Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the Cyber Security Legislative Package 2024

The Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024, included within the Cyber Security Legislative Package, is an important upgrade in Australia's ability to deal with major national crises and incidents.

In this regard, Global Shield strongly supports this bill, in particular its intention to enable the Government to better manage the impacts of all hazards on critical infrastructure and to direct entities to address serious deficiencies within their risk management programs.

Australia is likely to face major challenges over the coming decades, including climate disruptions, geopolitical tensions, infectious diseases and other threats to health security, and threats enabled by emerging technologies. Any of these could become catastrophic. The proposed reforms to the Security of Critical Infrastructure Act 2018 (SOCI Act), along with additional recommendations outlined below, would help provide the Australian Government reasonable and necessary authorities to prepare for and respond to a national crisis or catastrophic incident.

Schedule 1 – Data storage systems that hold business critical data

Artificial intelligence (AI) will become an increasingly important feature within critical infrastructure, potentially including data processing and analysis, and automated decision-making. For example, AI models might be deployed as part of a critical infrastructure asset's Supervisory Control and Data Acquisition (SCADA) system or related Industrial Control System (ICS). SCADA and related ICS have long been a key source of concern for cybersecurity of critical infrastructure, and the integration of AI models might make them even more vulnerable.

However, it is not clear if the authorities and obligations under the SOCI Act apply to AI models. For example, with the reform proposed under Schedule 3, it is not clear if the Minister would have the authority to issue action directions or intervention requests related to an AI model that is impairing the function of one or more critical infrastructure assets. The lack of clarity is due to the SOCI Act's definition of "critical data storage or processing asset" not adequately considering the possible inclusion of general-purpose and other AI models in the functional operation of critical infrastructure. **We recommend the reforms update the definition of "data processing asset" to better include possible effects resulting from the inclusion of AI models in critical infrastructure.** We propose the following legislative language be included under Section 3 of Schedule 1, after (7):

Data processing systems

(8) If, under this section, an asset is a critical infrastructure asset, then a data processing system in respect of which all of the following requirements are satisfied is taken to be part of the critical infrastructure asset:

(a) the responsible entity for the critical infrastructure asset owns or operates the data processing system;

(b) the data processing system is used, or is to be used, in connection with the critical infrastructure asset;

(c) the data processing includes any machine-based system that is designed to operate with varying levels of autonomy in business critical processes and that may exhibit adaptiveness after deployment;

(d) for a hazard where there is a material risk that the occurrence of the hazard could have an impact on the data processing system, there is also a material risk that the occurrence of the hazard could have a relevant impact on the critical infrastructure asset.

Schedule 2 – Managing consequences of impacts of incidents on critical infrastructure assets

We fully support the change to the SOCI Act proposed in Schedule 2, which allows the Government to better respond to major incidents of any kind, rather than only cyber security incidents. As the explanatory memorandum states, "The existing limits for utilising a Part 3A power do not adequately consider or address the current threat and risk environment…[including] physical incidents like terrorist attacks and natural incidents such as floods or bushfires."

We note that critical infrastructure asset owners and the Government must be ready for major incidents beyond just these scenarios outlined in the memorandum. Indeed, the authority provided by the legislation would be most likely to be exercised in extreme and unexpected scenarios. The memorandum does not *exclude* these scenarios, but without more explicit mention, entities, regulators and other stakeholders might have different expectations about the types of circumstances they need to consider when managing the consequences of incidents. **We recommend the revised explanatory memorandum for the legislative package explicitly mention the risk from a wider range of potentially catastrophic disruptions to critical infrastructure**. We propose the following addition to Paragraph 37 of the explanatory memorandum:

"The existing limits for utilising a Part 3A power do not adequately consider or address the current threat and risk environment, where an effective response must address non-cyber incidents and manage consequential impacts of incidents to other critical infrastructure sector assets. This includes physical incidents like terrorist attacks and natural incidents such as floods or bushfires, as well as potentially catastrophic disruptions, such as regional conflict in the Indo-Pacific, naturally occurring or engineered pandemics, extreme climatic or environmental disasters, faulty or malicious deployment of artificial intelligence models, space-based hazards such as near-Earth objects and solar storms, and major volcanic eruptions in the region."

Schedule 4 — Direction to vary critical infrastructure risk management program

We fully support the change to the SOCI Act proposed in Schedule 4, which would empower the regulator to issue directions to a critical infrastructure asset owner to address any serious deficiencies that are identified in a critical infrastructure risk management program.

However, we foresee a major discrepancy between what critical infrastructure asset owners include as hazards as part of their risk management program and what the Australian Government sees as the major hazards that need to be managed. In the SOCI Act, it is the responsibility of the asset owners to "identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset". Given the complex global threat environment, these entities are unlikely to have a holistic, updated or accurate assessment of the risk.

As a result, we would expect many asset owners to have "serious deficiencies" in their risk management program, as proposed in the reforms, regardless of their best efforts. **We strongly recommend that the Australian Government provides greater clarity to the types of threats, hazards and incidents that would be deemed material risk to "national security, the defence of Australia; or the social or economic stability of Australia or its people".** This could be done through the creation of a "National Risk Assessment", which would allow critical infrastructure asset owners to more effectively deliver their risk management program and proactively address any potential deficiencies. It would also allow a consistent Government approach across all critical infrastructure sectors and assets. **We therefore propose the bill include the requirement for the Government to develop a National Risk Assessment and provide its results to Parliament and critical infrastructure asset owners.** *See Appendix 1 for proposed legislative language.*

We also seek a small but meaningful revision to the legislation's multiple references to "national security, the defence of Australia; or the social or economic stability of Australia or its people". This list might inadvertently leave off an important fourth priority: the health, wellbeing and survival of Australians. There might be instances where an incident could directly harm many Australians

without it qualifying as a threat to national security, defence or social or economic stability. These instances could include, but are not limited to, naturally occurring or engineered pandemics, severe and extended heat waves, compromise of food and water safety, and antimicrobial resistance. **We recommend that, where "national security, the defence of Australia; or the social or economic stability of Australia or its people" is referenced throughout the legislation, another priority – along the lines of "*the health, wellbeing and survival of Australians*" – is added as to require critical infrastructure providers to better consider their obligations to human health.**

Budget considerations

We note that the additional authority under this reform requires the Home Affairs portfolio – most directly through the Cyber and Infrastructure Security Centre – to consider a greater number of scenarios impacting a larger set of critical infrastructure assets, and to engage more directly with entities in managing risk. A major incident is also likely to impact multiple critical infrastructure sectors and assets simultaneously. While we support the intention of this reform, it is only as useful as the resourcing and expertise needed to employ its authorities.

The Government budgeted $19.5m over 2023/24-2028/29 to "continue work to improve the security of critical infrastructure assets and assist owners and operators to respond to significant cyber-attacks". **We encourage the Government, with support of the Australian Parliament, to increase this budget by 50 per cent to effectively manage the additional authorities and responsibilities under this reform.** A mere $10m increase over five years is a minor cost for helping avoid or mitigate a potential catastrophic disruption to critical infrastructure that could cost billions of dollars of economic damage, many Australian lives or a significant deterioration of Australia's national security.

About Global Shield

Global Shield is the world's first international advocacy organization dedicated to reducing global catastrophic risk – that is, the risk that any major threat or combination of threats will inflict significant harm to human well-being on a global scale. We believe that humanity's prospects for security and flourishing depend on today's governments and global leaders adopting effective policies to reduce the risk of global catastrophe. Our mission is to ensure countries around the world enact and effectively implement policies that reduce global catastrophic risk.

Rumtin Sepasspour, Cofounder and Director of Policy, Global Shield
rumtin.sepasspour@globalshieldpolicy.org
25 October 2024

Appendix 1: Legislative language for a national risk assessment

Schedule 7 – Assessment of Risk of National Significance

Insert:

PART 2D – Assessment of Risk of National Significance

30DA – Simplified outline of this Part

This part sets up a requirement for the Secretary to undertake a comprehensive assessment of all threats and hazards that would pose a material risk to Australia.

30DB – Application of this Part

(1) The Secretary must, every five years, undertake a comprehensive assessment of all threats and hazards that would pose a material risk to:

(a) national security; or
(b) the defence of Australia; or
(c) the social or economic stability of Australia or its people; or
(d) the health, wellbeing and survival of Australians.

(2) The assessment must consider, but not be limited to, threats and hazards arising from natural disasters, technological development and use, weapons of mass destruction, geopolitical instability, economic disruption, foreign and malicious actors, diseases, and outer space; and consider the potential for catastrophic consequences on public safety, critical infrastructure, and the continuity of government and essential services.

(3) Upon completion of the assessment under section 1, the Secretary must provide a report to responsible entities for critical infrastructure assets outlining the results.

(4) Upon receiving the report, the responsible entities must vary their critical infrastructure risk management programs to account for material risk.

(5)The Secretary must give the Minister a report, for presentation to the Parliament within three (3) months of the completion of the assessment.

(6) The report must include the findings of the assessment, and any recommendations for actions to understand, prevent, prepare and respond to risk of national significance.