

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Submission by the Australian Council of Trade Unions to the
Parliamentary Joint Committee on Intelligence and Security
inquiry into Security Legislation Amendment (Critical
Infrastructure Protection) Bill 2022

ACTU Submission, 1 March 2022
ACTU D. No 08/2022

Contents

Introduction	1
Recommendations.....	2
1 Background.....	3
2 Consultation and transparency.....	4
3 Background checks	5
4 Impinging on workplace rights.....	7
5 Risk of overcompliance	9
6 Untransparent and unaccountable rule making.....	9
Recommendations.....	10
References	0

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.

This submission draws and builds upon the ACTU Submission to the Department of Home Affairs (Home Affairs, the Department) the Exposure draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*, ("the Bill"), and reiterates concerns with the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* the Bill is based on which have not been addressed.

The ACTU has significant concerns with this Bill and is not satisfied that the Department of Home Affairs adequately followed the instruction of this Committee, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to ensure primary and secondary legislation have been co-designed with industry and incorporate the suggestions by, among others, trade unions.

The Bill represents a significant infringement of the right to privacy and civil liberties enjoyed by Australians today. At least three million workers are potentially covered by these changes and the Minister would gain the power to expand this even further. The Government have not provided evidence to support this significant expansion of background checks, especially in a range of industries and some named occupations.

The Union movement has further concerns that the Bill could interfere with the workplace rights of workers and their union representatives. This Committee has already heard evidence that some employers are using the spectre of this Bill in bargaining and had prepared to conduct their own background checks on employees. Under this Bill employers could frustrate the right of entry of union officials on the basis of complying with these proposed laws, and could impinge on rights afforded under work health and safety, anti-discrimination, and privacy laws.

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 (nor union) right to consultation, negotiation or review and limited parliamentary oversight. The concern this

Committee raised of significantly delegated legislation with an unquantified impact on business and workers has not been addressed.

The submission will elaborate upon these concerns in detail.

Recommendations

1. The Committee reiterate its recommendation to the Department of Home Affairs to conduct meaningful consultation with concerned stakeholders on non-urgent parts of the Bill and return to the Committee with an appropriately amended Bill.
2. Improve transparency and certainty of the law by removing the substantial levels of delegated decision-making within the Bill and restoring effective parliamentary oversight.
3. Ensure that decisions made under the Bill are reviewable by the Administrative Appeals Tribunal.
4. Define in primary legislation and tightly limit the class of “critical worker” 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 legislated safeguards to prevent unwarranted, excessive, or unnecessary background checks.
5. Legislate for mandatory consultation with employees and their union representatives if an entity is considering implementing background checks.
6. 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 4.
7. Amend the Bill to ensure that rights under industrial, work health and safety, privacy or anti-discrimination laws are not in any way restricted.
8. Ensure that person’s private data that may be accessed under the Bill is quarantined from their past, current, or future employers.

1 Background

The ACTU and broader trade union movement opposed parts of the Critical Infrastructure Bill 2020 due to its broad and uncalculated impact on a large number of workers and workplaces.

The provisions passed in the Bill to deem the sectors 'critical infrastructure sectors'¹:

- 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 north of 3 million workers are now designated to work in 'critical infrastructure assets.'³ There is no upper limit on those implicated into the Bill should we include those who work or use roads or road networks which are 'critical freight infrastructure assets.'⁴

The union movement raised concerns that the original Bill would unnecessarily diminish workers' rights, civil liberties, and have an unquantifiable impact on industry by potentially requiring more the three million workers to undergo background checks in order to continue working in their industries.

¹ Commonwealth of Australia, *Security of Critical Infrastructure Act 2018, 2021* s 8D(a)-(k).

² Commonwealth of Australia 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 Commonwealth of Australia s 12B (1)(a), s 12B (2)(a).

2 Consultation and transparency

The introduction of this Bill to parliament days after the conclusion of the formal consultation period of the exposure draft should be a primary indicator to the Committee that meaningful consultation has not taken place, and concerns the Union Movement raised regarding the proportionality, impact on human rights, and potential breadth of the Bill have not been ameliorated. In its advisory report, the Committee recommending splitting the Bill into ‘urgent’ and ‘non-urgent’ component parts⁵, in particular to address deficiencies highlighted by stakeholders including business and the Union movement.

Given these provisions were accepted to be non-urgent by this Committee and the Minister when they moved to amend the Bill to allow passage of more urgent amendments, there is no justification for the speed at which the Government moved to reintroduce this to Parliament. The rapid reintroduction of the Bill undermines the Committee’s recommendation that co-design take place before the Bill is introduced to ensure Parliament has a full transparency of the impact of the law that is being considered.

Relatively few consultation meetings have taken place compared to the scope of the Bill with concerned stakeholders since the publication of the exposure draft and the Bill’s introduction to Parliament, with few opportunities to meaningfully change the Bill. The exposure draft, too, is not meaningfully different to the Bill presented to parliament demonstrating that the consultation process was not taken seriously by the Department of Home Affairs. This is in direct contradiction of the recommendations of this Committee.

The Department does not appear to have taken seriously the human rights and workers’ rights concerns raised by the Union movement and is instead relying on consultation, exclusively with asset owners and operates, to furnish its record of consultation. Concerns raised by the Union movement with respect to possible contravention of workplace rights are not reflected in the Bill, the incomplete draft Rules, nor the Explanatory Memorandum.

The Committee should insist that the Government reconsider the Bill and engage in meaningful co-design of the rules and consideration of amendments to the primary legislation with the union movement to ensure that workers rights and civil liberties are not undermined due to a false sense of urgency.

⁵ Parliamentary Joint Committee on Intelligence & Security, *Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018* (Canberra: Commonwealth of Australia, 29 September 2021) Recommendations 1 & 7.

3 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.”⁶

To enable this, the Bill also amends the AusCheck Act 2007 to allow entities with ‘Critical Infrastructure Risk Management Plans’ to conduct background checks under the AusCheck Scheme. The Department has a stated objective and has drafted rules to ‘enable’ businesses to access the AusCheck regime as ‘industry is best placed to determine what the ‘critical workers’ in their business are’.⁷ By gifting business owners and operators the power to determine what a critical worker is, even in the confines of the rules, would severely undermine workers’ rights to privacy. As outlined in evidence submitted to the Committee previously, the Union movement has raised concerns that some businesses have sought to subject their entire workforce to background checks. In consultation with the Department, the Union movement saw that based on their internal definitions an apprentice linesperson would be subject to a background check.

The definition of critical worker offered in the draft rules is insufficient protection against unnecessary background checks or abuse of the system. That the entity can deem someone a critical worker undermines the purpose of the definition, particularly as there is no reasonable pathway for workers to challenge their deeming a *critical worker* and being subject to background checks.

Definition of Critical Worker

“**critical worker** means an individual, including a position holder:

- (a) who is an employee, intern, contractor or subcontractor of an entity; and
- (b) whose absence or compromise would prevent the proper function of the asset or could cause significant damage to the asset, as assessed by the entity; and

⁶ Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, 2022 s30AH (4).

⁷ Department of Home Affairs, ‘Department of Home Affairs Submission into the Review of Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022’ (Commonwealth of Australia, 2022), p. 11.

- (c) who has access to, or control and management of, a critical component of a Part 2A asset.”⁸

Under this definition, anyone the entity employs could be considered a *critical worker*. Indeed, it would be difficult for an employer to justify employing someone or engage a class of employees “whose absence would not prevent the property functioning of the asset”. If the employee is not there to ensure the proper functioning of an asset, why are they there?

Worse, the Government has neglected to define what a critical component is. The incomplete rules state, “**critical component** means an asset, part of an asset or system that <TBA>.”⁹ While the Department is not expected to publish its rules describing “TBA” as a critical component, the ambiguity means that Home Affairs has no idea how to determine a critical component and Parliament has no transparency as to the impact of the Bill. The definition could be incredibly broad, left up to employers or simply excluded for expediency. This omission further emphasises that the Government is simply not ready to rush this Bill through Parliament if key definitions within the rules are *published* as “TBA.”

Once the determination of a critical worker for an individual or position has been made in the risk management plan, that worker nor the workforce have grounds to challenge it should it be unreasonable – as was a goal of the Department of Home Affairs. The original 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.’¹⁰

This objective, however, was dropped in the published Explanatory Memorandum and neither the Bill nor rules contain provisions defining or preventing unwarranted or excessive background checks. This significant delegation of authority to employers opens up the system to abuse.

The definition of critical worker should be strengthened and placed in primary legislation, and supplemented with safeguards to prevent the unnecessary, unwarranted, or excessive use of background checks.

⁸ Department of Home Affairs, ‘Department of Home Affairs Submission into the Review of Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022’ Exposure Draft Rules, definitions.

⁹ Department of Home Affairs, ‘Department of Home Affairs Submission into the Review of Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022’ Draft Rules, 3 Definitions.

¹⁰ Department of Home Affairs, ‘Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022’ (Commonwealth of Australia, 2021), p. 15
<<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].

Both unions and industry raised concerns with the potential regulatory cost of the Bill. The Department has provided an extremely high-level outline of the expected costs per entity, which are quite high and justified to be so against the cost of an incident. Industry should be concerned at the lack of detail in these costings, and that they are presented in a way which doesn't allow for comparison of expected values. The expected costs of incidents should be weighted by the likelihood of occurring, to measure the impact of the costs of the law more meaningfully.

A further concern to unions is that the expected costs of background checks is not estimated. The cost of an MSIC card can be \$400 and several weeks of lost productivity waiting for the card to be approved. Should industries at large be expected to implement background checks, the Government has not explained who bears the cost of those background checks – workers or their employers? This is not even considering the myriad problems workers seeking to renew their MSIC and ASIC cards face with constantly changing assessment criteria and background check depth.

4 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.
- Preventing the ability for workplace health and safety representatives or even officials from entering a worksite to conduct a safety assessment if that person does not have a background check.
- 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.

Further potential ways the bill could imperil workers’ rights is in the definition of material risks and personnel hazards. The definition of material risks is so broad that it could encapsulate any industrial action. A material risk is defined as

- ‘a stoppage or major slowdown of the asset’s function for an unmanageable period’ or
- ‘a substantive loss of access to, or deliberate or accidental manipulation of, a critical component of the asset;’ or
- ‘Any other material risks as identified by the entity that affect the functioning of the asset.’¹¹

These definitions can and may likely be required by employers to prevent industrial action by the workforce under risk management plans, as a ‘personnel hazard.’ In response to a protected action ballot lodged by workers in NSW, Endeavour Energy cited the 2020 Bill as evidence for why extended notice periods should be given – limiting workers’ rights to take industrial action.¹² No protections exist in the Act to ensure workers’ rights and civil liberties are protected to erosion under this act.

Such restrictions listed above are likely to be in breach of International Labour Organization (ILO) Core Conventions, to which Australia is a signatory. These conventions set the minimum rights and conditions expected of workers internationally, and breaches of such conventions are rare in the developed world but are increasingly common under the Coalition Government. The ILO allows for exemptions for the right to strike in exceptional circumstances or for ‘essential services.’ Essential services are tightly defined as “those the interruption of which would endanger the life, personal safety or health of the whole or part of the population.”¹³ This definition, particularly for a food secure, developed nation is incredibly limited. However, this bill,

¹¹ Department of Home Affairs, ‘Department of Home Affairs Submission into the Review of Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022’ Exposure Draft Rules, 4 Material risk (a)-(g).

¹² *Public Hearing of Inquiry into Security Legislation Amendment (Critical Infrastructure) Bill 2020* (Parliament House, Canberra), p. 27.

¹³ International Labour Organization, ‘Labour Legislation Guidelines’

<<https://www.ilo.org/legacy/english/dialogue/ifpdial/lgl/noframes/ch5.htm>> [accessed 18 February 2022].

with the proposed definitions, would place similar preventions on a host of industries which do not meet such a definition.

5 Risk of overcompliance

It is clear that the intention of the Bill is to raise the minimum level of preparedness and risk mitigation of critical infrastructure entities but is failing to ensure that this does not result in overcompliance which may result in unnecessary and disproportionate risk management plans from employers. As raised by the Australian Services Union and the Electrical Trades Union in submissions at the public hearing, in anticipation of the passage of the 2020 Bill, Powerlink enacted plans to conduct digital footprint checking and background checks on the vast majority of its workforce.¹⁴ This was replicated by Transgrid, which also began conducting background checks on its employees in preparation for the Bill's passage. There was no consultation on who should be background checked, with the employers determining anyone with access to the worksite should be subject to background checks.

Employers informed unions that past offences for drink driving, errant *liking* of a Facebook page could be sufficient to fail a background check despite neither posing a reasonable risk to the asset.¹⁵ The intention of these employers is representative of a concern the union movement has for employers taking a maximalist approach to complying with the proposed laws. There is nothing preventing employers from being extremely heavy handed in their determination of who should receive background checks, the nature of their risk management plans and how they might interact with other laws.

Many industries and workers are already subject to background checks, fit and proper person assessments, police checks and even medical history checks. The Department has suggested that in the design of Risk Management Plans, some existing procedures will be sufficient to satisfy assessments by employers in mitigating personnel hazards. However, the Department has not suggested that employers could be *restricted* from increasing their surveillance of workers in response. In the healthcare setting, unions are concerned that healthcare professionals like nurses could be subjected to even more invasive checks as hospitals implement new Risk Management Plans in response to the laws.

6 Untransparent and unaccountable rule making.

¹⁴ Public Hearing of Inquiry into Security Legislation Amendment (Critical Infrastructure) Bill 2020, p. 26.

¹⁵ Public Hearing of Inquiry into Security Legislation Amendment (Critical Infrastructure) Bill 2020, p. 31.

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. As outlined by the Committee it is essential that the Parliament have as much clarity as possible about the impact of the proposed law they are seeking to enact. As no risk management plans have been developed, nor industry-wide rules have been deployed, it is impossible for the Parliament to reasonably assess the impact of the Bill.

Finally, the AusCheck Scheme is already incredibly slow. This Bill does not provide for additional resources given very large increase in checks likely. It is not clear the employment status of workers waiting for their background check to clear the scheme.

Recommendations

1. The Committee reiterate its recommendation to the Department of Home Affairs to conduct meaningful consultation with concerned stakeholders on non-urgent parts of the Bill and return to the Committee with an appropriately amended Bill.
2. Improve transparency and certainty of the law by removing the substantial levels of delegated decision-making within the Bill and restoring effective parliamentary oversight.
3. Ensure that decisions made under the Bill are reviewable by the Administrative Appeals Tribunal.
4. Define in primary legislation and tightly limit the class of “critical worker” 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 legislated safeguards to prevent unwarranted, excessive, or unnecessary background checks.

5. Legislate for mandatory consultation with employees and their union representatives if an entity is considering implementing background checks.
6. 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.
7. Amend the Bill to ensure that rights under industrial, work health and safety, privacy or anti-discrimination laws are not in any way restricted.
8. Ensure that person's private data that may be accessed under the Bill is quarantined from their past, current, or future employers.

References

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

Commonwealth of Australia, *Security of Critical Infrastructure Act 2018*, 2021

Department of Home Affairs, 'Department of Home Affairs Submission into the Review of Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022' (Commonwealth of Australia, 2022)

—, 'Explanatory Document - Exposure Draft Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022' (Commonwealth of Australia, 2021)
<<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]

International Labour Organization, 'Labour Legislation Guidelines'
<<https://www.ilo.org/legacy/english/dialogue/ifpdial/llg/noframes/ch5.htm>> [accessed 18 February 2022]

Parliamentary Joint Committee on Intelligence & Security, *Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018* (Canberra: Commonwealth of Australia, 29 September 2021)

Public Hearing of Inquiry into Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Parliament House, Canberra)

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, 2022

\

address

ACTU
Level 4 / 365 Queen Street
Melbourne VIC 3000

phone

1300 486 466

web

actu.org.au
australianunions.org.au

