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

ACTU Submission, 7 July 2021
ACTU D. No 34/2021

ACTU
australian council of trade unions

At the outset we point out that the ACTU and its affiliated unions recognise and support the need to ensure that effective measures are in place to protect Australian national security interests. We understand that the protection of key critical infrastructure assets is a central component of any scheme which has our security interests in mind.

We are concerned however to ensure any system that is put in place is well-designed and proportionate and does not encroach unnecessarily into areas of everyday life, particularly the workplaces of ordinary Australians. Our view is that the bill in its present form has some serious shortcomings. Our focus is the impact the bill will have on workers in critical infrastructure sectors.

First, the scope of the legislation is extensive. Many industries and many individuals who were not previously subject to security measures will be affected by this bill if it passes in its current form. At the same time, the exact boundaries of the bill are imprecise, both because of the inherent difficulty of defining these sectors and because the details of the new rules that will apply to these sectors are presently unknown.

Finally, the bill mandates (proposed s 8(1)(ba) of the *AusCheck Act a*nd s 30AH(4)) that the AusCheck system of background checks will be extended to those working on critical infrastructure assets. This means that vast swathes of the Australian population can be subjected to invasive security checks, eroding fundamental rights to privacy and seriously undermining our civil liberties. We will deal with these problems in turn.

The reach of the legislation as currently drafted is very wide. Eleven new critical infrastructure sectors are identified in the Bill. Those sectors are large and diverse. They extend to industries from transport, to financial services, from communications to water and sewerage. Almost one third off the 150+ page bill is devoted to defining exactly what the boundaries of these new sectors, and their critical infrastructure assets, will be.

There is some difficulty in determining the exact numbers of people engaged in these new critical infrastructure sectors. Several of the sectors do not exactly coincide with ANSZIC industry or sub-industry categories. Some, such as data storage and space technology, have no equivalent ANZSIC sub-group. Some manufacturing sub-groups would contribute to the manufacture of defence materiel, though it is difficult to be precise. If you use the figures in the May 2021 Labour Force Industry Sub-division release, sectors such as Hospitals', 'Transport', 'medical and other health care services' and 'food retailing' account for some 2 million workers by themselves. It is conceivable then that the new measures would extend to sectors covering upwards of 3 million people.

At the centre of the changes is the new requirement for entities to have in place a 'risk management programme' for the critical infrastructure assets that they are responsible for. These 'responsible entities' vary from industry to industry. They can include asset owners, operators or

licence holders. They can also include any entity the Minister prescribes by the rules as being responsible for the asset.

The precise details of these risk management programmes are unknown because the Bill allows for this detail to be included in rules which are yet to be designed and released. There has been no indication thus far that unions would have an input into the design of these rules even though these risk management programmes would apply to vast numbers of workers. The Explanatory Memorandum says the Department will co-design the rules 'with industry and states and territories on a sector-specific basis.' There are no minimum requirements or outer limits to the scope of these programmes, beyond the bills requirement that they be 'in writing.'

Not only is the content of these programmes unknown, it is also unclear how far down the contractual chain they will devolve and who they will apply to. For example, it is unlikely that an asset owner's risk management programme would only apply to its employees and not extend to the employees of contractors who have access to the asset itself. Physical assets caught by the provisions would require regular maintenance and upgrading. This could extend risk management programmes to the workforces of literally thousands of construction and maintenance contractors.

What we do know is that those risk management programmes will be required by rules to include provisions that require background checks of individuals to be conducted under the AusCheck system. 'AusCheck' currently applies to those with Aviation and Maritime Security Identification Cards, and those working with security sensitive biological agents and major national events.

The elements of a background check that can be enabled under the AusCheck scheme include an identity check, a criminal history check, an immigration status check, and a security assessment conducted by ASIO. Extending the AusCheck scheme to these new sectors would be an enormous, if not impossible, logistical exercise.

A 2011 ANAO review of the Aviation and Maritime Security Identification Card Schemes (ASIC and MSIC) found that just for those two schemes alone there were over 1200 industry participants that were required to develop security plans that outlined arrangements by which access to designated secure areas is restricted to ASIC and MSIC holders, and over 200 government and non-government bodies were authorised to issue ASICs and MSICs, including many commercially-based third party entities that had no relationship with ASIC/MSIC applicants. There were over 250,000 ASIC and MSIC cardholders.

The privacy and civil liberties implications of extending the AusCheck system on such a vast scale are obvious. Sensitive information will be issued in respect of millions of Australian workers. The potential for misuse and unauthorised disclosure is serious and real. The storage, access and dissemination of sensitive information on this scale poses its own serious security challenges.

Already ACTU-affiliated unions have reported instances of employers requiring their workforces to submit to background and digital footprint checks citing the bill as the reason, even though it has not yet passed into law.

A blanket extension of the AusCheck system to these new sectors based on a person's physical presence at or connection with a critical infrastructure asset pays little regard to the scale of any potential security risk that many of these people might ultimately pose. For example, there would be many workers associated with the food and grocery sector that, because of the nature of their work, would be unlikely to present any security risk. The same could be said for areas of the health care, education, financial services sectors, and others.

We are also concerned that employer access to sensitive information will be misused to 'filter' employees on grounds unrelated to security issues. We are concerned about practical problems associated with extending these background checks and imposing MSIC/ASIC equivalent requirements on entire sectors of the labour force. Affiliates report problems with waiting periods for security cards to issue, when they are effectively unable to work without them, delays associated with adverse information when cards are being renewed even where the information was assessed in issuing previous cards, and costs to employees in applying for security clearance cards.

The Maritime Union of Australia (MUA) has advised that its members have reported over the last 2 years several instances where AusCheck background checks have taken up to 3 months to complete. On one such occasion AusCheck waited 2.5 months to ask the Applicant's MSIC Issuing Body to confirm the Applicant's identification, due to a new automated ID verification system being used rejecting his authenticated birth certificate despite the fact that he had successfully used it in the past to obtain an MSIC.

The problem with Applicants needing a discretionary MSIC due to an adverse criminal record is that they are usually advised, and even prevented from applying by some Issuing Bodies by default, to apply 3 months prior to their expiration. So even if AusCheck takes 2 months to complete a background check and reject the Applicant, the process is not over and an Applicant is likely to be at real risk of losing their employment if they cannot complete the process with the Department of Home Affairs in time due to the often onerous amount of information they request. On one occasion, despite Auscheck being relatively quick in the criminal background check phase, it took an additional 4 months for an Applicant to have his MSIC approved from the date he was rejected by AusCheck.

address

ACTU

Level 4 / 365 Queen Street

Melbourne VIC 3000

phone

1300 486 466

web

actu.org.au

australianunions.org.au

ACTU Australian Unions