USTDA
U.S. TRADE AND DEVELOPMENT AGENCY

AFTER ACTION REPORT:

U.S. – THAILAND CYBERSECURITY DATA PROTECTION AND STANDARDS WORKSHOP

March 3-5, 2021

US-Indio Pacific Standards and Technology Cooperation Program (STCP)
Contract No.: 1131PL19CCP31207)

Produced by the **American National Standards Institute (ANSI)**
under sponsorship of the **United States Trade and Development Agency (USTDA)**

APRIL 2021

This report was funded by the U.S. Trade and Development Agency (USTDA), an agency of the U.S. Government. The opinions, findings, conclusions, or recommendations expressed in this document are those of the author(s) and do not necessarily represent the official position or policies of USTDA. USTDA makes no representation about, nor does it accept responsibility for, the accuracy or completeness of the information contained in this report.

USTDA

U.S. TRADE AND DEVELOPMENT AGENCY

The U.S. Trade and Development Agency

The U.S. Trade and Development Agency helps companies create U.S. jobs through the export of U.S. goods and services for priority development projects in emerging economies. USTDA links U.S. businesses to export opportunities by funding project planning activities, pilot projects, and reverse trade missions while creating sustainable infrastructure and economic growth in partner countries.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On March 3-5, 2021 the American National Standards Institute (ANSI), through the United States Trade and Development Agency (USTDA) funded U.S.-Indo-Pacific Standards and Technology Cooperation Program (STCP), coordinated the U.S.-Thailand Data Protection and Cybersecurity Standards Workshop. The hybrid workshop took place online via Zoom, and in-person at the Intercontinental Bangkok Thailand.

Below are key highlights from the workshop:

- Co-organizers included The Software Alliance (BSA), AmCham Thailand, and the Thailand Ministry of Digital Economy and Society (MDES) with significant contributions from the National Cyber Security Agency (NCSA) and the Office of the Personal Data Protection Committee.
- Nine U.S. companies were represented in the agenda while 27 total U.S. firms participated in the workshop; as well as 4 U.S. government agencies and 2 U.S. research and development organizations.
- Ms. Ajarin Pattanapanchai, Permanent Secretary of the Ministry of Digital Economy and Society, and Michael Heath, Charge ď ’ Affaires, U.S. Embassy gave opening remarks.
- Four representatives from the Thailand government delivered remarks, including speakers from the Office of the Personal Data Protection Committee and the National Cybersecurity Agency Working Group.
- Almost 600 individuals participated in the workshop, with the majority being Thai government and industry representatives.
- 84% of all surveyed participants indicated that the workshop met their objectives in attending.
- 75% or more of surveyed U.S. companies believe that the workshop will improve or greatly improve international best practices, national cybersecurity strategies, and advanced technology in Thailand. Over 90% of surveyed U.S. companies indicated that the workshop will at least somewhat improve all five topics, including personal data protection and information and digital policy and data governance.
- Several noteworthy outcomes are in development after this workshop including the following: The Software Alliance has continued to engage with the Government of Thailand to discuss the implementation of the Personal Data Protection Act, and is looking to step up engagement directly with MDES. A U.S. company has also started working with several organizations, including BSA and the U.S.-ASEAN Business Council to maintain engagement with the Thai government on digital issues. Discussions related both to the implementation of the PDPA and Thailand's participation in an ASEAN Cross Border Data Transfer mechanism are ongoing. Overall, statements from the Thailand government regarding policy approaches to privacy, data protection, and cross-border data flows are encouraging.

This Public Report includes the following elements: (i) Executive Summary, (ii) Final Agenda, (iii) Detailed Workshop Summary including technical analysis and links to workshop photos and presentations, (iv) Participant and Stakeholder Feedback.

FINAL WORKSHOP AGENDA

U.S.-Thailand Cybersecurity and Data Protection Standards Workshop

INTERCONTINENTAL BANGKOK| VIRTUAL VIA ZOOM
Bangkok, Thailand| March 3-5, 2021

To submit and vote on questions, use your smartphone or computer to join us at slido.com | #ANSI

<u>Day 1</u>

7:30-8:00AM: On-site Registration / Log into virtual Zoom Workshop.

8:00AM **Welcome and Opening Remarks**
Brandon Megorden, Regional Manager for Asia, U.S. Trade and Development Agency (USTDA)
Michael Heath, Chargé d' Affaires, U.S. Embassy
Ms. Ajarin Pattanapanchai, Permanent Secretary of the Ministry of Digital Economy and Society (MDES)

8:25-11:00AM: Presentation of Topics

Cybersecurity Regulatory Overview and Update:
Gp. Capt. Amorn Chomchoey, National Cyber Security Agency Working Group

- National Cyber Strategy
- Mission Function Structure for NCSA
- Cybersecurity Challenges for Thailand

Panel Discussion – A Practical Guide to Build a Cybersecurity National Strategy and Infrastructure
Moderator: Barbara Grewe, Portfolio Director of International Strategy and Policy, MITRE

Panelists:

Tracy A. Bills, CERT® Division, Software Engineering Institute (SEI)
Michelle Yezierski, Stakeholder Engagement Division, Section Chief – Dams, CISA
Amy Mahn, International Policy Specialist, Applied Cybersecurity Division, NIST

- *Where incident management fits into a strategy*
- *Types of structures that support that function (i.e. national CSIRT, coordinating centers, etc)*
- *Other strategy implementation considerations*

9:40-10:00AM: Coffee Break

Cybersecurity and Global Standards
National and International Cybersecurity Strategy – Importance
David Kaiser, Product Security Office Director, Seagate

- Industry view and practice of global standard adoption
- Benefits of ASEAN standard harmonization

Protecting Critical Infrastructure: 5G, Operational Technology, and Other Measures Against Emerging Threats
Joshua McCloud, National Cybersecurity Officer, Cisco

- Overview Critical Infrastructure Platforms
- Top Risks to Critical Infrastructure
- Critical Infrastructure Cybersecurity Strategy
- National SOC Use Case

Proactive Cyber Threat Hunting in National SOC based on Sectoral SOC and Info Sharing and Analysis Centre (ISAC)
Paul Pang, Senior Cybersecurity Specialist, Splunk

- Modernize SOC by intelligence-driven analysis
- Threat intelligence exchange model in Sectoral SOC and ISAC
- Case study in other countries

Day 2

7:30-8:00AM: On-site Registration / Log into virtual Zoom Workshop

8:00AM **Welcome and Opening Remarks**
Tibor Pandi, Vice President, AMCHAM Thailand
Aaron Cooper, Vice President of Global Policy, the Software Alliance (BSA)

8:20-11:00AM: Presentations of Topics

Panel: Overview and Application of Privacy Framework and Information Sharing
Moderator: Julie Snyder, Principal/Privacy Domain Capability Area Lead, MITRE
Panelists:
Dylan Gilbert, Privacy Policy Advisor, NIST

Tracy A. Bills, CERT® Division, Software Engineering Institute (SEI)
John Nelson, Senior Privacy Analyst, DHS Cybersecurity and Infrastructure Security Agency

- NIST’s privacy frameworks and application for small and medium enterprises (SMEs) (NIST/CISA)
- Policy frameworks and best practices
- Benefits and challenges of information sharing (SEI)
- Privacy considerations in action for cyber information sharing, AIS case study

Sovereign Cloud for Government
Putti Tangtrakulwongse, Customer Engineer Manager, Google Cloud Thailand

- Privacy & Data Sovereignty Requirements
- Case Studies

9:30-9:45AM: Coffee Break

Overview of Data and Privacy Protection in the ASEAN region
Dr. Praphanpong Khumon, Office of the Personal Data Protection Committee

- A glance at the data and privacy laws
- Cross-border Data Transfer
- Thailand's approach and other ASEAN countries (e.g., ASEAN Framework on Personal Data Protection)

Thailand's Personal Data Protection Act (PDPA) Regulatory Approach
Dr. Soontaree Songserm, Office of the Personal Data Protection Committee

- Key priorities and updates on subordinate regulations
- Enforcement Mechanism

Thailand's Personal Data Protection Act (PDPA) from an Operational Perspective
Mr. Veerachai Chuenchompoonut, Thai Bankers’ Association

- Key provisions and industry implications
- Guideline on Personal Data Protection for Thai Banks

Data flows and Cross-Border Transfer Mechanisms
Michael diPaula-Coyle, Head of International Trade Policy, IBM

- The growth and benefits of digital trade and cross-border data flows
- Digital Trade and "Thailand 4.0"
- The challenges posed by digital trade barriers
- Modernizing trade agreements and data flow mechanisms for the post-COVID global economy
- Building trust in the global data economy

Day 3

7:30-8:00AM: Log into virtual Zoom Workshop

8:00AM **Welcome and Opening Remarks**
Leslie McDermott, Senior Director of International Development, ANSI

8:05-10:00AM: Presentations of Topics

Sectoral Approach to Cybersecurity Risk Management
Sean Duca, Vice President, Regional Chief Security Officer – Asia Pacific & Japan, Palo Alto Networks
Robert Kolasky, Assistant Director, National Risk Management Center, DHS Cybersecurity and Infrastructure Security Agency

- Perspectives on a framework for cybersecurity across multiple and disparate industry sectors
- Threats across sectors
- Practical steps and best practices
- Case studies

How to Build National Cyber Capabilities
Nathan Cook, Vice President & CTO National Security & Defense EMEA & JAPAC, Oracle

Data Protection as part of Digital Ecosystems and Economic Recovery
Marcus Bartley Johns, Regional Director, Government Affairs, Microsoft ASIA

- The digital policy regulatory environment and growth and investment in the COVID-19 economic recovery
- Strengthening regulatory transparency and predictability related to data governance (e.g. privacy, cross-border data flows, cybersecurity)
- The regional dimension for Thailand, especially ASEAN and APEC

Shared responsibility model in cloud computing
Annabel Lee, Public Policy Lead for Data (APAC), Amazon Web Services (AWS)

- Security services and principles for data controllers
- New premise of data centers

Closing Remarks

Brandon Megorden, Regional Manager for Asia, U.S. Trade and Development Agency (USTDA)
Jennifer Mleczko, International Development, ANSI

DETAILED WORKSHOP SUMMARY

Background

As the first workshop held under the U.S.-Indo-Pacific STCP, the U.S-Thailand Data Protection and Cybersecurity Standards Workshop focused on providing a forum for U.S. industry to engage with key Thai government decision-makers while implementing regulations for Thailand's new cybersecurity and data protection laws are being developed and promulgated. The event also provided an opportunity for U.S. companies to highlight solutions that can help both the Thai government and private sector to meet their cybersecurity and data protection needs in compliance with these new laws, which represents a significant commercial opportunity for U.S. companies.

According to U.S. industry, Thailand is a top performer amongst developing Asian countries making strong efforts towards embracing the digital economy[1]. While a digital gap remains and only 67% of Thai people reported using the internet in 2019, the Thai government is counting on the digital economy to lift the country to higher income levels through several programs geared at enhancing digital skills and infrastructure. [2] Much of the growth in digital infrastructure is due to the explosion of e-commerce during COVID-19 lockdowns. However, organizations and companies face major challenges in this transition, requiring adjustments to rigid structures, in addition to major investments in resources. According to a survey conducted by Deloitte, the top three challenges for digital transformation are talent gaps, lack of digital culture, and organizational silos. This highlights major knowledge gaps and the need for capacity-building efforts to bring technical capacity and awareness to the Thai population. These gaps are most evident in companies affected by digital disruption, such as telecoms and financial services. Overall, the vast majority of industries are set to experience digital disruption or transformation to a certain extent.

According to the International Trade Administration, U.S. Department of Commerce, telecommunications is viewed as the best prospect sector in Thailand including the following leading sub-sectors: Internet of Things (IoT), Mobile Security Solutions, Cloud Computing, Telecommunication Infrastructure, and Network Management. Growth in the information, communications, and technology (ICT) sector will be stimulated by strong government support and its plans to create a digital economy. The value of Thailand's digital economy is expected to surge to US$37 billion in 2025, according to the "e-Economy Southeast Asia Spotlight 2017" report. [3] Concurrently, Thailand has been grappling with regulatory changes to address certain cybersecurity and data protection challenges associated with this growth. In May of 2020, Thailand published the Personal Data Protection Act (PDPA), however, enforcement has been delayed until May 31, 2021, to allow industries time to comply. Falling under the power of the Personal Data Protection Committee (PDPC) and similar to the European Union's GDPR, the law gives consumers the right to access, erase, object or rectify personal data upon request. As of

[1] https://www.export.gov/apex/article2?id=Thailand-telecommunications
[2] https://www.bangkokpost.com/business/1992755/a-better-digital-future
[3] https://www.nationthailand.com/noname/30339480

today, the PDPC has not yet appointed members; however, the subsidiary legislation regarding consent procedures, complaint reception, and expert panels has been drafted and is awaiting approval by the PDPC[4]. While frameworks for data protection and cybersecurity are crucial, increased regulations and unique and disparate laws create hurdles, burdens, and even barriers for organizations that need to comply with various countries' rules regarding data law compliance. This emphasizes the importance of regulations based on international best practices and standards to limit trade barriers and associated financial burdens, particularly for small and medium enterprises (SMEs).

Summary of Workshop Topics

The target audience included the Thai government and industry, as well as U.S. government, and industry representatives. Several topics were covered over the course of 3-day sessions that lasted 3 hours each. The agenda balanced perspectives from U.S. industry, U.S. government, and Thai government speakers and representatives.

Day 1 (In-person/virtual) – Cybersecurity

Key Themes:

- Government can protect the security of our nations without limiting innovation, decreasing access to technologies, reducing competition, or reducing trade barriers
- Sacrificing the free flow of data across borders is not necessary to protect and secure personal data. World-class cybersecurity can protect data wherever it resides in the cloud and common interoperable data protection principles that democracies share can guard privacy around the globe.
- In the process of establishing the Thai National Cyber Security Agency, the challenge is to recruit talent and strengthen the organization. Thailand faces an increase of major cybersecurity instances but is just starting to build the capability to handle them. It is important for Thai agencies to rely on international standards and benchmarks such as ISO 27001, NIST framework, COBIT, and others.
- Panelists discussed the importance of a phased approach to implementing a cybersecurity infrastructure. The National Institute of Standards and Technology (NIST's) engagement with stakeholders and the public on the cybersecurity framework (https://www.nist.gov/cyberframework) to ensure all perspectives are brought to the table is a viable example. The benefits to stakeholders include information sharing, effective practices, valuable input for a usable product. The value of these discussions is to obtain ongoing feedback. A cybersecurity framework is a living document and meant to be accessible for both technical experts and non-experts.
- In terms of developing a CSIRT, and national CSIRT versus a sector CSIRT, speakers emphasized the need to first decide on requirements, mission, and objectives, then develop and recruit talent. It is best to start small with immediate needs, then build up.
- Critical infrastructure cybersecurity is built on mature standards (NIST, ISO, 3PP) at a basic level and should adopt an overarching cybersecurity strategy, which includes reducing attack surfaces, mitigating threats, protecting data privacy.

[4] https://www.bangkokpost.com/business/2093467/new-minister-ponders-delay-of-personal-data-protection-act

- The National Security Center is not designed to do everything. It is also important for all enterprises and government agencies to have experts with similar skill sets to provide threat intelligence feedback and incident response and sharing

Day 2 (in-person/virtual) – Data Protection

Key Themes

- Information sharing is critical to cybersecurity, but the issue of trust is at the foundation of effective information sharing that protects data and personal identifying information
- The NIST Privacy Framework (https://www.nist.gov/privacy-framework) offers resources for organizations starting to set up a privacy program, including SMEs. It allows users to map local law/policy requirements against framework to help determine compliance.
- CISA Automated Indicator Sharing (https://www.cisa.gov/ais) is open to participants at no cost and offers the ability to join the network and receive information about cyberattacks, threat indicators from other participants.
- How a company treats data in providing cloud services to public and commercial sectors is fundamental. Companies should also consider the importance of data sovereignty, operational sovereignty, software sovereignty.
- Data and privacy protection in the ASEAN region – regional mechanisms like the ASEAN Cross Border Data Flows (CBDF), the MCCs as contractual clauses, and the ASEAN Framework on Digital Data Governance offer a flexible template for states to establish rules for cross border data flows.
- Thailand has recently established its Personal Data Protection Act (PDPA), with several key steps underway for early implementation:
    - 2021 will focus on establishing the Personal Data Protection Committee and Office; developing draft sub-regulations; developing a master plan; and developing draft guidelines for data controllers and processors, including 7 guidelines for sectoral agencies and are in the process of welcoming and obtaining feedback.
- How can the PDPA be viewed for implementation by an organization? – a discussion of the definitions provided in the Act, applicability and requirements, and samples of how one organization is establishing the required notifications and other elements.
- Data is more impactful than ever, showing explosive growth even pre-COVID. It is important to factor data flows and data protection into trade agreements and some good examples exist such as the USMCA. Data localization does not necessarily equal security.

Day 3 (virtual) – Sectoral Cybersecurity and Data Protection

Key Themes

- Strong frameworks are required to support national cybersecurity and data protection, including risk management, cross-sectoral collaboration, and identifying weaknesses. International standards can help ensure regulatory coherence, privacy, and cybersecurity without introducing regulatory barriers.
- Effective risk management depends on the critical infrastructure community's ability to engage across the sectors to facilitate a shared understanding of risk and integrate a wide

range of activities to manage risk. This includes understanding what functions are so vital, that if disrupted, could cause cross-sector impacts or cascading consequences across industry/society—National Critical Functions Set.

- Further emphasis on trust, sectoral approaches alongside cross-sector collaboration requires integrity, transparency, and developing trust for effective communication and facilitation of partnerships. Trust is crucial for a digitally powered economic recovery.
- Sophisticated actors will look to exploit fundamental weaknesses in human decision-making processes and trust across levels, fragmentation and silos exacerbate weaknesses. On the other hand, the convergence of technologies and different national ecosystems can also have severe impacts on cybersecurity if not done carefully. Cloud technology can help provide platforms for this but require shared responsibility models.
- COVID-19 has put Thailand's core sectors (i.e. tourism and exports) under pressure. Public and private sectors continue to remain resilient through the digital economy and technology. This offers an opportunity for forward-looking policies and capitalizes on Thailand's digital ambitions. Regulatory transparency and predictability will be essential.
- The regulatory framework for cross-border transfers of personal data is crucial to protecting privacy when data moves across borders, without introducing regulatory complexity.

Technical Analysis of Content Featured and Key Takeaways

Following the final presentations of the workshop, a smaller Executive Roundtable Discussion was held, bringing together 20 U.S. and 20 Thai representatives including, the co-organizers and speakers from the previous 3 days of the workshop. During the Executive Roundtable, participants focused on the key takeaways from the workshop and recommendations for future collaboration. A summary of these points is included below.

1. Participants agreed on several considerations that support a successful, science-based cybersecurity and data protection landscape:

Risk prioritization: frameworks such as the NIST Cybersecurity Framework can help prioritize risks, especially where the capacity to mitigate all risks doesn't exist.

Stakeholder Partnerships: trust and transparency are critical to building successful partnerships. International standards can add huge value to Thailand, allowing for flexibility to enable a full range of future business models. Working with industry is critical for this to be successful, and stakeholders have to be involved in conversations. Information sharing is critical between industry and government.

- ***International Standards.*** Regulators aligning with companies on international standards and trusted products can build assurance, integrity, and transparency. Agreeing on the same frameworks and guidelines can assure genuine, authentic products while fostering economic growth. Products certified to international standards are vital to generating trust and cooperation.
- ***Privacy Risk Frameworks***. Implementing a strong privacy risk framework is crucial, with the need to think about the types of data and what is being done with it—trust is a combination of security and privacy. Fair information practices are key, remembering there is a human end of the data.

- ***Collaboration*.** Open and collaborative interaction between all stakeholders helps to achieve outcomes successfully and to ensure that the correct processes are in place. Transparency in feasibility and capabilities are also important, and a project should not be rushed to completion based off an artificial deadline, but through real constructive input..

Workforce Capacity: There is a critical need to build technical expertise for cybersecurity professionals, this includes data scientists and analysts, as well as law professionals from a cyber and data perspective.

- *Aligning national and international measures.* Aligning national measures to internationally recognized standards is critical. Training local workforce by relying on international workforce can be facilitated by internationally interoperable approaches. There is a need to train, develop, build. Major opportunities exist to build new generations of technology alongside building the skill, knowledge, and expertise.
- *Public education*. Public awareness, citizen and consumer education will also be crucial to strengthen systems.

Cybersecurity and Data Protection Compliance: Cybersecurity issues lead to data protection and privacy issues, and vice versa. Understanding that compliance with both leads to overall better outcomes and increased security. This requires cybersecurity and data protection teams to work closely together, fostering collaboration while limiting silos.

- ***Compliance issues*.** Businesses need to ask themselves where they are with compliance, while regulators need to ask if businesses are aware of how to comply and if they have the appropriate tools to meet compliance. Most organizations tend to look at compliance from the perspective of documentation; innovation and flexibility will be important to find ways to help companies and organizations through the process. There are generally big gaps remaining. Additionally, it is important to raise awareness about the concept that compliance is a floor, not a ceiling.
- ***Privacy versus security.*** Technology tends to just presume protection, foregoing impacts to individuals on privacy, issues that go beyond security. Foresight that includes long-term effects to data breaches should be considered, should a cyberattack bring data beyond the walls of a company or organization. Data privacy needs to be considered as part of the design when thinking about security. Effective privacy protection varies according to context and data collection and use. PDPA can support this by taking a principles-based approach, rather than being very technically prescriptive (i.e. mandating specific forms).
- ***Helping SMEs.*** Regulators need to take into account the burden SMEs may face in compliance. At the same time, innovative approaches and considering of different technologies that can come online can be used to ease the burdens or outsource their needs while meeting international standards and complying with regulations.

2. Several potential action items were suggested during the Executive Roundtable. Potential action items:

- **MDES cooperation with U.S. partners:** MDES proposes more exchanging of information on how to help set up a national CERT with a team from MITRE, how to build up sectorial CERT, and encourage sectors to build up their own capabilities. Establishing baselines can help drive sector engagement, as many issues will be relevant across sectors with some small variations. Baselines help drive a coordinated approach. This work can be lead by DEPA, whose mission is mandated by law to promote digital workforce development for cybersecurity and data protection. They are already offering trainings for 500 SMEs, raising awareness of PDPA and compliance. Still, there is a tremendous need for workforce development.

- **Additional Engagement:** Additional workshops and engagements for sector participants could be held, including ones that are tailored to specific regulators/government agencies focused on 1-2 discreet topics (e.g. cross-border data flows, IoT, AI).
- **Clear consultative process:** There is a need to establish a more concrete consultative process for both the personal data protection law and the cybersecurity law and to effect changes in draft implementing measures, especially with respect to the personal data protection law, to ensure the law is effective and internationally interoperable.
- **Cross-Border Transfers:** Engage and support Thailand's participation in an ASEAN Cross Border Data Transfer mechanism.

Relevant Links

Links to a flyer, photos, the final agenda, and presentations from the workshop are available on the U.S.- Indo-Pacific STCP website:
https://standardsportal.org/USa_en/toolbox/US%E2%80%93Indo-Pacific-STCP.aspx

Included in the materials on that website is a list of compiled resources and links, specific requests that came out of this workshop. This list is included at the end of this report in Annex A.

PARTICIPANT AND STAKEHOLDER FEEDBACK

Sixty-five participants or approximately 11% of workshop participants filled out a questionnaire, which was distributed via email to participants following the workshop, with three reminders sent. Highlights from the questionnaires include:

- **84% of all respondents** indicated that the workshop met their objectives in attending.
- **75% or more of U.S. respondents** believe that the workshop will improve or greatly improve international best practices, national cybersecurity strategies, and advanced technology in Thailand.
- **Over 90% of U.S. respondents** believe the workshop will at least somewhat improve all five topics, including personal data protection and information and digital policy and data governance.
- **88% of Thai respondents** are either moderately involved or very involved in standards development; this positively confirms the target audience of workshop attendees.
- Overall, a majority of the feedback highlighted positive results from the objectives of increased learning, knowledge, and understanding of PDPA implementation cybersecurity and data protection standards largely met. Key takeaways included: exchange of perspectives from practitioners, understanding differences between Thai and U.S. standards, understanding the PDPA, and learning about new technologies such as cloud computing, as well as overall global trends. Furthermore, the workshop also highlighted areas that remain unclear in terms of the PDPA implementation of data protection and cybersecurity standards.

- Generally, respondents highlighted that they believe the workshop will have a positive impact on Thai data protection and cybersecurity policies, through sharing knowledge and experiences, increasing the understanding of policymakers on how to align standards across markets.

Additional highlights from the responses, including industry recommendations and feedback, are included below:

- **Ensure stakeholder-centered consultation for the implementation of the Personal Data Protection Act:** Industry respondents welcome that Thailand releases the Personal Data Protection Act (PDPA) and appreciate that the Ministry of Digital Economy and Society (MDES) continues to give the opportunities to all stakeholders to discuss and address their concerns, including the public consultation recently organized from February 15-18, 2021. Respondents recommend the timely implementation of the PDPA that will provide a solid legal framework for personal data protection, and also understand it is challenging for MDES to ensure that the rules to implement the PDPA are linguistically and technically complete and do not have any legal flaws. For this reason, respondents urge MDES to continue to conduct and enhance an open and transparent step-by-step process when developing the implementing rules of the PDPA, including soliciting the input of interested stakeholders including the American business community, and taking into consideration the view of cloud service providers (CSPs). This can help MDES spot potential obstacles and pitfalls to avoid expensive errors in the implementation at a later stage. However, public consultation will be appreciated by interested stakeholders so long as it involves genuine engagement with sufficient time and detailed input to make a productive contribution. Additionally, since small-and-medium-sized businesses (SMBs), which play a key role in promoting Thailand’s digital economy, appear to be seriously affected by the economic slowdown due to the COVID-19 pandemic, MDES may consider an extension of the transition period, especially for SMBs to ensure their seamless business transition.
- **Adopt flexible mechanisms to promote cross-border data transfers while preserving data privacy and security:** Promoting cross-border data transfers, while preserving adequate and appropriate protections for data privacy and security, will enable Thailand to become ASEAN’s digital hub. Measures that mandate data across borders will not only impede the development of new and innovative services to every sector of the economy but will also put local businesses at a competitive disadvantage in international markets. Respondents recommend that the Ministry of Digital Economy and Society (MDES) support flexible mechanisms for cross-border data transfers, including international data transfer frameworks e.g. APEC Cross-Border Privacy Rules, etc.
- **Foster trust through legal clarity on government access to data:** Trust is essential to the increase of the adoption and consumption of cloud services. It is well accepted that legal clarity in processes and procedures of government access to data stored in the cloud will also foster the trust of cloud service users. Such legal clarity should be aligned with the ownership principle that cloud service users are the owner of data and have full control

over their data. There should be no other organizations that can access their data without their knowledge or approval.

- **Promote coherence and alignment with international standards:** As Thailand continues its journey of digital transformation, it is vital to ensure that digital policies are developed and implemented in ways that are consistent with international standards. This pertains to areas such as data protection, cybersecurity, artificial intelligence, cloud computing, among others. This will allow businesses operating in Thailand to experience a policy regime that is consistent with international best practices and not be challenged to overcome particular issues unique to Thailand. The commonality in aligning with international standards will support Thailand's role in becoming a regional hub and serve as a bridge to link Thailand to the global digital economy.
- Respondents welcome further discussions with the Thai government (particularly the Ministry of Trade & Industry) on digital trade. This could include a "deep dive" on key provisions that are increasingly standard in trade agreements and a discussion around the benefits of Thailand joining the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).
- Respondents noted that the U.S.-Thailand Data Protection and Cybersecurity Standards Workshop has already established a strong partnership between Thailand and the U.S.. Given that cyber-security standards are global issues that need strong cooperation on an international level, all those sharing of knowledge and experiences in the workshop and the proposed action plan for cooperation between Thailand and the U.S. are truly beneficial to both countries. In terms of Data Protection, it is good to have the opportunity to share the local new scheme of personal data protection law (i.e. the PDPA), which adopts the General Data Protection Regulation of the EU.
- Many countries in ASEAN are developing new regulations or adopting new frameworks for the digital economy. Some respondents recommended that countries should be encouraged to adopt international standards where possible, and trainings/communications should be made available to raise awareness about the global standards that exist, and to prevent countries from creating their own new standards and regulations.

ANNEX A

REFERENCES
(Provided to all participants following the workshop)

U.S. Cybersecurity and Infrastructure Security Agency

Critical Infrastructure Sectors

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain

secure, functioning and resilient critical infrastructure. This site offers guidance on the essential critical infrastructure workforce, as well as resources for each of the 16 sectors.
https://www.cisa.gov/critical-infrastructure-sectors

CISA Ransomware Guidance and Resources

The CISA Ransomware Guide, released in September 2020, represents a joint effort between CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The joint Ransomware Guide includes industry best practices and a response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans. In January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to raise awareness and instigate actions to combat this ongoing and evolving threat. The campaign is a focused, coordinated and sustained effort to encourage public and private sector organizations to implement best practices, tools, and resources that can help them mitigate ransomware risk.
www.cisa.gov/ransomware

CISA Industrial Control Systems Security Offerings

Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions. To support the ICS community's cyber risk management efforts, CISA offers ICS owners and operators a wide range of products, services, and capabilities. Click on the CISA Industrial Control Systems Security Offerings and Capabilities fact sheet below to learn more.
www.cisa.gov/publication/ics-security-offerings

Cybersecurity Best Practices For Industrial Control Systems

Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions. As ICS owners and operators adopt new technologies to improve operational efficiencies, they should be aware of the additional cybersecurity risk of connecting operational technology (OT) to enterprise information technology (IT) systems and Internet of Things (IoT) devices.
https://www.cisa.gov/publication/cybersecurity-best-practices-for-industrial-control-systems

National Critical Functions

The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
https://www.cisa.gov/national-critical-functions-set

Software Engineering Institute

Steps for Creating National CSIRTs

The purpose of this document is to provide a high-level description of a Computer Security Incident Response Team (CSIRT), the problems and challenges facing these CSIRTs, and the benefits of developing such a team or response capability at a national level.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53062

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability

In this report, the authors provide insight that interested organizations and governments can use to develop a national incident management capability.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9221

Other National CSIRT Resources

This collection contains information that governments can use to develop a National Computer Security Incident Response Team (NatCSIRT).
https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=505132

Other CSIRT Resources

These resources help you create and maintain a CSIRT, staff and train CSIRTs and describe common issues CSIRTs face. Also included is information governments can use to develop and manage National CSIRTs.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=505118

Cybersecurity Center Development

Critical to these incident response efforts are cybersecurity centers, which are teams of experts who mitigate threats by identifying, protecting, detecting, responding to, and recovering from incidents. These centers may take the form of computer security incident response teams (CSIRTs), security operations centers (SOCs), product security incident response teams (PSIRTs), CSIRTs of national responsibility, or other similar incident management teams. This international capacity building, information sharing, and global cyber workforce development are key efforts in the pursuance of U.S. objectives in cyberspace. The SEI prepares these cybersecurity center teams to effectively assess and manage cybersecurity incidents.
https://sei.cmu.edu/our-work/cybersecurity-center-development/

Forum of Incident Response and Security Teams [various resources]

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, stimulate rapid reaction to incidents, and promote information sharing among members and the community at large. Apart from the trusted network that FIRST forms in the global incident response community, FIRST also provides value-added services.
https://www.first.org

FIRST CSIRT Services Framework

The Computer Security Incident Response Team (CSIRT) Services Framework is a high-level document describing in a structured way a collection of cybersecurity services and associated functions that Computer Security Incident Response Teams and other teams providing incident management-related services may provide. The framework is developed by recognized experts from the FIRST community with strong support from the Task Force CSIRT (TF-CSIRT) Community, and the International Telecommunications Union (ITU).
https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

National Institute of Standards and Technology (NIST)

Cybersecurity Framework:

Helping organizations to better understand and improve their management of cybersecurity risk

- Main Site: https://www.nist.gov/cyberframework

- International Resources (including translations and adaptations): https://www.nist.gov/cyberframework/international-resources

Privacy Framework:

The NIST Privacy Framework is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy
https://www.nist.gov/privacy-framework

IoT Cybersecurity Program:

NIST's Cybersecurity for the Internet of Things (IoT) program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale. The main site (includes links to published documents, documents out for comment, and upcoming workshops)
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

National Initiative for Cybersecurity Education (NICE):

The mission of NICE is to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

- Main site: https://www.nist.gov/itl/applied-cybersecurity/nice
- NICE Framework: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

National Cybersecurity Center of Excellence (NCCoE):

Each project results in a freely available NIST Cybersecurity Practice Guide (Special Publication series 1800), which includes information and instructions organizations can use to implement an example solution for themselves. Organizations that want to adopt similar solutions can use products from our collaborating vendors, or products with similar characteristics that fit their budgets and IT infrastructure.
https://www.nccoe.nist.gov

Small Business Cybersecurity Corner:

Your resources for keeping your small business secure. Get cybersecurity basics, guidance, solutions, and training to protect your information and manage your cybersecurity risks.
https://www.nist.gov/itl/smallbusinesscyber

Thailand Cybersecurity Act, English

https://thainetizen.org/wp-content/uploads/2019/11/thailand-cybersecrutiy-act-2019-en.pdf

Governments support of SME Capacity Building

Examples:

- Nymity Privacy Management Framework
  https://iapp.org/resources/nymity-workbook-tool/

- Singapore PDPC Guide to Developing a Data Protection Management Programme https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPMP/Guide-to-Developing-a-Data-Protection-Management-Programme-(18-Nov-2020).pdf?la=en

- **Promoting regulatory coherence and alignment with international standards**Strengthening Privacy Regulatory Coherence in Asia: https://aka.ms/asiaprivacycoherence
- Call for Closer Policy Collaboration on Artificial Intelligence: https://www.Aiinapec.info
- https://techpost.bsa.org/2021/03/03/gda-cross-border-data-policy-principles-the-international-economic-rule-of-law-and-data-transfer-policy/
- https://www.globaldataalliance.org/ - see infographics and other material on the site.