The Institute for Integrated Economic Research-Australia Ltd

ABN 79 623 951 226

Submission to the Parliamentary Joint Committee on Intelligence and Security
Review of Cyber Security Legislative Package 2024

Introduction

The Institute for Integrated Economic Research - Australia (IIER-A) was formed in 2018. Our purpose is to address the need for greater resilience in our society, both structurally and culturally, given the significant transition challenges that we will have to face in coming decades, of which cyber security is an increasingly demanding aspect. Our National Resilience Project reports can be accessed at https://www.jbcs.co/iieraustralia-projects.

We thank the Parliamentary Joint Committee on Intelligence and Security for the opportunity to provide input into the Review of the Cyber Security Legislative Package 2024.

Cyber Security Bill 2024

IIER-A acknowledges that the Cyber Security Bill 2024 provides the holistic legislative framework to address whole-of-nation cybersecurity issues and to respond to new and emerging threats.

In terms of the first measure, mandating minimum cyber security standards for smart devices is most welcomed. Adopting international standards, with the flexibility to change as the threat changes, would be sensible. Compliance with the standards should be enforced. Australia should align closely with the UK's PSTI Act for consumer product safety, which requires vendors, suppliers, importers and manufacturers to comply with the standard. Legislating the first three principles of the ETSI EN 303 645 standard should be a minimum. Adopting multiple standards could send mixed messages; thus, it would be useful to set the one standard and enforce compliance. The Regulatory Powers (Standards Provisions) Act 2014 should to be adopted for the regulatory scheme, ensuring consistency with the compliance framework under the SOCI Act.

In terms of the second measure, mandatory reporting of ransomware payments, regulatory burden is a genuine concern. All critical infrastructure entities should be included, as all need to be more proactive with their cyber security. **A missing element continues to be cyber threat intelligence sharing across all critical infrastructure sectors**.

Anonymised information sharing such as summaries of the types of incident and levels of impact must be encouraged to help all businesses strengthen their own cyber defences and better prepare for cyber-attacks. A public report would be useful, including a focus on specific sectors, and while a quarterly report might be used initially, flexibility should be retained to change that as circumstances dictate.

In terms of the third measure, supporting and assuring Australian organisations as they respond to a cybersecurity incident, we fully support the role of the National Cyber Security Coordinator to coordinate whole-of-government cyber incident response efforts.

Limiting the circumstances under which the coordinator can use and share information that has been voluntarily provided by an affected entity is a vital aspect of this Bill. The 'limited use' obligation is supported; however, **legislative and regulatory obligations must still be enforced and businesses cannot be exempted from their cyber security accountabilities**.

In terms of the fourth measure, the Cyber Incident Review Board (CIRB) is essential; however, a no-fault principle is critical to maximise stakeholder engagement with the CIRB. A national mechanism is needed to review the root causes of cyber incidents and assess the effectiveness of post-incident response. A wide range of stakeholders should be engaged in regular post-incident review sessions, examining the technical severity and complexity of the incident; and the likelihood and severity of the consequences of the incident, including the impacts on national security, economy and the broader public.

The US Cyber Safety Review Board provides a definition for its threshold for commencing a review, which should be used as a baseline for the CIRB. The CIRB should have limited information gathering powers to require entities to provide appropriate information to facilitate the review of cyber incidents.

Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024

IIER-A supports all Divisions of this Bill, and especially welcomes the limited use of certain cyber security information, including communication of that information, and its secondary use.

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

IIER-A has reviewed the six Schedules and comments as follows:

Schedule 1—Data storage systems that hold business critical data. We welcome the inclusion of data storage systems as an intrinsic part of a critical infrastructure asset.

Schedule 2—Managing consequences of impacts of incidents on critical infrastructure assets. Clarification around the precise meaning of incidents and impacts is welcomed.

Schedule 3—Use and disclosure of protected information. Clarification around protected information and relevant information is welcomed, as is the inclusion of protected information when referring to an operator asset. The changes comprehensively cover the links to national security; the defence of Australia; social and economic stability of Australia; confidential commercial information; and the availability, integrity, reliability and security of a critical infrastructure asset.

Schedule 4—Direction to vary critical infrastructure risk management program. We welcome these changes, and highlight the importance of clarifying that a serious deficiency relates to a material risk to: national security; the defence of Australia; or the social or economic stability of Australia or its people.

Schedule 5—Security regulation for critical telecommunications assets. We welcome the addition of 'imposing enhanced security obligations for critical telecommunications assets' to the exiting 'imposing enhanced cyber security obligations that relate to systems of national significance'.

Similarly, we acknowledge that a critical public transport asset that is owned or operated by a carrier may also be a critical telecommunications asset; and that a critical telecommunications asset that is owned or operated by a carrier may be part of the space technology sector. Clarifying the meanings of satellite-based facilities, submarine cables, telecommunications services, and telecommunications systems is also welcomed. Setting out the enhanced security regulation for critical telecommunications assets is welcomed, so that there will not be any misunderstanding, including Secretary and Ministerial directions.

Schedule 6—Notification of declaration of system of national significance. We fully support the rewording of a 'reporting' entity to a 'responsible' entity for an asset that is a declared a system of national significance must notify the Secretary of changes.

Dr Gary Waters
Director, IIER-A
15 October 2024