U.S. CHAMBER OF COMMERCE

1615 H Street, NW
Washington, DC 20062-2000
www.uschamber.com

December 13, 2018

Ms. Ajarin Pattanapanchai
Permanent Secretary
Ministry of Digital Economy and Society
120 Moo 3, 6-9 floor
The Government Complex Commemorating His Majesty
Chaeng Watthana Road, Thung Song Hong, Khet Laksi
Bangkok 10210

By email to:
ajarin.p@mdes.go.th
sataporn.s@mdes.go.th
darunee.p@mdes.go.th

Dear Ms. Ajarin Pattanapanchai:

The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing the interests of more than three million businesses of all sizes and sectors, many of whom are major employers and provide significant investment in the Thai economy. We welcome the opportunity to provide comments to the Government of Thailand's National Cybersecurity Preparation Committee regarding the draft Cybersecurity Act ("the Act").

The Chamber considers cybersecurity to be a top priority. Network systems today underpin many of the most critical systems in our respective economies. These systems must be adequately protected against cyber threats if we are to ensure that the benefits created by the digitization of our economies are not outweighed by the risks.

Accordingly, the Chamber has worked with more than 30 governments to develop and implement cybersecurity solutions that ensure appropriate levels of cybersecurity for businesses of all sizes and in all sectors of the economy. This engagement has afforded us the opportunity to see first-hand what makes for effective cybersecurity policy.

One particular message has resonated: governments and businesses face shared, cross-border cyber threats. Unnecessary divergence in the regulatory responses of likeminded governments makes our defenses weaker, and our adversaries strong. As such, we support international efforts aimed at aligning regulatory approaches to better reflect globally-accepted best practices.

While much of the content of the Act aligns with international best practices, there are certain areas where we believe the text could be improved, to better enable the ultimate goal of improving cybersecurity in Thailand. Accordingly, we offer the following recommendations.

Align Security Measures with International Standards

Where possible, cybersecurity policies should rely on existing standards from ISO, IEC, OECD, UL and other high-quality international standards bodies meeting the WTO TBT principles. Examples include the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (and the forthcoming ISO/IEC 27103) and ISO/IEC 27001.

Sections 11, 12 and 47 of the Act reference developing minimum standards for critical infrastructure – implying that these will be unique to Thailand. The Chamber strongly recommends that the Government of Thailand not develop its own minimum standards for critical information infrastructure ("CII") operators, for the following reasons.

Firstly, the nature of cyber threats is constantly evolving as attackers become more sophisticated and adapt their methods to overcome the defensive measures taken by CII operators. Effective cybersecurity practices must therefore be iterative in nature, in order to defend against new and improved tactics of aggressors. Codifying minimum standards in response to today's threats will only serve to constrain the ability of CII operators to adapt their activities in response to tomorrow's threats.

Secondly, the threats that CII operators in Thailand face are not materially different from those faced in the U.S. and other major economies. There is therefore no need for Thailand to impose requirements on CII operators that diverge from the international standards utilized by CII operators in those countries.

By developing standards at the national level, Thailand will create regulatory divergence, which inhibits the ability of CII operators to deploy best practices seamlessly across borders. This in turn increases the compliance burden – forcing companies to divert precious cybersecurity resources away from operational activities – and creates 'blindspots' when responding to cross-border threats. In short, it aids cyber attackers, while hampering CII operators.

A more effective approach would be for Thailand to collaborate with the private sector to identify existing, or develop new, consensus-based international standards that are technically sound and comprised of objective assessment criteria to deliver on cybersecurity policy objectives. This builds upon the international standards principles established by the WTO TBT Agreement, facilitates the harmonization of standards and certification schemes across borders, facilitates trade in connected products and stimulates innovation in industry.

Recommendation: The Chamber strongly recommends that Thailand not seek to develop unique national minimum requirements for CII operators, given the counter-productive impact of this approach. Rather they should collaborate with the private sector to identify or develop international standards that can serve as best practices for CII operators.

Narrow the Designation of Critical Infrastructure

We broadly agree with the Government of Thailand's choice of sectors to designate as critical infrastructure in Section 44 of the Act. They are broadly aligned with international best practices and make sense in the context of Thailand. Nevertheless, the Act does not outline a methodology for identifying which companies within those sectors are critical to Thailand's national or economic security. As a result, entire sectors of the economy risk being wrapped up in the requirements of the Act.

Such overly broad designations dilute finite regulatory resources, create unnecessary compliance burdens - in particular for small and medium enterprises - and make the country less attractive destination for foreign investment in these sectors. If everything is critical, nothing is critical.

By way of reference, the United States - which has a population, land mass and economy far larger than that of Thailand – has identified fewer than 100 companies as owners or operators of critical information infrastructure.

Recommendation: The Chamber recommends that the government, through secondary legislation if necessary, narrow the designation of critical infrastructure entities to encompass only the most critical systems within each of the sectors identified. Doing so will ensure that public and private resources are directed to where the cyber risk is greatest.

Ensure Incident Reporting Requirements are Sufficiently Narrow

Sections 52 and 53 outline a 3-tiered structure for assessing the severity of a cyber attack. There is nothing concerning about such an approach. We would, however, make the following suggestions regarding the development of incident reporting requirements:

Firstly, given the transnational nature of most cyber attacks, we would encourage the Government of Thailand to adopt an approach that does not materially diverge from those of other major countries. Following a cyber incident, CII operators will be attempting to implement their strategy for responding to, and recovering from, the incident in circumstances which are challenging, at best. Divergence between countries in terms of thresholds for cyber incidents only serves to make incident response more challenging.

Secondly, we would strongly recommend that Government of Thailand avoid imposing mandatory reporting at the lower thresholds of cyber attack, as suggested in Section 52. It is not uncommon for major institutions to face millions of cyber attacks per day – a number of which may breach the institution's perimeter, while posing no threat to the confidentiality, integrity or availability of critical systems. Requiring disclosure of each instance would not only force companies to divert resources towards compliance, and away from operational activities, it creates unnecessary "noise" for governmental agencies, making it more difficult for them to fulfill their mandate.

Thirdly, whether in threat information sharing or cyber incident reporting, it is our experience that the most valuable and actionable information is shared where it is voluntary to do so, and where CII operators have liability protections in place. Allowing private sector experts to identify the most pertinent information and report it without fear of repercussions is the basis of the most sophisticated information sharing entities such as ISAC networks in the U.S.

Recommendation: The Chamber recommends that Thailand align its thresholds for measuring the severity of an attack with international best practices, to avoid the kind of unnecessary regulatory divergence that inhibits incident response. Further, we strongly recommend that most, if not all, thresholds allow for voluntary incident reporting to ensure that there is not unnecessary "noise" created which inhibits the work of public and private stakeholders.

Make Preparatory Cyber Programs Voluntary

Section 50 of the Act says that CII operators "shall participate in the testing of availability status in dealing with Cyber Threats held by the Office."

While programs such as cyber exercises, war games and audits can be valuable in enabling companies to improve their cyber defenses and incident response, their utility is dependent upon the relevance of that activity to a particular CII operator. Where an activity is not of relevance, a CII operator is better served devoting resources to other activities which materially improve the cybersecurity of their systems. In such instances, they should not be required to take part.

Recommendation: The Chamber recommends that Thailand move forward with the programs referenced above but make participation voluntary. Through engagement with the

private sector during the development of such programs, NCSC can ensure the relevance of such programs to a broad range of CII operators.

Remove Provisions Allowing Forceful Government Intervention after a Cyber Incident

Sections 55-59 of the Act grant the NCSC and Secretary-General unnecessarily obtrusive authorities with insufficient judicial oversight.

Public-private partnerships are at the core of effective cybersecurity initiatives, including incident response. Our member companies routinely coordinate and cooperate with governments around the world as they seek to ensure the resilience of the systems that they operate against cyber attacks. Moreover, the governments with whom they work rely upon their expertise, not least in the midst of cyber incidents.

The extension of these powers not only undermines the trust and cooperation which underpins such partnerships, it shows scant regard for the value of private sector expertise in responding to cyber incidents. Were the government to utilize these powers, in particular those outlined in Section 59, it would represent an unacceptable expropriation of private assets by the Government of Thailand. This would almost certainly have a chilling effect on Thailand's investment environment, and thus its economy 4.0 objectives.

Recommendation: The Chamber understands that these powers are being reviewed by Committee Members in response to stakeholder concerns. We strongly recommend that these powers be removed and/or subject to significantly greater judicial oversight.

Victims of Cyber Attacks should not be Subject to Criminal Penalties

Sections 67 and 68 of the draft law propose overly onerous penalty provisions for non-compliance. Those which allow for imprisonment of individuals acting in a professional capacity, in particular, fall outside of international norms and will raise significant concerns for companies with employees in Thailand.

Such criminal liability of this nature is disproportionate and, combined with personal liability for corporate officers, raises the cost of operations, insurance, and compliance, which dis-incentivizes companies to invest in Thailand. Criminal liability should be reserved for perpetrators of attacks, rather than those actors working to protect Thailand's critical infrastructure. Not only do such penalties punish the wrong party, they create a significant disincentive for investment in Thailand.

Recommendation: We recommend that Thailand remove all criminal liabilities from the Act and instead rely on fines or injunctive relief as a means to promote compliance.

Conclusion

We thank you for your consideration of the above comments. The Chamber firmly believes that a well-crafted cybersecurity strategy is the basis upon which sustainable digital growth must be built. We look forward to working with you to implement such a strategy, which will facilitate further growth in Thailand-U.S. trade ties.

Sincerely,

John Goyer
Executive Director
Southeast Asia Program
U.S. Chamber of Commerce

Sean Heather
Vice President
Center for Global Regulatory Cooperation (GRC)
U.S. Chamber of Commerce