THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

Khang Nguyen

Master of Cyber Security Student

Former official in Ministry of Information and Communication Viet Nam

A submission for the National Cyber Security Strategy discussion paper

Queensland, 2023

Q1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

Ministry of Education and Training coops in academic operating courses to enhance Australia's cyber security workforce and skills pipeline. Scholarship for talented students from Australia as well as our allies and strategic regional such as ASEAN.

Minister for Government service along with **Finance minister** join together in investing in the cyber security ecosystem. A common cloud-base data center for SMEs could lift up the cost barrier for these type of companies and mitigate the risks as the Centre is run by cybersecurity specialist from ACSC or private sector.

Minister for Communications, Treasurer, Minister for Health, and Minister for Family and Social services promote Community awareness and victim support with adequate media campaigns, support packages, vitals supply reservations, etc

National Intelligence Office and **Department of Defense** establish a network of intelligence assets on the darknet, and cyber gangs and gather intel on every malicious activity such as money transferring, malware as a service, increasing payload to Australia networks, etc, especially from the former threats actors and hostile states to Australia.

Q2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

- ***Set heavy penalty disciplines for not abiding by the SOCI Act***. The penalty should be significant to the business as compliance with the act is mandatory. In UK, The Network and Information Systems Regulations 2018 (NIS) set the penalty for failure to comply with the duty to notify a NIS incident is up to £1,000,000[1]. In EU, up to €10 million or 2% of the entities' total turnover worldwide, whichever is higher[2] or in US, If the company fails to comply with the subpoena, the operators may be charged by the Department of Justice for civil action, potentially including contempt of court proceedings.[3]

Q6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

[1] NIS Regulations 2018 r.11

[2] NIS2 Directive Art. 20 (Directive on security of network and information systems to repeal and replace the EU's existing cyber security directive (Directive 2016/1148) -

[3] Cyber Incident Reporting for Critical Infrastructure Act s2220A(d)(1)

- ***Facilitating framework to assist SoNSs***, the Government has experts from ACSC to cooperate with the operator's sight monitoring and supervising in terms of risk management and response plan. This personnel also serves as a supervisor for the SoNS executing Minister's direction.
- ***Adapt industry best practices and standards for risk management and incident response*** instead of regulating rules. The Government should let the SoNS's operator freedom to choose what is the best model that suits the business's objectives.
- ***Leveraging cyber security exercises to national scale***, the SOCI Act regularly requires SoNS to perform cyber security exercises within itself and also cooperate with other SoNS as well. The government facilitating exercise environment (test-bed) for formulate response sequences in the event of an attack to the system.
- ***Fostering collaboration with other departments in terms of data and intelligence forensics as well as incidents response program.*** Many other authorities can cooperate with Department of Home Affair (DoHA) and ASD for example the AFP, they have launched the Joint Police Cybercrime Coordination Centre to respond to the escalating threat and prevalence of cybercrime and the significant cost to the Australian community.

Q7. What can government do to improve information sharing with industry on cyber threats?

- **Collaboration within the SoNSs.** SoNS operators in particular and Critical infrastructure asset (CIA) operators in general can form an association among themselves to share real-time data regarding cyber incident response plans and threats to the infrastructure. The DoHA may not share information collected from the SoNS and CIA operation with each other due to security features. However, a regime that fosters transparency between those operators will benefit greatly the resilience of their systems. The Act can nurture this regime by pioneering ACSC or Critical Infrastructure and Cybersecurity Centre as founders of such association.

Q8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

See Q7

Q13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?
a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

- ***Unify reporting mechanism to one single point of contact from the Government,*** the information is analyzed and shared with relevant authorities for further action. The data forensics This helps the victims react faster to the incidents, saving time and unnecessary action since the priority is initiating response actions to seize the breach.