Electrical Trades Union of Australia
Proud to be Union

1st March 2022

Committee Members
Parliamentary Joint Committee on Intelligence and Security

By email: pjcis@aph.gov.au

ETU Submission to the PJCIS Inquiry into the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

The Electrical Trades Union of Australia ('the ETU') is a division of the Communications, Electrical and Plumbing Union ('the CEPU').[1] The ETU is the principal union for electrical and electrotechnology tradespeople and apprentices in Australia, representing well over sixty-one thousand workers around the country. The CEPU represents close to one hundred thousand workers nationally, making us amongst the largest trade unions in Australia.

In the spirit of reconciliation, the ETU acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

The ETU welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the 2022 Bill) and would appreciate the opportunity to appear at a future public hearing of this inquiry.

The ETU is aware of the Australian Council of Trade Unions submission to this inquiry and supports the content and recommendations contained therein.

The Department of Home Affairs (DoHA) did not follow the instruction of the PJCIS to ensure all levels of the proposed legislation were co-designed with industry stakeholders, nor did they incorporate suggestions, concerns or proposals from stakeholders, including, among others, trade unions.

The Bill continues to represent an infringement on 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 has not provided evidence to support this significant expansion of background checks, especially in a range of industries and some named occupations.

[1] CEPU is a registered organisation under the *Fair Work (Registered Organisations) Act 2009* (Cth).

[Type here]

The 2022 Bill continues to apply multiple levels of delegated decision making to both employers and the relevant Minister on highly significant issues with limited or no worker right to consultation, negotiation, or review and with limited parliamentary oversight. The concern this Committee raised of significantly delegated legislation with an unquantified impact on business and workers has not been addressed. Nothing in the regulatory impact statement has properly assessed the regulatory costs to business or workers.

The ETU remains concerned that the Bill will interfere with the industrial rights of workers and their union representatives. The ETU and other unions put forward last year evidence that some employers are using the spectre of security legislation changes in bargaining while others were preparing to conduct their own background checks on employees. Under the 2022 Bill employers can go further and could foreseeably 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.

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.

Consultation

DoHA completely failed in its approach to consulting on such significant reforms. The ETU shares the concerns of many other stakeholders, including:

- both timing of the release and length of consultation period for the 2022 Bill exposure draft coincided with the end of year, Christmas / New Year period and a time when many organisations and key employees are on leave,
- that proactive engagement appears to only occur with select stakeholders and then treats those stakeholders as if they are equally resourced and therefore somehow equally capable of the same levels of engagement, and

[Type here]

- consultation is not contextualised or targeted in a way that maximises the quality of stakeholder engagement.

The co-design process for the rule's framework contemplated in the 2022 Bill has not occurred to the ETU's knowledge. There was no transparent framework for this co-design process and no requirement to either consult with Unions or to consider, incorporate or respond to concerns raised by Unions. At the town hall meetings arranged by DoHA on 25 January 2022 it was stated that consultation was occurring on proposed rules and other unspecified elements of the 2022 Bill. It is unclear where those consultations occurred, what was being consulted, who was being consulted and how the views and concerns of workers were considered. When questioned about this apparent deficiency by participants on the town hall meeting, DoHA representatives were unable to provide any answers.

Following the town hall meetings, the ETU received a request to meet with the head of the Cyber and Infrastructure Security Centre to "*discuss your submission on the Critical Infrastructure Bill Exposure Draft".* This invitation to meet was sent to the ETU on 7 February 2022 after the 2022 Bill had already been listed for introduction to the Parliament and the meeting was proposed to be on the 10 February 2022 after the 2022 Bill had been introduced. No meetings occurred with the ETU or any other Union to our knowledge for the purpose of co-designing any part of the rules under the revised 2022 Bill.

Prior to this, the last time DoHA engaged with the ETU on the framework was 25 November 2021 which was the conclusion of several meetings at which the ETU raised numerous concerns about the 2021 Bill. To date, DoHA has not addressed or formally responded to any of the concerns raised by the ETU and nothing in the 2022 Bill deal with or addresses the concerns raised by the Union.

For transparency, set out in Annexure A to this submission is a summary of the matters raised by the ETU with DoHA of which the Union has not received a response.

Proportionality, Transparency and Certainty

The ETU opposed the initial Security Legislation Amendment (Critical Infrastructure) Bill 2021 (the 2021 Bill) due to its unreasonable requirement to subject workers in a large number of industries to invasive and unnecessary security assessments.[2]

The 2021 Bill 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 were removed and the PJCIS recommended the Government reconsult on these contentious provisions of the 2021 Bill with a view to reintroducing these provisions separately later.

Whilst the 2022 Bill appears to have some minor modifications directed towards the criticisms and deficiencies identified through the PJCIS process, these modifications could only really be characterised as negligible, and have been constructed in such a way as to increase uncertainty at worst, or at best, serve no purpose.

[2] https://www.aph.gov.au/DocumentStore.ashx?id=b410ce43-12d1-45a0-9c6a-a59963cf7215&subId=701514

[Type here]

The ETU retains our strong concerns previously articulated in our various submissions and during our 2021 inquiry appearance. The proposed 2022 Bill should be rejected in its current form due to:

a. The continued failure to understand and recognise the industries it is proposed to cover and the existing systems and processes already in place in these industries to manage security risks,
b. An absence of a clear case of heightened risk to the critical infrastructure ETU members work on which are contained in the recently passed act or to the new sectors introduced by it,
c. No argument or evidence being put forward which demonstrates the recently updated legislation is deficient absent these further amendments or that existing arrangements, including in other legislation regulating security in these industries is inadequate nor has any information been provided as to what deficiency in the current act is purportedly being addressed by the proposed amendment,
d. The proposed schemes for critical infrastructure risk management programs and enhanced cyber security obligations (and indeed the cyber security provisions more generally) wholly fail to ensure the rights, particularly the right to privacy and civil liberties, of employees is taken into account; and
e. The introduction of unnecessary and uncertain regulatory burden that is not reasonably offset by any real net benefit.

Despite the Department of Home Affairs assertions that the 2022 Bill has incorporated and responded to the concerns raised during the inquiry into the previous version of the Bill, nothing in the current draft:

1. Improves transparency and certainty of the law by removing the substantial levels of delegated decision-making and restoring parliamentary oversight.
2. Ensures that all decisions made under the Bill are reviewable by the Administrative Appeals Tribunal.
3. Delineates the class of “critical employees” or other personnel subject to possible background checks to ensure that civil liberties are not unnecessarily impinged upon.
4. Legislates for mandatory consultation with employees and their union representatives if the entity is considering implementing background checking, prevents an entity from taking a maximalist approach to background checking or limits an employer from using information obtained during background checks for unrelated purposes.
5. Amends the Bill to ensure that rights under industrial, work health and safety, privacy or anti-discrimination laws are not impinged upon.
6. Ensures that Citizen’s private data that may be accessed under the Bill is quarantined from employers.
7. Puts in place an appeal mechanism to an independent mediator for workers and their representatives to appeal an entity’s Risk Management Plan should background checking be ‘unwarranted’ or ‘excessive’ for all, or for a class of employees.
8. Establishes a proportional cost benefit analysis of the regulatory burden these additional measures will place on businesses and therefore consumers such as electricity consumers, nor does it provide certainty on the parameters in which the provisions need to be applied.

[Type here]

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022

Despite the PJCIS recommendation for co-design of the rules framework there remains significant issues arising from Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022 (the Rules) outlined in the Explanatory Memoranda of Bill 2 (from page 127 of the memorandum).

None of the concerns outlined in this submission, including those raised in Annexure A, have been adequately addressed in the Rules. It is also quite extraordinary that much of the critical aspects of the 2022 Bill are left to definitions which are subject to delegated legislation.

The definition of critical worker in the exposure draft of the rules remains too broad and could include any ETU member in the relevant industry. The clauses pertaining to critical workers are in essence a tautology, which if applied, are a self-perpetuating 'ratchet' mechanism that would ensure employers always take a maximalist approach to personnel hazards irrespective of the actual risk.

The term "beginning on the compliance day" in Rule 7 Personnel hazards (2) (see also Rule 8 Supply chain hazards, Rule 9 Physical and natural hazards) is worse than the previous iterations of proposed rules where periods of 6 and 12 months were available for developing provisions of a risk management program.

The rules outlined in the explanatory memorandum to the 2022 Bill no longer provide such a period for developing the relevant considerations of a responsible entity's risk management program.

- This provides no time to consult or negotiate with each and all of the employers in the industry to establish measures that comply with the rules
- There will be both a timing and a jurisdictional issue in accessing the FWC for assistance
- "Compliance day" is undefined in the explanatory memorandum or the current Security of Critical Infrastructure Act 2018
- It appears that "compliance day" will be a matter for the Minister, which will increase ministerial discretion and make the legislation more authoritarian.

Significantly, the AusCheck background check regime remains without any amelioration of the issues that have been raised with DoHA with regard to proportionality, privacy or retention and observance of the preservation of civil liberties. No real assessment of regulatory cost or accessibility have been contemplated. It is well known that checks via the Auscheck system are both costly and time consuming.

The provisions of Rule 7 (2) are particularly onerous, discriminatory, authoritarian and difficult to comply with. They are worse than anything in previous draft rules provided to the Union. They include:

7 Personnel hazards
(1) For paragraph 30AH(1)(c) of the Act, subsection (2) specifies a requirement in relation to a material risk that an occurrence of a personnel hazard could have a relevant impact on a Part 2A asset.

[Type here]

(2) Beginning on the compliance day, an entity must establish and maintain a process or system in the entity's program:

(a) to identify the entity's critical workers; and
(b) to assess, on an ongoing basis, the suitability of a critical worker to have access to the critical components of the asset; and
(c) minimise or eliminate material risks that negligent employees and malicious insiders may cause to the functioning of the asset; and
(d) minimise or eliminate material risks arising from the off-boarding process for outgoing employees and contractors.

The explanatory memorandum of the 2022 Bill at page 34 refers to consultation provisions in relation to the Minister's rules, extract below:

Subsections 30ABA(2)-(3)—Consultation

153. Subsection (2) provides that, before making or amending rules for the purposes of section 30AB, the Minister must do all of the following:

- *cause to be published on the Department's website a notice setting out the draft rules or amendments and inviting persons to make submissions to the Minister about the draft rules or amendments within the period of time specified the notice (paragraph (a)), which under subsection (3) must be at least 28 days;*
- *give a copy of the notice to each First Minister (paragraph (b)); and*
- *consider any submissions received under paragraph (a) (paragraph (c)).*

154. This consultation requirement will ensure that the critical infrastructure risk management program obligation is only activated after entities have been provided with an opportunity to provide the Government with submissions about why applying this obligation is, or is not necessary, and to provide entities with early warning to adjust their businesses without undue burden.

155. The Bill newly includes the obligation for the Minister to consider submissions received in response to consultation prior to making rules, consistent with PJCIS recommendation 7 and paragraph 3.49 as well as feedback from industry stakeholders.

The ETU is concerned that the above provisions:

- Provide no obligation on the minister other than to publish draft rules and invite and consider submissions,
- Reinforce ministerial discretion and make the legislation more authoritarian, and
- May be applied in a discriminatory fashion either directly or indirectly to organisations to which a minister may be politically opposed.

Based on this assessment, the 2022 Bill appears, *prima facie*, significantly worse than the various iterations of this legislative regime presented by DoHA last year.

[Type here]

Conclusion

The 2022 Bill will significantly impinge on the rights of Australians including their civil liberties, right to privacy as well as their legitimate industrial rights in the workplace. Contrary to the principles of the Rule of Law, this legislation is not transparent, it creates significant uncertainty, and it will be largely inaccessible to the majority of people impacted by it who are excluded from having any meaningful say in the ongoing iterations of subordinate legislation.

Absent proper consultation and engagement followed by sensible amendments to address the concerns raised in this submission the proposed Bill should not be progressed any further.

Notwithstanding the above issues, the ETU would welcome more meaningful engagement in order to properly participate and be afforded the opportunity to meaningfully contribute to any final development of a proposed Bill through a properly conducted exposure draft consultation process going forward.

[Type here]

Annexure A

Matters raised by the ETU.

1. What is the imperative for this process?
    a. What has caused this to be undertaken?
    b. Why is it aimed at operational staff?
2. How will it impact workers:
    a. With previous, or current, associations - such as with Motorcycle Clubs?
    b. With previous civil matters and / or criminal convictions?
    c. Who are born overseas, or with parents from overseas, in countries with perceived security risks?
3. How will the legislation eliminate:
    a. Employer overreach and mission creep?
    b. Employer abuse of legislation for other purposes (Right of Entry, access to work sites, enterprise bargaining etc.)?
4. Explain the reasoning behind why legislation has been drafted with so many delegated powers and potential for abuse (delegated legislation represented by regulations and rules are subject to ministerial discretion?
5. What would prevent a government that doesn't like unions abusing the nature of the legislation, the delegated regs and rules, and include people who have undertaken union activity?
6. What guaranteed protections of personal information and privacy is in the legislation?
7. The SOCI Bill seems to be cyber security focussed so why does it need to cover operational workers with limited or no access or influence on an organisations IT/OT systems?
8. How has the Department assessed the cost impost on PCBUs and what affect it may have on resources needed for infrastructure construction and maintenance, safety, wages and conditions?
9. Why isn't there a no-cost appeals process established by the appropriate regulator where an adverse finding is made against a worker?
10. How does the legislation ensure employer can't access a workers' digital footprint as it should be securely retained by the appropriate regulator or another acceptable Commonwealth entity?
11. What assurance of security of personnel data is provided for in the legislation? and
12. What indemnity is provided against financial, reputational, physical or any other personal loss due to leak of employee data?