

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



18 February 2021

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

By email: pjcis@aph.gov.au

**Re: Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and
Statutory Review of the Security of Critical Infrastructure Act 2018**

The Australian Services Union (ASU) welcomes the opportunity to make a submission on the *Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020* and *Statutory Review of the Security of Critical Infrastructure Act 2018*.

We note the proposed legislation expands the application of the *Security of Critical Infrastructure Act 2018* (SOCl). Currently the SOCl only applies to specific entities in the electricity, gas, water and maritime port sectors. The Draft Bill proposes to expand the application to the following critical infrastructure assets:

- communications;
- financial services and markets;
- data storage and processing;
- food and grocery;
- transport
- defence industry;
- higher education and research;
- energy (e.g. organisations involved in the production, distribution and supply of electricity, gas or fuel);
- healthcare and medical;
- space technology; and
- water and sewerage.

Of relevance to the ASU is the expansion to energy, water and sewerage sectors.

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 is deeply concerned how the drafted Bill will impact our members in energy and water.

The Australian Government, Security Legislation Amendment (Critical Infrastructure) Bill 2020 Explanatory Document provides an overview for each new critical infrastructure sector and critical infrastructure asset. Our members work for operators and providers in the following sectors:

Energy sector:

- Critical electricity asset
- Critical gas asset
- Critical liquid fuel asset
- Critical energy market operator asset

Water and sewerage sector:

- Critical water asset

The Draft Bill outlines how these assets may be subject to Positive Security Obligations and Enhanced Cyber Security Obligations. The Positive Security Obligations may require a critical infrastructure asset to report serious cyber security incidences. We are concerned about the potential for employers to use this Bill/Legislation to increase its cyber surveillance of employees under the guise of being able to report a serious cyber security incidence.

The Draft Bill also inserts legislation that provides “the ability for an AusCheck Scheme to be established in the regulations if the critical infrastructure risk management program requires background checking of individuals to be conducted under that scheme.”¹

“These provisions mean that sector-specific rules can be made as part of the critical infrastructure risk management program to require background checks to be conducted under the AusCheck Scheme for certain individuals or employees that are involved in the operation of, or have access to, critical infrastructure assets.”²

The ASU is extremely concerned about the new Cyber Security Obligations that allow for a critical infrastructure asset to be deemed a “system of national significance” and therefore required to lawfully comply with enhanced obligations including: incident response planning; cyber security exercises; vulnerability assessments; and access to system information.

Furthermore, we are extremely concerned about the AusCheck scheme background check that often involves an invasion of privacy for workers including the assessment of whether a person has a criminal history, their citizenship status, or if a worker has an adverse security assessment. Dependent on the nature of the information gathered, there is the potential for workers to be discriminated against by their employer. In addition, we are concerned the AusCheck scheme may be used as a general intelligence resource for use by an unspecified range of agencies.

The question must be asked: why should workers employed by critical infrastructure assets have lesser rights and privacy than other Australian workers? And why have these important issues not received any recognition or debate during this inquiry?

The ASU ascribe to a strong sense of civil liberties and the privacy rights of workers and we believe the Bill in its current form compromises these rights.

¹ Australian Government, Security Legislation Amendment (Critical Infrastructure) Bill 2020 Explanatory Document [Online] Accessed at: <https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf>

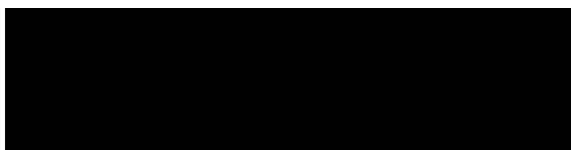
² Ibid.

In addition, the Draft Bill, the Explanatory Memorandum and the Statement of Compatibility with Human Rights have no detail as to how workers will be impacted by this proposed legislation. This is completely unacceptable given the millions of workers who will be affected.

Finally, we note the short timeframe for the review of this important legislation and protest the inadequate time provided for consultation with our broad membership. We believe the Committee should extend the length for consultation with key stakeholders, particularly affected workers, to allow proper debate on the scope of the Draft Bill.

In conclusion, the ASU believes the proposed *Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020* should be rejected.

Yours faithfully



Robert Potter
NATIONAL SECRETARY