protected within any new regulatory framework.


The following legislative amendments have implications for our members who are engaged in critical infrastructure sectors:

- Greater incident reporting obligations and the need to establish risk management programs. For the industries where this is a new and/or additional requirement, relevant professional employees will require appropriate industry cybersecurity/risk management training to fulfil this legislative requirement for their employer.
- A requirement for background checks for professionals who have privileged access to critical infrastructure systems and sensitive information systems. Where background checks are required, appropriate systems and protections will need to be put in place to ensure the cost and time involved in obtaining background checks is borne by the employer rather than employees. In addition, employers will need to ensure strong privacy and confidentiality measures are built around data obtained through background checks and that this information is not used to discriminate in employment.

We ask that these matters be given further consideration and would appreciate the opportunity to be further engaged in the development of the new regulatory framework to protect critical infrastructure and systems.

Please note that we are happy for our submission to be made public.

Yours sincerely

  
Jill McCabe  
Chief Executive Officer