Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

NOKIA Submission

Melissa Golledge,
Nokia
111 Pacific Hwy,
North Sydney NSW 2060,
Australia
[redacted]

23 November 2020

Dear Sir or Madam,

Thank you for the opportunity to comment on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* ("the Bill").

Nokia is the world's leading supplier of safe and secure, end-to-end communications technology for nation-building projects like 5G networks as well as solutions enabling growth and innovation at the enterprise level. We support the Australian Government's commitment to protecting essential services by enhancing the security and resilience of critical infrastructure. We raise the following for your consideration as you finalise the provisions of the new Bill and prepare to consult on the co-design of the principles animating the Positive Security Obligations ("PSO") for each sector:

Definitions of critical infrastructure sectors and critical infrastructure assets

Nokia supports the intention of the Bill and the expansion of sectors and assets deemed critical to national security and economic resilience (subject to considerations specific to the communications sector outlined below). As the economy becomes more connected in the move to 5G, safe and secure communications networks will be a key driver of innovation and growth across all industries. Communications will have the ubiquity of energy in terms of providing an essential input to businesses and the economy in the 21st century, so more entities across more sectors will need to actively consider cyber security and how best to mitigate associated risks.

Nokia also supports the proposed definition of "critical infrastructure asset" and the specific definitions in each "critical infrastructure sector" (again, subject to our specific comments on the communications sector below). However, we recommend the Department of Home Affairs ("the Department") periodically review these definitions, especially any features or thresholds within the definitions, to ensure provisions continue to cover assets as advances in communications and other technologies evolve the concept of "criticality."

Finally, we believe more education and advice for entities in sectors now considered "critical" for the purposes of national security will be vital to ensure they truly understand the new obligations and to help build a greater consciousness of security and resilience across essential sectors of the economy.

Interaction with the existing regulations for the telecommunications sector

For the communications sector specifically, Nokia's view is that 2017 reforms to the Telecommunications Act 1997 and current policy settings regarding the risk status of equipment vendors work well to protect the security of critical telco assets. We are keen to learn more about how the Bill's new provisions are intended to work with this existing regime, noting the Government's intention (expressed in the Explanatory Document), to avoid duplicating regulation.

We also note that the Telecommunications Act 1997 is currently the subject of a review by Joint Parliamentary Committee on Intelligence and Security and trust the findings of this review will also help inform the final approach to regulation in the communications sector. Nokia looks forward to participating in this review and to assisting the Department by sharing intelligence and insights on the global cyber risk environment and the mitigation strategies our technology enables for carriers and associated entities.

Positive Security Obligation (PSO)

Nokia broadly supports the concept of co-designing sector-specific principles to give effect to the PSO, as this approach is likely to result in requirements that reflect the particular risks in each sector; that are proportionate to those risks; and that avoid duplicating existing regulation.

To the extent communications networks in the new critical infrastructure sectors may introduce a source of cyber risk, we believe it would be helpful for the Department to consult with vendors like Nokia during the co-design process. This would ensure sector-specific PSOs address the full range of risks and would help achieve the Bill's intention to increase both security and resilience.

Furthermore, we understand it is the Department's intention to work closely with relevant industry associations regarding the co-design of PSO principles for each sector. While we understand this approach will expedite the process of developing principles, we are concerned the Department may not gain a comprehensive picture of risks and effective mitigations unless it also engages more directly with entities subject to the PSO and those businesses providing essential infrastructure and products to those entities, such as Nokia.

Systems of national significance

Nokia agrees in principle that there are assets that are especially critical to national security, sovereignty and the economy and that these systems should be subject to additional, bespoke obligations. However, we would appreciate more clarity about the exercise of the power to declare a "system of national significance" in the context of the communications sector, given the existing regulatory regime that already applies here.

Indirect impact of the Positive Security Obligation

While Nokia appreciates the Bill does not intend to cascade new obligations through supply chains in critical infrastructure sectors, our understanding of the new provisions is that a responsible entity should have a thorough understanding of suppliers, vendors and partners in order to meet the PSO. For example, it will be difficult - if not impossible - to develop a "critical infrastructure risk management program" that accurately identifies material risks, mitigates these risks and provides for effective governance without knowing, at the very least, the security and supply chain resilience strategies of the parties with whom a responsible entity does business.

For the communications sector itself and for communications projects in other critical infrastructure sectors, Nokia's view is that suppliers and vendors should work with responsible entities on fulfilling the requirements of the PSO. This is the optimal way for both responsible entities and the Department to develop a comprehensive understanding of unique risk and resilience profile of a particular asset.

Nokia firmly believes producers of telecommunication equipment should actively monitor their products and supply chains for security risks. To this end, we undertake extensive monitoring and testing of our products, at all stages from inception and during development, manufacturing, deployment and maintenance. All Nokia products and our supplies are subject to the same security verification procedures to ensure their integrity, regardless of their place of development, manufacture or operation.

Our multi-stage production chain greatly minimises the possibility of supply disruption and malicious interference with our equipment. Nokia's suppliers are also subject to our stringent security verification programs when they become part of our supply chain. These practices are derived from more than 150 years of impeccable ethical business conduct.

Our global leadership in the development and supply of communications technology is built on the assurance we give our customers on the security and quality of our equipment. Because of this, Nokia customers will be able to rely on the security profile of our equipment and our transparent, resilient supply chains for the purposes of demonstrating their compliance with the PSO.

Thank you again for the opportunity to comment on the Exposure Draft of this Bill. Nokia looks forward to participating in the consultation on the co-design of the principles informing the PSO. If you would like to discuss this submission further or require additional information, please don't hesitate to contact me.

Yours sincerely

Melissa Golledge
Head of Marketing and Communication
Oceania