ITI Promoting Innovation Worldwide

ITI Response to Protecting Critical Infrastructure and Systems of National Significance

September 16, 2020

We would like to thank the Australian Department of Home Affairs for the opportunity to provide input on *Protecting Critical Infrastructure and Systems of National Significance*.

About ITI

ITI is the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and represents leading companies from across the ICT sector, including hardware, software, digital services, semiconductor, network equipment and Internet companies. Our members are global companies whose products and services support critical infrastructure across virtually all sectors.

Comments

Defining Critical Infrastructure

With increasing reliance of every sector on information technology to deliver goods and services, cybersecurity threats exist across all sectors. Because the *Security of Critical Infrastructure Act 2018* defines "critical infrastructure" as only electricity, gas, water and maritime ports, we agree that the current definition does not reflect the range of sectors critical to Australia's national security and economic prosperity. At the same time, we recommend that the framework elaborate more clearly on definitions for systems in each the sectors deemed critical in the current draft, as defining CII too broadly risks undermining the point of a targeted and careful cybersecurity regime.

A helpful definition of "critical infrastructure" (CI) defined in U.S. statute for over for 15 years and well-settled within the context of the U.S. Department of Homeland Security's public-private partnership activities with CI owners/operators can be found in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)):

> ***(e) CRITICAL INFRASTRUCTURE DEFINED***
>
> *In this section, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

We note that the draft identifies "data and cloud," but does not provide any further clarification on scope and definition, which makes it difficult for companies to understand to whom the positive reporting obligations would apply. It will be important that the Government is clear on what elements are captured as "business critical." "Data and cloud" can be supplementary to a broad number of services and sectors, not all of which carry inherent national security risks. A great deal of Internet-related activity is purely consumer or business-oriented and should not be considered "business critical." The Government should consider the *impacts* on national security related to the potential destruction of business critical elements when defining the term. Even within sectors that

are typically included in governments' considerations for protecting CI, such as telecommunications, a risk-based approach should be taken towards identifying those entities subject to enhanced CI regulation. For example, it might not be appropriate to apply additional regulation to services providers primarily reliant on the infrastructure owned or operated by other service providers. Relatedly, we commend the Australian Government's explicit assurance that any new requirements with respect to CI "build on and do not duplicate existing regulatory frameworks."

In addition, the COVID-19 crisis has reshaped many governments' thinking on what sectors are considered "essential" or "critical." In the United States, identification of CI is evolving from being primarily 'sector'-based to 'function'-based, in the belief that this approach more accurately conveys the interconnectedness of modern supply chains. COVID-19 also has led governments to think about the essential nature of companies that support essential services; that is, companies which might otherwise not be considered essential or critical, but which supply components or provide manufacturing services for essential activities and therefore should be covered under the same essential services guidance. It is appropriate that the Australian Government take a fresh look at the sectors or functions that have emerged as "critical" while also maintaining specificity to avoid undermining and overburdening security and assistance efforts.

Advancing Resilience

We support your efforts to enhance CI resilience through increased education and communication. It is important that the Australian Government also pursue coordinating within and strengthen pre-existing mechanisms and structures to defend its economy and security.

Alignment and Coordination

To advance the framework and its 2020 Cybersecurity Strategy, the Australian Government should seek appropriate changes to demonstrate leadership in security and provide a model for organizations as well as other governments. In particular, Australia could update its procurement policies (i.e. the Commonwealth Procurement Rules and the ASDEFCON Suite) to reference both cybersecurity and supply chain security risk. It is important for all Government departments to consider the security and integrity of the technology, goods and services as part of their procurement processes. This would demonstrate the Government's commitment to cybersecurity and supply chain risk management.

All departments should include cybersecurity in all key policy documents it produces, acknowledging the horizontal, cross-cutting nature of cybersecurity and cyber threats. It is extremely important to push for alignment of federal agency cybersecurity practices, including orientation of federal agency efforts to the final framework, which will in turn facilitate mapping of agencies' cybersecurity risks to their missions across the government. The Australian government should consider developing updated guidance for agencies to assess and manage risk for specific sectors. Any regulatory efforts by those same agencies should be streamlined to reduce regulatory redundancy.

Roles

The Australian Cybersecurity Centre (ACSC) should continue to have a prominent role in the framework and serve as a point of contact for industry on cyber. However, the Critical

Infrastructure Center (CIC) and the Trusted Information Sharing Network (TISN) could be strengthened to better assist in strategy and implementation around the proposed regulatory framework. The TISNs are well-positioned to increase education and communications efforts as it is representative of all CI sectors as well as Australia's various regions. TISNs may also be expanded to reflect any additional sectors that the Department of Home Affairs adds to its CI definition based on this consultation.

The TISNs can further many of the initiatives outlined in the consultation, including:

- facilitation of a government-industry secondment mechanism
- sharing best practices and convening expert briefings
- eliciting feedback on the regulatory framework and implementing appropriate changes

Furthermore, the ACSC should rely on the CIC and TISNs when it convenes industry for cyber exercises and events. The CIC and TISNs will require dedicated time and funding to implement these changes.

Increasing Awareness

Sector-specific guidance and guidance on emerging security techniques is only one component of improving and updating the current approach. We recommend that the Australian government prioritize communication of new guidance and be prepared to work with organizations on its use. The CIC and regulators should undertake extensive campaigns to raise awareness among organizations, states, and territory governments while also establishing mechanisms for feedback on the framework. This information campaign can include a range of activities such as workshops, webinars, and practical cyber exercises with implementers.

Many organizations are unable or unwilling to employ the newest technologies, which often also have some of the most up-to-date security features. It is important that in promoting a reinvigorated CI strategy and regulatory framework that the Australian government also encourage organizations to embrace new technologies, addressing worries about use of new tech. Practical and pragmatic guidance about how early adopters have successfully integrated state-of-the-art cybersecurity technologies would be useful, for example. This could be particularly helpful for utilities or other companies reliant on industrial control/SCADA systems. Other companies are also worried about disruption of their operational technology environments when integrating new technologies.

Strengthening Public-Private Partnerships

ITI supports continued strengthening of public-private partnerships (PPPs) and bolstering information sharing among industry and government in order to appropriately assess threats and prevent incidents. We appreciate that the Australian government is offering a framework that provides for voluntary information sharing as a means of testing these concepts, and in the longer term, we recommend that Australia also consult industry about the specific limitations and effectiveness of the information provided. It is important that the information requested can both be accessible to organizations at respective levels of capacity and protect any proprietary information of the commercial entity. The Australian government may refer to other PPP models that have proven effective, such as the ICT Supply Chain Risk Management (SCRM) Task Force led by industry and the Department of Homeland Security. The effort brings together various agencies

in the U.S. government and more than 40 industry partners to identify risks, produce policy recommendations, and develop a commonly understood framework.[1]

As the Australian government continues to contemplate creation or amendment of regulations, we would encourage that any regulation be designed with enough flexibility to accommodate technological developments. Highly prescriptive rules are not capable of accommodating new and evolving technologies. This jeopardizes the security of users and operators as operators may not be able to deploy the most up-to-date and efficient solutions and mechanisms. Hence a dynamic, risk-based approach to cybersecurity is demonstrably superior to prescriptive requirements. Before final publication, we would also encourage the Australian government to allow appropriate time for public consultation that includes all stakeholders.

Collaborative Tools

The Australian Government should consider establishing a program in which private sector experts can work alongside ACSC experts on a part-time basis at a declassified level.[2] This would be complementary to the TISN government-industry secondment mechanism and provide additional opportunities for government and industry to effectively collaborate. This strengthens education and awareness around real-world cybersecurity challenges.

Supporting Small and Medium Size Enterprises

ITI recognizes that not all companies have mature programs or the technical expertise to keep up with the latest developments in cybersecurity. Given the interconnected nature of the cyber ecosystem, we are keenly aware that cyber elements of the CI can be compromised by weaknesses in smaller entities to which they are technologically connected. Given this fact, it is critical for us to create a sustainably secure cyber ecosystem for all entities, large and small. Therefore, we recommend that the Department of Home Affairs work with interagency partners in the Australian government to better understand the cybersecurity and implementation challenges faced by organizations of all sizes and consider ways to make any framework approachable for all organizations.

The Department of Home Affairs should prioritize understanding the issues confronting theses smaller entities and addressing their unique concerns and needs. Developing this understanding will create a clearer picture of how certain practices can best meet the requirements and risk tolerances of organizations of various sizes across numerous industry segments. Along with respecting business needs such as cost effectiveness, this knowledge will help organizations become more likely to adopt processes that they know they can afford and are more readily applicable to their particular risk environments.

It may be helpful to specifically consider how to approach information sharing with small and medium sized enterprises, who may have more difficulty accessing information than larger, better-resourced companies. Australia is not alone in this challenge and may look to examples of other SME outreach programs. The National Telecommunications and Information Administration has recently initiated a "communications Supply Chain Risk Information Partnership" which will

[1] https://www.cisa.gov/ict-scrm-task-force

[2] International examples of such programs include the Industry 100: https://www.ncsc.gov.uk/information/industry-100

specifically target small and rural suppliers via a phased approach to ensure that these providers are aware and have access to vital supply chain information.[3]

International Standards

We recommend that Australia's policies continue to support and utilize globally recognized and state-of-art approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards. ITI would also recommend that Australia consider using other relevant tools that provide a common language to better help organizations comprehend, communicate, and manage cybersecurity risks (such as the U.S. NIST Framework[4] and NIST SP800-171). Furthermore, we recommend that any approach should be implemented in a way that is adaptive and risk-based. Any approach should recognize that not all organizations are alike – in size, scope, complexity, business, cyber-risk or sophistication.

We hope that Australia will continue to encourage appropriate government, industry, and academic participation in international standards development related to CI. The diversity of expertise engaged increases the likelihood that the resulting standard reflects the state of the art with regard to cybersecurity technical procedures, governance methods, and risk management operations. In its efforts to advance supply chain security, the ICT SCRM Task Force in the United States has made significant efforts to inventory and refer to industry-led, international standards development related to supply chain security. The Australian government should consider similar efforts to reference ongoing standards development before developing new standards-related workstreams and thus avoiding duplication. In building up cybersecurity expertise and capacity, we also encourage the government of Australia to look to international standards and best practices and consider tools like the NIST NICE Framework.[5]

Government Oversight and Authority

Our companies understand the importance of national security and the need for flexible, agile rules of the road to respond to emergencies. There should be precise definitions of both national harm and interest to determine where the government should intervene.

Emergencies and Precautions

The Australian government should work on developing a clear methodology for the determination of threat levels and "emergencies" to best understand where government intervention would be necessary**.** Among other safeguards and assurances, government should always seek to protect any related personal or proprietary information in responding to an imminent threat.

Governments should also be clear in providing timely notification and description of an imminent realized threat, along with objectives of their actions or of additional technical requests imposed on entities. To understand an "imminent threat," there must also be a clear and shared definition among all stakeholders of the threat classification. The consultation provides that certain factors will be considered, but more clarity is needed to understand responses with differing "potential

[3] https://www.ntia.doc.gov/blog/2020/ntia-announces-supply-chain-information-sharing-program
[4] NIST Cybersecurity Framework. https://www.nist.gov/cyberframework
[5] "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework" https://csrc.nist.gov/publications/detail/sp/800-181/final

consequences" to the Australian economy, security, or sovereignty. Any direct action in response to an emergency should require sign off at the highest levels of government (e.g., Ministerial level), and be cleared from all relevant ministries with cybersecurity responsibility, including Home Affairs and Defence. Related processes and responsibility for oversight of emergencies should not be over-classified and instead be transparent to the public.

The Government should address liabilities and immunities in the event that a government directed change adversely impacts other customers or causes an entity or their providers financial losses. It will be important to clarify whether immunities are afforded to CI sector subcontractors. For example, whether immunities would apply to a cybersecurity company that takes actions on behalf of their critical information client at the direction of the Government.

To stem the economic loss associated with cybercrime and the impacts of a widespread cyber attack, Australia should harden its national defenses and address these threats at scale via leveraging internet services providers (ISPs) to detect and stop cyber attacks in real time. ISPs and telecommunication providers should have constant real-time visibility across traffic passing through their networks and be able to detect and stop in real time cybersecurity threats within that traffic. This would significantly reduce the volume of malicious traffic targeting CI sectors and make Australia a less attractive target for cybercriminals.

Information Sharing

When providing information to the government, entities should be able to share threat intelligence anonymously and in real with the ability to highlight information for the attention of certain audiences. The Government should provide assurances that under no circumstances will they share information beyond the terms agreed, without the explicit consent of the original source of information. Threat information shared voluntarily with the Government should be used solely for cybersecurity purposes (e.g., regulatory purposes). The Government should ensure appropriate privacy protections and that threat information is not subject to the Freedom of Information Act. Failure to undertake these measures may impact the willingness of many companies to share information, for fear that it may make its way into the public domain.

We would also encourage the Australian Government to make more of an effort to declassify cyberthreat information and share in real-time with industry. This will provide industry with the information required to detect and prevent threats and mitigate significant economic harm. The Government should leverage the traffic light protocol[6] and educate CI sector contributors on its use and value.

The National Institute of Standards and Technology (NIST) conducted a thorough, multi-year process to bring together various stakeholders around a Framework for Improving Critical Infrastructure Cybersecurity[7] and has been similarly successful in the promotion of its Cybersecurity Framework. We recommend that the Australian government pursue a similar consultation and informational campaign to develop a robust framework.

[6] https://www.first.org/tlp//

[7] "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1" https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11