

SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

COMMENTS ON EXPOSURE DRAFT

NOVEMBER 2020



Opening comments

AustCyber welcomes the opportunity to review and comment on the *Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020* (the Bill). The cyber security sector and associated stakeholders appreciate the opportunity to review the Bill before it is introduced to the Australian Parliament so industry can develop an understanding of and respond to the new proposed arrangements.

From AustCyber's discussions with stakeholders, including those in our ecosystem of cyber security companies, there is broad support for the intended cyber security uplift in the proposed Bill. AustCyber understands several stakeholders will provide separate submissions with detailed comments on issues in relation to the Bill. Accordingly, the comments in this submission are confined to the priority issues that have been raised through our consultations, namely:

- the urgency with which the Australian Government is proceeding with such a complex piece of legislation
- Ministerial action directions, intervention requests and independent reviews
- potential global and local impacts
- lack of clarity about terms in the Bill and rule making.



Urgency of the Bill

AustCyber has been part of the set of organisations advocating across the economy for the need for businesses to improve their cyber security posture, reflecting ever increasing complexity in the cyber threat landscape and increased malicious targeting across all sectors. Industry continues to support the Government's sentiments prior to the Bill's release consultations – that Government will engage with industry in developing suitable arrangements to improve overall industry cyber security posture.

The Explanatory Memorandum to the Exposure Draft reflects this when it mentions co-designing the arrangements under the Bill. AustCyber would like to see this reflected in the approach to the Bill itself by providing industry with more time to work closely with the Government to make sure the provisions in the Bill are relevant and will operate effectively in practice.

The Bill enables legislation with over-arching arrangements, that in some cases duplicate regulatory arrangements for critical infrastructure in other legislation. In other areas its drafting obviously extends the regulation of critical infrastructure into new industries. It also places new obligations on entities, with greater oversight and powers for the Government to act. We and industry welcome the maturing of the regulatory landscape in this way, but more time is needed to flesh out the complexity and reduce the real risk of unintended consequences.

The arrangements in the Bill are 'dormant', to be activated when needed. When activated, certain entities are to register critical assets, meet risk management obligations and comply with cyber security reporting arrangements as a starting point to demonstrate they are operating their assets to effectively to deal with hazards including cyber security incidents. Given the arrangements in the Bill are to be gradually activated, AustCyber strongly requests Government to be transparent about why there is urgency with introducing the Bill into the Parliament when a co-design process will better assure the resulting legislation's ability to achieve the intended outcomes.

Further, with comments to be with the Government less than ten days before the Government plans to introduce the Bill to the Parliament, industry is concerned about how genuine the consultation is, given the limited time available to amend the Bill in response to industry concerns. AustCyber therefore requests additional time for industry to work with the Department of Home Affairs to improve the arrangements provided for in the Bill.



Ministerial directions and intervention requests

Under Part 35AB of the Bill, the Minister for Home Affairs is to have the power to direct an entity to take action in relation to a cyber security incident that has occurred, is occurring or is imminent. We note that no definition of 'imminent' is provided, giving the Minister considerable discretionary power in relation to what are called 'action directions'.

The Minister for Home Affairs can use his or her action direction to authorise the Secretary of Home Affairs to direct an entity to:

- provide information (this power is considered important because the malicious activity may obscure the methodology of their attack)
- do acts or things in response to an incident; and
- provide specified assistance.

From information obtained through international networks of lived experience, and in the context of Australia, Canada, New Zealand, the United Kingdom and the United States, the extent of this action direction power is unprecedented.

In relation to directing an entity to take certain action, the Bill says that where an entity is "...unwilling or unable to take all reasonable steps to appropriately resolve an incident..."¹, the intervention requests authorised by the Minister for Home Affairs (in agreement with the Prime Minister and the Minister for Defence) and made by the Secretary may include:

- access to a computer
- undertaking analysis of a computer
- altering data held on a computer, or
- altering the functioning of the computer.

Although there are arrangements to consult with the responsible entity in relation to the intervention request, ultimately the entity is required to comply with the intervention request, which are highly intrusive.

The need for a review or appeal process

The Bill contains no avenues of recourse if there is a dispute between the entity and the Ministers (or Secretary) about whether the action direction can be or needs to be complied with.

¹ Paragraph (35AB(7)(a)) of the Bill

The reason for not including an *Administrative Decision (Judicial Review) Act 1977* (ADJR ACT) review mechanism to resolve disputes about these actions and intervention requests is explained in paragraph 418 in the Explanatory Memorandum which says that:

“...ARC [Administrative Review Council] concluded that national security considerations may be a reason for excluding ADJR Act review, particularly where sensitive information is involved which may be publicly disseminated through judicial proceedings...”

And further, paragraph 419 says:

“...Decisions of this nature are likely to be based on sensitive classified information and deal with the capabilities of intelligence agencies. This includes intelligence information and covert investigation procedures, the disclosure of which may impact ongoing investigations or operations, or compromise intelligence methodologies. For this reason, it is entirely reasonable to exempt decisions made under new Part 3A from review under the ADJR Act as the public dissemination of the information and capabilities used to make decisions under new Part 3A would pose a risk to national security...”

With the sensitive nature of the intelligence in mind, the need for a review process is even more important. For example, if there are issues around intelligence sharing and the adequacy of information provided to the entity about the threat the entity may not be able to take appropriate action, because it does not have sufficient information to develop the most appropriate response.

This is not about being unable to or unwilling to act, rather inadequate communication. Having an avenue for such a matter to be resolved independently would not only help resolve the situation, but also put the onus on the parties to make sure they act in good faith in sharing intelligence without compromising national security, so serious cyber security activities and threats can be dealt with.

Requiring action to be taken in relation to assets that are operating in highly complex environments that the Minister or the Secretary of Home Affairs and advisors are unfamiliar with, are a concern for industry. AustCyber recommends the Government proceeds with caution and does not implement this so called 'last resort' action direction power for intervention requests without an avenue for independent review.

This could include national security cleared independent technical advisor(s) as necessary so responsible entities and industry more broadly have confidence that suitable technical advice is received by the Ministers so decisions will be made that are appropriate for the circumstances and achieve the desired result.

With the Bill focused on regulating an entity's assets, the concerns about action directions and intervention requests becomes more complicated with assets that are part of a global network of assets, including the use of, for example, offshore cloud infrastructure. Ministers issuing intervention requests could create both local, national and international flow on impacts for the owners and operators of these assets and their customers, who may not be in Australia. Thus, such action could have international implications.

Further, where the source of the malicious activity is from an offshore location, the impact may not be able to be isolated to the one asset, but also impacting multiple parts of the supply chain. This complicated situation could require intervention requests that go beyond an asset, and to multiple assets in the whole supply chain.

In light of this, AustCyber supports the recommendation of the Australian Information Industry Association (AIIA) that the more intrusive intervention requests can be examined by an independent appeals board that can be stood up urgently when necessary, chaired by an adjudicator that is a former federal judicial officer and supported by an independent technical advisor.

This board could review (or appeal) intervention requests of the tri-Minister (Ministers for Home Affairs and Defence and the Prime Minister) where there are disputes about the intervention requests (which are actually not requests, but ultimately mandatory requirements).

The AIIA proposes that the government insert an eighteenth section under s35AB:

Ministerial discretion subject to entity's *right to appeal to independent board*

(18) If the entity subject to the ministerial authorisation or intervention request disagrees with the directions or requests made under 35AB(2) or (10) in relation to a critical infrastructure asset, the entity may have recourse to an independent critical infrastructure appeals board comprised of an adjudicator, that being a former federal judicial officer, and a mutually agreed industry appointee with the requisite expertise in cyber security management, upon which time a 12 hour injunction will take effect until the independent appeals board has made a declaration as to the reasonableness and justification of the Ministerial authorisation or direction.

This will make sure the intervention requests do not create the potential for unintended consequences, given the highly interconnected nature of the critical infrastructure assets, that could make the threat situation worse.



Potential global and local impacts

Looking at the Bill from the perspective of the entity and their investors, their lens will be whether the requirements in the Bill are reasonable and proportionate, which is the intention of the Bill. As noted above, the powers in the Bill in relation to action directions are out of step with the way other five eye countries are regulating their critical infrastructure.

Currently, in response to the current increased threat landscape, AustCyber is seeing organisations bringing their data and key infrastructure onshore so that Australians and Australian businesses have their data and digital activity here for sovereign security reasons. Unfortunately, the Bill introduces arrangements, including the action directions and intervention requests, in particular, that create concerns and uncertainty for the industries covered by the Bill.

There is a potential unintended consequence that the Bill could encourage critical infrastructure providers to have their data and data holdings offshore so they are out of reach of the Bill and the Australian jurisdiction.

Further, critical infrastructure entities that are concerned about how the Bill will operate may slow down their investments in digitalised assets, as they work through the complexities of the regulatory arrangements in the Bill. This is contrary to the current pace of accelerating digitalisation of infrastructure with the positive blurring of the lines between operational technologies and information technologies to improve critical infrastructure performance and efficiencies.



Clarity about terms in the Bill and rule making

Clarity about terms in the Bill

The Bill includes a range of terms that are not clear and need clarifying to assist effective implementation of the provisions. Such terms such as, “critical cyber security incident” and “significant impact” in relation to whether a cyber security incident needs to be reported in subsection 30BC(1)(b)(ii) need to be better defined.

AustCyber has consistently encouraged greater two-way sharing of intelligence between industry and the Australian Government about cyber security threats. Improving clarity of terms for reporting incidents, such as a critical security incident and significant impact will help industry and the Government develop arrangements so industry captures and shares necessary intelligence. It will ensure the right intelligence is captured and provided to Government so it understands the threats, incidents and can share the intelligence more widely, alerting industry as necessary.

With these terms unclear, the proposed intelligence sharing arrangements run the risk of entities regulated under the Bill being required to over or under-report threat activity, with too little or too much information being shared. This situation could create confusion with important threat patterns and behaviour being missed, as informative intelligence is not surfaced for Government and industry attention and awareness.

With greater clarity in definitions, the Bill will set the scene for Government and industry to provide useful intelligence and to focus on active corporation rather than meeting unclear regulatory obligations. The expectation of industry is that by setting these arrangements up well, both the Government and industry can focus on cooperatively working through suitable arrangements for two-way sharing of intelligence.

Clarity about rule making

The Exposure Draft of the Bill indicates that rules will be developed under the Bill once it is legislated and industry will be included in the co-design process. AustCyber believes this will operate differently across the sectors, entities and the relevant regulators involved. There are differing levels of maturity in relation to cyber security across industry. Industries, such as finance, banking, telecommunications, electricity, gas and water that are very familiar with cyber security arrangements for critical infrastructure with their arrangements expected to continue to be relevant, but this is not certain.

There is also to be considerable activity making sure industry maturity is catered for and that there is minimal regulatory duplication across the industries to avoid confusion and red tape. Currently, how the Government plans to work with entities and industries that operate under different arrangements for protecting their assets is not clear. To date, with the Bill being treated urgently and consultation at a minimum there is wariness about the proposed co-design processes.

Industry seeks greater clarity about the way rulemaking is going to be undertaken and the amount of consultation that will be undertaken and seeks this information sooner to avoid the co-design processes also being rushed.



In conclusion

AustCyber believes that given the concerns raised in this submission that we understand are shared by a range of industry stakeholders, the introduction of the Bill needs to slow down and not be introduced until the concerns of industry are either addressed or responded to.

One of the potential shortcomings of the Bill with its focus on critical infrastructure assets that are to be the subject of action directions and intervention requests, is that the Bill doesn't recognise that the assets do not operate independently and to operate effectively they are part of a wider environment of complex technology. This issue alone, highlights the need for an appeal mechanism.

Indeed, the Department of Home Affairs is aware of interconnected nature of critical infrastructure assets, as demonstrated through its consultation on critical infrastructure supply chain principles. AustCyber urges that the interconnectedness of supply chains is considered when working through the means to manage and respond to a complex threat environment to make sure assets, networks and data are effectively risk managed so they are protected, and remain resilient.

AustCyber believes the Bill needs both refinement through greater clarity in definitions as well as strengthening by including suitable appeal arrangements which will assist making sure intervention requests have an eye to this complex environment. This way the expanded and tightened regulatory arrangements in the Bill that aim to help keep critical infrastructure secure by minimising the potential impact of serious malicious intrusions will be more likely to achieve this aim and ensure Australia responds effectively to significant cyber security threats.




About AustCyber

AustCyber is a publicly funded, private entity which commenced on 1 January 2017. Our mission is to grow Australia's cyber security sector, to support the development of a vibrant and globally competitive Australian cyber security sector and to ensure there is a pipeline of skills and educated cyber security professionals. In doing so, our activities enhance Australia's future economic growth in a digitally enabled global economy and improve the sovereign cyber capabilities available to protect our nation's economy and community.

We form a part of the Australian Government's Industry Growth Centres Initiative, established through the 2015 National Innovation and Science Agenda and Australia's 2016 Cyber Security Strategy, in sectors of competitive strength and strategic priority to boost innovation and science in Australia. Industry Growth Centres are required under contract with the Government to achieve for their sector:

- increased R&D coordination and collaboration leading to improved commercialisation outcomes
- improved management and workforce skills of businesses
- more businesses, including small and medium enterprises, integrated into global supply chains leading to increased export income
- a reduction in the cost of business through regulatory reform; and
- additional or indirect (spillover) outcomes.



Our funding comes from majority Federal Government grants – funding for operations and programs, and for the AU\$15 million AustCyber Projects Fund which provides grants to projects that deliver national benefit. We also receive funding under contracts with the governments of the ACT, NSW, QLD, SA, TAS, WA and the Sunshine Coast Regional Council and Townsville City Council, which we match, to deliver AustCyber’s national network of Cyber Security Innovation Nodes – with the NT and VIC soon to join.

We work to align and scale Australian cyber security research and innovation related activities across the private sector, research communities, academia and within Australian governments. We are responsible for maintaining a strong supply of innovative Australian cyber security solutions and capability and have established ourselves as an independent advocate for the competitive and comparative advantages of Australian technical and non-technical cyber security capabilities.

Beyond our shores, we work with partners across many countries to develop export pathways for Australian solutions and capability. This helps the rapidly growing Australian cyber security sector tap into market ‘hot spots’ around the world.