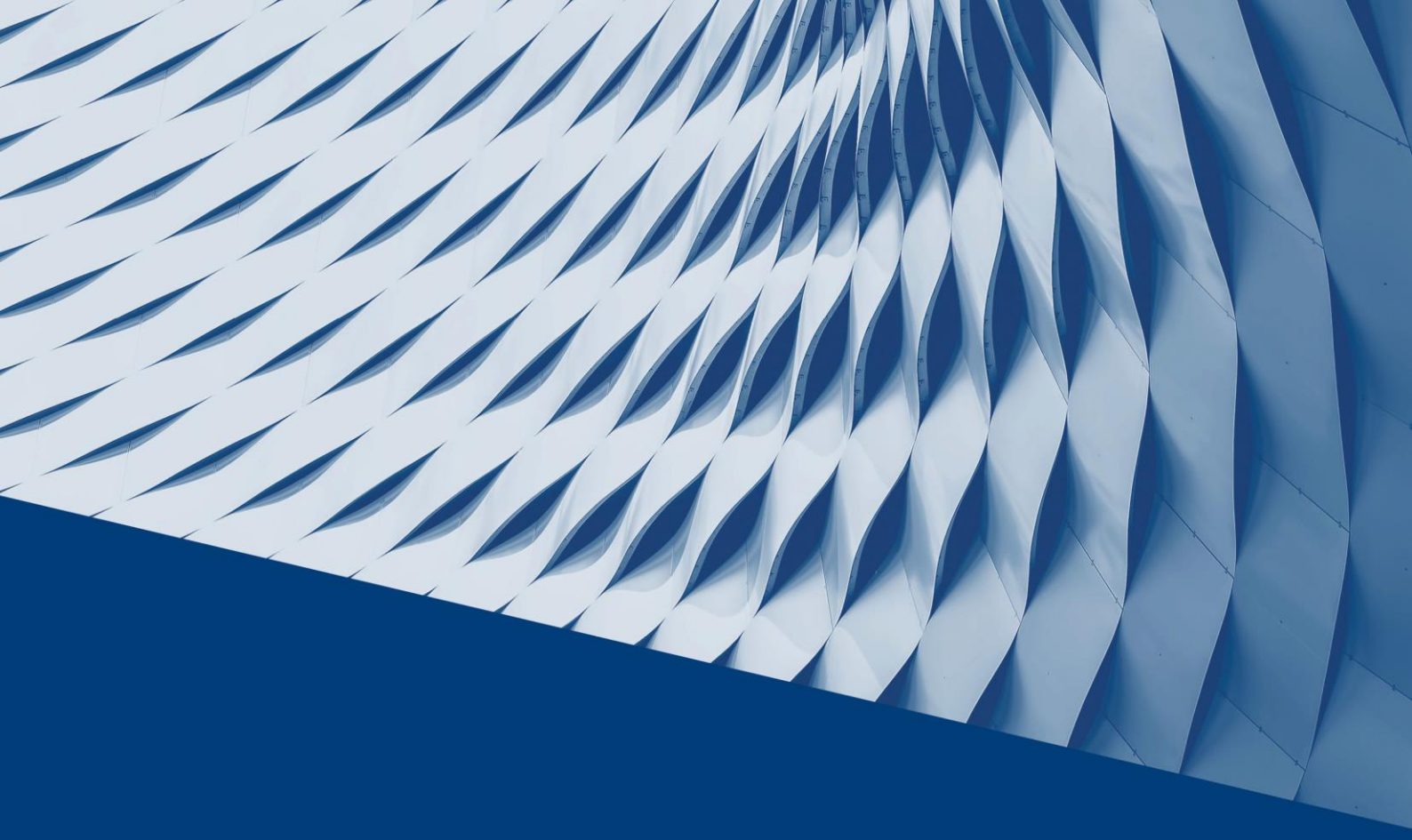

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022. Exposure Draft

Submission by the Australian Council of Trade Unions to the Department of Home Affairs Inquiry

ACTU Submission, January 2022
ACTU D. No 00/2022

ACTU
australian council of trade unions

Contents

1. Introduction

The Australian Council of Trade Unions (ACTU) represents 43 affiliated unions who together represent over 1.5 million members.

The ACTU and Australian Unions are strong supporters of measures to ensure that Australia's essential services are secure and resilient. The failure to strengthen our critical supply chains and to keep workers safe during the current Omicron crisis has exacerbated a national public health crisis.

The measures put forward in the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022,* ("the Bill") however are an unnecessary intrusion into the civil liberties and workplace rights of a potentially vast number of Australia workers. Among other measures, the Bill will require managers of assets in "critical infrastructure sectors" to develop, implement and update "critical infrastructure Risk Management Plans". Those plans will need to identify and take steps to minimise, mitigate against and eliminate risks to those assets. The detail of such plans are to be determined both by the relevant entities, and rules yet to be issued by the relevant Minister, usually on an industry or sectoral basis. The Bill also includes the ability for Rules to be made to allow employers to conduct background checks of staff or other personnel, via AusCheck as part of such a plan.

The ACTU has significant concerns with this Bill.

Firstly, it is a significant intrusion into the privacy and civil liberties of a very broad range of workers – up to 3 million workers are potentially covered by these changes on ACTU estimates - and the Minister has the power under the proposed Bill to expand this scope even further. Yet almost no evidence has been provided by the Government to justify such broad and intrusive measures.

Secondly, it could also potentially interfere with the workplace rights of workers and their union representatives. Unions have already had employers stating that they will effectively frustrate the right of entry to union officials on the basis of complying with these proposed laws. The laws could also impinge upon privacy, anti-discrimination and work health and safety laws.

Thirdly, the Bill creates substantial levels of delegated decision making to both employers and the relevant Minister on highly significant issues with limited or no worker (or union) right to consultation, negotiation or review and limited parliamentary oversight.

This submission provides more detail on each of these concerns.

To address these concerns the ACTU recommends that the Bill be amended to:

1. Improve transparency and certainty of the law by removing the substantial levels of delegated decision-making within the Bill and restoring effective parliamentary oversight.
2. Ensure that decisions made under the Bill are reviewable by the Administrative Appeals Tribunal.
3. Define and tightly limit the class of "critical employees" or other "critical personnel" subject to possible background checks to ensure that the right to privacy and other civil liberties are not unnecessarily impinged upon. Also put in place safeguards to prevent unwarranted, excessive or unnecessary background checks.
4. Legislate for mandatory consultation with employees and their union representatives if an entity is considering implementing background checks.
5. Put in place an appeal mechanism to an independent mediator for workers and their representatives to challenge an entity's Risk Management Plan on the grounds that it breaches any safeguard in recommendation 3.
6. Amend the Bill to ensure that rights under industrial, work health and safety, privacy or anti-discrimination laws are not in any way restricted.
7. Ensure that citizen's private data that may be accessed under the Bill is quarantined from employers.

2. Background

The ACTU and broader trade union movement opposed the initial Security Legislation Amendment (Critical Infrastructure) Bill 2020 due to its unreasonable requirement to subject workers in a large number of industries to invasive and unnecessary security assessments.[1]

[1] Australian Council of Trade Unions, Submission on the Security Legislation Amendment (Critical Infrastructure) Bill 2020, 21 February 2021 https://www.aph.gov.au/DocumentStore.ashx?id=3ddb7a9e-ac07-467d-a2f8-09cc8b1e8266&subId=702957 ; Australian Council of Trade Unions, 'D34 - Critical Infrastructure: Supplementary Submission by the Australian Council of Trade Unions to the Parliamentary Joint Standing Committee on Intelligence and Security Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020', 2021.

This Bill was passed on 2 December 2021 with significant amendments based on the recommendation of the Parliamentary Joint Committee on Intelligence and Security (PJCIS). Among many other provisions, the requirement for employers to conduct security assessments of their employees was repealed and the PJCIS recommended the Government reconsult on the contentious provisions of the Bill with a view to introducing it as a separate Bill later.
While security assessments for workers were excluded under the legislation passed, the Bill did introduce a broad list of critical infrastructure sectors for the purposes of legislating additional powers and requirements in the second Bill. These critical sectors include:

- Communications,
- Data storage or processing,
- Financial services and markets,
- Water and sewerage,
- Energy,
- Health care and medical,
- Higher education and research,
- Food and grocery,
- Transport,
- Space technology, and
- Defence industry.

The following assets or businesses are defined as 'critical infrastructure assets'[2], subject to rules prescribed by the Secretary of Home Affairs: Telecommunications, Broadcasting, Domain name system, Data storage or processing, Banking, Superannuation, Insurance, Financial market infrastructure, Water, Electricity, Gas, Energy market operator, Liquid fuel, Hospital, Education, Food and grocery, Port, Freight infrastructure (including roads), Freight services, Public transport, Aviation or Defence Industry.

The ACTU estimates more than 3 million workers are now designated to work in 'critical infrastructure assets.'[3] NB: There is no upper limit on those captured by the Bill should it include those who work or use roads or road networks which are 'critical freight infrastructure assets.'[4]

---

[2] *Security of Critical Infrastructure (SOCI) Act* s 9(1)(a)-(f).
[3] Australian Council of Trade Unions, 'D34 - Critical Infrastructure: Supplementary Submission by the Australian Council of Trade Unions to the Parliamentary Joint Standing Committee on Intelligence and Security Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020', 2021.
[4] *SOCI Act* s 12B (1)(a), s 12B (2)(a).

The rule-making power under the Act also allows the Government to expand the scope by including additional 'critical infrastructure' entities, groups or classes of entities, or sectors.

3. The Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Under the proposed Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, managers or operators of Critical Infrastructure Assets would be required to develop Risk Management Programs which must:

- Identify hazards to the 'availability, integrity, reliability or confidentiality of the asset'[5],
- Identify which of these hazards are 'material' to the 'availability, integrity, reliability, or confidentiality'[6] of the asset with reference to its likelihood and impact on the asset,
- Identify and take steps to minimise, mitigate, or eliminate the risk.

While the scope and content of a Risk Management Program is deliberately vague, the Explanatory Document to the Exposure Draft outlines an intention for accompanying Ministerial Rules to be developed that would require responsible entities to consider and address risks in these four areas:

- Physical security and natural hazards,
- Cyber and information security hazards,
- Personnel security hazards, and
- Supply chain hazards.[7]

According to the explanatory document, "Personnel security hazards" refers to the 'insider threat' or the risk of employees exploiting their legitimate access to an organisations' assets for unauthorised purposes including corporate espionage and sabotage. Further, **"**Supply chain hazards" refers to entities exploiting their legitimate access to, or control of, an organisations'

[5] Department of Home Affairs, 'Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022' (Commonwealth of Australia, 2021), p. 13 <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/exposure-draft-security-legislation-amendment-ci-protection-bill-2022> [accessed 16 December 2021].
[6] Department of Home Affairs, 'Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022', p. 13.
[7] Department of Home Affairs, 'Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022', p. 14.

assets for unauthorised purposes or otherwise creating a cascading impact to dependent assets."[8]

Risk Management Plans are required to be held by the entity but are not required to be submitted for assessment by the Department. They can be examined and reviewed by the Department to ensure its suitability, and rules may be issued by the Department to an entity, sector or class of entities requiring particular steps entities will need to take through their Risk Management Plans.

4. Background Checks

Section 30AH(4) of the Bill enables the Secretary or Minister to issue rules to a critical infrastructure sector, asset or Government entity to conduct background checks on its employees or personnel through the AusCheck Scheme as follows:

> "Rules made for the purposes of paragraph (1)(c) may require that a critical infrastructure risk management program include one or more provisions that permit a background check of an individual to be conducted under the AusCheck scheme."[9]

To further enable this, the Bill also amends the *AusCheck Act 2007* to enable entities with 'Critical Infrastructure Risk Management Plans' to conduct background checks under the AusCheck Scheme.[10]

This could enable an employer to require an employee to undergo an AusCheck assessment and then let the employer know if the employee has an adverse criminal history or security assessment.[11]

The Explanatory Document says this will not be a mandatory background check for staff in critical infrastructure. Nor is it to be used as a justification for excessive and unwarranted background checking of staff,' and should apply only to individuals the entity considers 'critical.'[12] The Bill, however, contains no provisions defining or preventing 'unwarranted' or 'excessive' background checks. Nor does it define who a "critical employee or personnel" might be.

---

[8] Department of Home Affairs, 'Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022', p. 14.
[9] Department of Home Affairs, 'Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022' (Commonwealth of Australia, 2021) Schedule 2 s 30AH(4).
[10] Department of Home Affairs, 'Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022' Schedule 1 s1 - 2.
[11] https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/crime-prevention/auscheck
[12] Department of Home Affairs, 'Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022', p. 15.

These ambiguities, along the vague scope of Risk Management Plans, means that the assessment of whether or not background checks are necessary lies nearly entirely with the employer. Without clear protections in place the process of background checking is open to significant abuse by employers.

5. Concerns with the Bill

Disproportionate and excessive scope

The ACTU estimates that up to 3 million workers are currently covered under definitions of "critical infrastructure" under these Bills and hence potentially subject to a background check. The Minister will also have the power to expand the coverage of these laws even further. This represents a massive, unjustified and unnecessary intrusion into the privacy and civil liberties of a large part of Australia's workforce.

Excessive employer discretion

Most of the discretion for conducting background checks lies with employers. Further, under the proposed laws, the Government may mandate a Risk Management Plan which requires unreasonable background checks to be conducted for its workers. Managers of critical infrastructure assets may calso reate a Risk Management Plan which requires unreasonable background checks of its staff.

No safeguards to prevent abuse

There are no safeguards in the Bill to prevent such abuse. There is no prohibition on 'unwarranted' or 'excessive' use of background checks on staff in the Bill, despite such comments in the explanatory document to the Bill. Similarly, there is no definition of who are "critical employees" or "critical personnel" in the Bill.
The supply chain risk assessment is a self-assessment, and employers or operators may be selective on the implementation of background checks. This is already the case in shipping, where background checks are conducted only on Australian-flagged seafarers.

Potentially impinging on workplace rights.

Such background checking risks interfering with a range of individual and workplace rights, including under privacy, discrimination, workplace relations and work health and safety laws. Key examples highlighting these concerns are employers:

- Using background checks as a way to frustrate the right of entry of a union organiser to enter a workplace. This further interferes with the right to freedom of association for workers. The ETU and ASU reported that employers were already conducting security

assessments, refusing to enter into good faith bargaining and threatening the right of entry of union officials based on the imminent passage of the 2021 predecessor to this legislation.

- Being tempted to discriminate against an employee or prospective employee for holding a criminal record, despite the record not being relevant to the employment. Further, a worker could be effectively excluded from their profession if they fail a security assessment with one employer, and all employers in the industry are subject to the same rules.
- Identifying "Hazards" and the steps that take to minimise, mitigate or eliminate such hazards could also interfere with the rights of workers under workplace laws to take protected industrial action, or to take action under work health and safety laws.
- Using background checks as a way to victimise or unfairly single out particular employees.

Untransparent and unaccountable rule making.

The Bill creates substantial levels of delegated decision making on highly significant issues. Firstly it empowers the Minister to make Rules in a wide range of areas. Secondly, employers have significant scope to determine the nature of their critical infrastructure plans. Unions will have limited or no rights to consultation or ability to bargain and negotiate to either the development of rules or the requirements of critical infrastructure plans.

For example, Risk Management Plans are unlikely to be a matter which trade unions can assist with developing, limiting the recourse for employees to challenge an unreasonable or excessive instantiation of background checking. There is also no mechanism for staff subject to a Risk Management Plan developed by an employer or mandated by the Department to appeal the imposition of background checks.

There is also limited parliamentary oversight. Many of the issues the plans many impinge upon are about fundamental rights that should be clearly protected in primary legislation.

Finally, the AusCheck Scheme is already incredibly slow. This Bill does not provide for additional resources given very large increase in checks likely.

6. Recommendations

To correctly the deficiencies identified with this Bill the ACTU makes the following recommendations:

1. Improve transparency and certainty of the law by removing the substantial levels of delegated decision-making within the Bill and restoring effective parliamentary oversight.
2. Ensure that decisions made under the Bill are reviewable by the Administrative Appeals Tribunal.
3. Define and tightly limit the class of "critical employees" or other "critical personnel" subject to possible background checks to ensure that the right to privacy and other civil liberties are not unnecessarily impinged upon. Also put in place safeguards to prevent unwarranted, excessive or unnecessary background checks.
4. Legislate for mandatory consultation with employees and their union representatives if an entity is considering implementing background checks.
5. Put in place an appeal mechanism to an independent mediator for workers and their representatives to challenge an entity's Risk Management Plan on the grounds that it breaches any safeguard in recommendation 3.
6. Amend the Bill to ensure that rights under industrial, work health and safety, privacy or anti-discrimination laws are not in any way restricted.
7. Ensure that citizen's private data that may be accessed under the Bill is quarantined from employers.

address

ACTU

Level 4 / 365 Queen Street

Melbourne VIC 3000

phone

1300 486 466

web

actu.org.au

australianunions.org.au