



Mr. Adisorn Pimolrat  
The National Cyber Security Agency (NCSA)  
120 Moo 3, Rattthaprasasanabhakti Building (Building B), 7th Floor,  
Government Complex Commemorating His Majesty the King's 80th Birthday Anniversary,  
Chaeng Watthana Road, Thung Song Hong, Laksi, Bangkok 10210, Thailand  
Sent via email to [EOL@ncsa.or.th](mailto:EOL@ncsa.or.th) and [saraban@ncsa.or.th](mailto:saraban@ncsa.or.th)

31 July 2025

Dear sir,

**Re: Feedback on the Draft Amendment to the Cybersecurity Act B.E.2562 (2019)**

The Coalition for Cybersecurity in Asia Pacific (CCAPAC) is a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building.

We understand that the National Cyber Security Agency (NCSA) is in the process of inviting comments on the Draft Amendment to the Cybersecurity Act B.E. 2562 (2019).

We applaud Thailand for introducing the amendments to strengthen Thailand's cybersecurity framework.

In light of the proposed amendments, we would like to offer several observations and recommendations to ensure that cybersecurity governance and resilience are adequately addressed.

- 1. Clarifying the scope of Critical Information Infrastructure functions and activities.** The amendment specified that private sector entities serving or holding data for designated Critical Information Infrastructure (CII) Agencies would be considered as CII agencies. To provide greater certainty to businesses, it would be helpful to clarify that only computer systems and infrastructure directly supporting the functions outlined in Section 3—namely, activities related to national security, international relations, economic and military security, public safety, or infrastructure of public benefit—would fall within scope. Day-to-day operational systems, such as word processing or HR platforms, should be excluded. This distinction will support efficient resource allocation by enabling the NCSA to focus on regulating systems that are truly critical in nature.
- 2. Promoting the use of internationally recognised standards for cybersecurity products and services.** Section 9 of the amendments empowers the National Cyber Security Commission (NCSC) to set minimum standards for computers and computer systems. We encourage the NCSC to adopt internationally recognised standards—such as the Common Criteria (CC), as well as standards developed by the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC), and other relevant international bodies. Leveraging such standards, rather than developing bespoke domestic ones, can help reduce compliance costs and improve operational efficiency.



To promote consistency and interoperability, we also recommend that the scope of certifying bodies include internationally accredited testing laboratories, rather than being limited to entities based in Thailand.

3. **Clarifying cybersecurity incident reporting thresholds.** Section 3 of the amendments defines a cyber incident as an unlawful act or operation involving a computer system, device, or data that "is expected to cause damage or impact the confidentiality, integrity, or availability of those systems". In Section 58, it also introduces an obligation for CII agencies to report cyber incidents that have "occurred or are expected to occur" within 24 hours "from the time the inspection results are known".

While we support timely reporting of cybersecurity incidents to the NCSA, we recommend that reporting be limited to incidents that have actually occurred. Given the high volume of daily security alerts, requiring reports based on anticipated incidents may lead to over-reporting and dilute the value of incident notifications. To improve the effectiveness and practicality of reporting, we recommend the NCSA to:

- Clearly articulate the purpose of reporting
- Establish a reporting threshold with defined criteria. For example, the US Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) provides clear definitions of cyber incidents which require reporting<sup>1</sup>
- Align incident reporting timeframe with international norms. For instance, CIRCA, EU's revised Network and Information Systems Directive (NIS 2), and in Australia's amended Security of Critical Infrastructure Act (SOCIA Act) generally prescribe a 72-hour reporting period from the time of discovery.

We believe that these recommendations can help provide clarity and strengthen the cybersecurity regulatory landscape in Thailand. We would be happy to have the opportunity to discuss these suggestions further and collaborate with NCSA on future cybersecurity regulatory developments.

Sincerely,  
Lim May-Ann  
Director  
Coalition for Cybersecurity in Asia Pacific  
[ccapac@accesspartnership.com](mailto:ccapac@accesspartnership.com)

---

<sup>1</sup> <https://www.cisa.gov/sites/default/files/2024-05/24-0630-CCI-One-Page-20240410-2-508c.pdf>