15 August 2025

BSA RECOMMENDATIONS ON PROPOSED AMENDMENTS TO THE NATIONAL CYBERSECURITY LAW

On behalf of the Business Software Alliance (**BSA**),[1] we appreciate the opportunity to provide our recommendations on Thailand's Proposed Amendments to the National Cybersecurity Law (**draft Cybersecurity Bill**) to the National Cyber Security Agency (**NCSA**). BSA continues to engage extensively on cybersecurity issues in Thailand, including the most recent event where NCSA and BSA co-hosted the roundtable discussion "Cloud and Security: Shaping Thailand's Digital Future with Smart Policies" on 6 May 2025. BSA also commented extensively on the 2019 Cybersecurity Bill.[2]

BSA is the global trade association of the enterprise software industry. Our member companies are leaders in artificial intelligence, cybersecurity, cloud computing, and other cutting-edge technologies. BSA hopes to continue our longstanding collaboration with the NCSA, and we offer our extensive global experience in technology policy to serve as a resource. We hope that our recommendations below will be helpful to the Government of Thailand as you amend the National Cybersecurity Law.

Definitions

Based on our understanding, Section 3 of the draft Cybersecurity Bill defines a **Cyber Threat** as an "unlawful act or operation using a computer, computer system, or computer data, whether from within or outside the country, that occurs to a government agency, regulatory agency, critical information infrastructure agency, or private critical information infrastructure agency and **may cause damage to or impact** the ability to maintain the confidentiality, integrity, or availability of a computer, computer system or computer data or other relevant information of the agency" (emphasis added). Section 3 further defines a **Cyber Incident** as "any unlawful act or action using a computer, computer system, or computer information, whether from within the country or outside the country, that occurs to a government regulatory agency, government critical information infrastructure agency, or private critical information infrastructure agency and **causes or is expected to cause damage or impact** on the ability to maintain the confidentiality, integrity, or availability of the computer, computer system, or computer data or other related information of such agencies" (emphasis added). We commend the NCSA's intent to distinguish between cyber threats and cyber incidents, which is an important step toward ensuring a targeted and effective cybersecurity framework. However, the distinction between the two categories will

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] See BSA Comments on Dec 2018 Version of Thailand's Personal Data Protection and Cybersecurity Bill, 30 Jan 2019 at https://www.bsa.org/policy-filings/thailand-bsa-comments-on-dec-2018-version-of-thailands-personal-data-protection-and-cybersecurity-bill; BSA Comments on Nov 2018 Version of Thailand's Cybersecurity Bill, 29 Nov 2018, at https://www.bsa.org/policy-filings/thailand-bsa-comments-on-nov-2018-version-of-thailands-cybersecurity-bill; and BSA Comments on Sep 2018 Version of Thailand's Cybersecurity Bill, 11 Oct 2018 at https://www.bsa.org/policy-filings/thailand-bsa-comments-on-sep-2018-version-of-thailands-cybersecurity-bill.

be clearer without the inclusion of the phrase "or is expected to cause" in the definition of Cyber Incident which blurs the lines between an actual cyber incident and a potential incident that is a threat.

Recommendation: The definition of **Cyber Incident** should not include an act or operation that is expected to cause damage or impact, only those that actually cause damage or impact.

A Cyber Incident should not include ***expected*** damage or impact as this should be classified as a Cyber Threat instead. This clearly distinguishes a potential threat from an actual incident, ensuring that obligations like reporting are triggered by actual events.

Section 3 defines **Critical Information Infrastructure** (**CII**) as "a computer or computer system used by a government agency or a private agency in its business related to the maintenance of state security, international relations, economic security, military security, public safety or public order, domestic security, or infrastructure in the public interest." This definition of CII is broad and could include many non-critical services that are related to the maintenance of the various forms of national security that may not result in disaster if the organization suffers a cybersecurity incident.

Recommendation: The definition of CII should make clear that the relevant computer or computer system (including network systems and related assets) must be **essential to the function** of the public or private sector agency and its role in maintaining state security and related critical functions. A computer or computer system should NOT be considered CII simply because it is used by such an agency if the system is not essential for the agency's function as a critical infrastructure operator. In other words, a computer or computer system should only be considered CII if its loss, disruption, or destruction would have a debilitating impact on the critical agency's functions in maintaining or securing national security interests and related critical infrastructure.

Scope of Covered Entities

Section 22 of the draft Cybersecurity Bill amends Sections 48 and 49 of the National Cybersecurity Law and confers the supervisory board (**Board**) the power to designate public and non-public entities as CII agencies whose missions or services are provided in the fields of state security, important government services, finance and banking, information technology (**IT**), telecommunications, transportation and logistics, energy and public utilities, public health, industry, and other aspects as further determined by the Board. Further, a private entity assigned to store or possess information of such CII agencies shall be considered as a CII agency and have the same duties and responsibilities as other designated CII agencies.

The scope of sectors is very broad, allowing the Board to designate a wide variety of entities as CII agencies. It is important that the Law specify criteria that narrows the scope of entities operating in such fields that may be so designated. The Law should make clear that only entities that are so vital to Thailand's national security that the incapacity or destruction of the relevant systems and assets of such entities would have a debilitating impact on security, national economic security, national public health, or national safety.

Furthermore, many of the private sector entities offering IT services to designated CII agencies, including cloud service providers (**CSPs**), also offer such services to a wide variety of customers which are not CII agencies. Therefore, it is important that the law clearly states that such IT providers and CSPs are not considered CII agencies per se but are only obligated to assume relevant duties and responsibilities, **as directed by their CII agency customers**, to the extent that they are, and in the context of, providing services that are necessary for the continuous

delivery of an essential service offered by their CII customers. In other words, the responsibilities and obligations should be borne by the CII agencies themselves. To the extent relevant, CII agencies should provide clear instructions related to such responsibilities and obligations to their IT providers, including through contractual obligations.

Recommendation: The draft Cybersecurity Bill must provide **clear criteria for identifying the CII agencies and the private sector organizations responsible for supporting the obligations of designated CII agencies**. These entities should be limited to essential service providers whose assets, if disrupted or compromised, would have a serious impact on public services, national defense, economic security, or public safety in Thailand. Private entities providing IT and cloud services to designated CII agencies should not be directly regulated by the National Cybersecurity Law and its provisions but instead should take on responsibilities and obligations as instructed by their designated CII agency partners, for example via contractual arrangements.

Recommendation: **The IT sector should not be separately designated as a category of critical infrastructure** as it is more appropriately viewed as an enabler that supports other businesses and industry sectors, including some critical sectors and CII agencies, such as finance or energy, which may themselves be classified as critical infrastructure. We recommend removing the IT sector from the list within the proposed revised Section 49.

If NCSA, nonetheless, designates third-party IT service providers as CII, we urge NCSA to ensure that the process for any such designation is conducted through a transparent and collaborative process with the potential designee. We recommend that NCSA gives the potential designee advance notice of such designation and the opportunity to challenge such potential designation through a formal consultation process. We also encourage NCSA to provide the designee with the ability to meaningfully challenge such designations after the fact. Further, we recommend that such designations be revisited on an annual or bi-annual basis to ensure they remain relevant and proportionate to the evolving threat landscape and technological capabilities.

Incident Reporting Requirements

Section 25 of the draft Cybersecurity Bill amends Sections 56-58 of the National Cybersecurity Law; revised Section 57 requires the CII agency to report "serious" and "critical" cyber incidents (refer to amended Section 60) to the NCSA and take action to respond to the cyber incident in accordance with prescribed rules, and when the incident affects the information system of a structural agency, further requires annual reporting of cyber incidents.

Revised Section 58 requires that, in the case where a cyber incident has occurred **or is expected to occur**, the CII agency is required to take steps to prevent and reduce the risk of similar cyber threats and incidents in the future, including by responding to the cyber incident that is occurring (or is expected to occur), and to **notify the NCSA within 24 hours**.

Recommendation: The thresholds and timelines for incident reporting should be guided by clear principles set out in the legislation rather than left to be specified in implementing guidelines.

First, the legislation should clarify that **only designated CII agencies**, whether government or private agencies, that are the victims of a cyber incident **are required to report cyber incidents**.

Second, **only cyber incidents that have actually occurred should be required to be reported**. Incidents that are merely "expected" to occur should not incur mandatory reporting requirements.

Third, the requirements should be risk-based, such **that only cyber incidents that are significant and compromise a CII agency's ability to deliver critical functions are required to be reported**. Threats and suspected activities or occurrences that only risk, jeopardize, or otherwise make a cyber incident more likely should not incur an obligation to be reported.

Finally, in major cybersecurity incidents, the first 24-48 hours involve a combination of ongoing investigation and analysis, with assessments changing in real time as new facts are uncovered. For example, the US Department of Defense defines "rapidly report" to mean "within 72 hours."[3] Short-term, mandatory reporting takes responders away from the investigation and response effort, which harms everyone relying on that service. Although there are some jurisdictions and sector specific regulations with incident reporting periods shorter than 72 hours, a 72-hour reporting period is widely accepted as a reasonable window of time. Moreover, the 72-hour period has not been proven to be problematic, and it is sufficient to meet governments' needs for transparency and visibility into a cybersecurity incident. Therefore, **the notification timeline of 24 hours for preliminary information should be extended to 72 hours** from when the CII agency — which is best positioned to assess whether an incident has impacted the efficiency of critical services — becomes aware that a notifiable cyber incident has occurred.

To address the ambiguity in the draft bill, we recommend incorporating clear, risk-based definitions for different levels of incidents. The legislation should clearly define **a Critical Cyber Incident** to include only those incidents that have caused a significant disruption to the continuous delivery of essential services, compromise of critical data, or serious impact on national security, public safety, or the economy. **Serious cyber incidents** should be defined to include only those that have caused material degradation of essential services or compromise of sensitive information, but without the broader impacts of a Critical Cyber Incident. Adopting these definitions will align reporting obligations and the severity of the incident.

Recommendation: Section 26 of the draft Cybersecurity Bill amends Section 60 of the National Cybersecurity Law and defines three categories of cybersecurity incidents, including Critical and Serious Cyber Incidents as referenced above. It is helpful to distinguish different levels of severity in cybersecurity incidents and tailor obligations and for responding accordingly. However, revised Section 60 creates a category defined as "Non-serious cyber incident." This type of "incident" is defined as a "cyber incident that has a significant ***risk*** of causing an impact to the country's critical infrastructure or ***degrading the provision of government services or making the provision of such services inefficient***" (emphasis added). The category of "non-serious" cyber incident is inappropriate to include in this section because it describes a "risk" of an incident, otherwise defined in the draft Cybersecurity Bill itself as a "Cyber Threat" (see above regarding Section 3). Therefore, **we recommend removing the category of "non-serious cyber incident" from Section 26 of the draft Cybersecurity Bill amending Section 60 of the National Cybersecurity Law and adjusting all other relevant provisions in the draft Cybersecurity Bill accordingly.**

[3] See 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, 17 January 2025 at https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

For more information and guidance on how to best craft cybersecurity incident reporting, please see BSA's 10 Principles for Cyber Incident Reporting Harmonization Around the Globe.[4] In this document, we lay out the following principles and the justification for our recommendations:

1. **Align domestically,**
2. **Define "reportable cyber incident" consistently,**
3. **Apply only to the business (entity or agency) that is the victim of a reportable cyber incident,**
4. **Commence reporting requirements based on the same knowledge threshold,**
5. **Standardize timeframes,**
6. **Collect the same information,**
7. **Designate a single government agency responsible for receiving all cyber incident reports,**
8. **Use information obtained in cyber incident reports only for cybersecurity purposes,**
9. **Protect information from public disclosure and share only anonymized analysis, and**
10. **Create reciprocity mechanisms a business's cyber incident report to one government satisfies its reporting requirements to other governments.**

Broad Regulatory Powers

Section 31 and 32 of the draft Cybersecurity Bill amend Sections 65 and 66 of the National Cybersecurity Law and grant broad power to the NCSA to issue orders to the property owner affected by a cyber incident. The powers include the authority to access computer systems, inspect premises, implement remedial measures, and seize computers and related equipment in connection with serious and critical cyber incidents.

Recommendation: While Sections 65 and 66 include the term "where truly necessary" in regard to the authorities issuing such orders, **the legislation should define serious and critical cyber incidents precisely such that the authorities exercise their powers within appropriate limits**.

We recognize the government's interest in protecting critical assets and enabling swift responses to major cyber incidents. However, **direct intervention risks undermining these objectives**. In most cases, **individual organizations are best positioned to respond effectively**, given their deep understanding of their own systems, configurations, and threat environments.

Government teams require significant time to assess a live incident, understand the technical landscape, and make informed decisions — delays that could hinder containment and recovery. A more effective approach is to **empower organizations to lead incident responses**, with government support as needed.

Recommendation: The proposed Section 69 of the National Cybersecurity Law (as amended by Section 32 of the draft Cybersecurity Bill) allows an appeal against an order by the NCSA only if it is a non-serious cyber incident (see our recommendation above regarding this category of "incident"). We recommend **allowing appeals for serious and critical cyber incidents**. However, the entity making the appeal should continue to cooperate with the authorities and make best efforts to mitigate any damage caused by the cyber incident.

[4] 10 Principles for Cyber Incident Reporting Harmonization Around the Globe, BSA, February 18, 2025 at https://www.bsa.org/policy-filings/global-10-principles-for-cyber-incident-reporting-harmonization-around-the-globe

Conclusion

BSA thanks the NCSA for considering our recommendations on the draft Cybersecurity Bill. We welcome proposed amendments to establish baseline cybersecurity standards and encourage the NCSA to continue engaging industry stakeholders in setting practical, internationally aligned standards and practices. BSA and our members remain ready to contribute to this dialogue. Please do not hesitate to contact me at waisanw@bsa.org or +65 9729 1253 to make arrangements. Thank you once more for your time and consideration.

Yours sincerely,

Wong Wai San
Senior Manager, Policy – APAC