September 27, 2019

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 Indonesian economy. Through its *Initiative Indonesia* program, the Chamber engages closely with the U.S. and Indonesian governments to address the most pressing policy issues and concerns that hinder the growth of trade and investment between our countries.

The Chamber commends the Government of Indonesia ("the Government") for launching a public consultation on the Draft Law Concerning Cyber Security and Resilience ("the Draft Law"). Incorporating a wide range of stakeholder perspectives serves to enrich the quality of legislation.

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 35 governments to develop and implement approaches to cybersecurity 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 message has resonated: governments and businesses face shared, cross-border cyber threats. Unnecessary divergence in the regulatory frameworks and responses of governments makes our defenses weaker, and our adversaries stronger. As such, we

support international efforts aimed at aligning regulatory approaches to better reflect globally-accepted best practices.

There are certain areas where we believe the text of the Draft Law could be improved, to better facilitate our shared goal of improving cybersecurity outcomes in Indonesia. Accordingly, we offer the following recommendations.

Throughout the draft law, the Government should better leverage international standards to avoid creating barriers to trade and the deployment of effective cyber solutions across borders. 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 ISO/IEC 27001. Certification schemes where required should similarly recognize test reports from internationally accredited testing labs and not be limited to only Indonesia testing facilities. Instead of the Government creating a new set of standards and requirements, we suggest looking to these proven guidelines that will increase overall cybersecurity in Indonesia.

The Draft Law's proposed penalties are unnecessarily harsh and ultimately counter-productive. Critical infrastructure operators already experience significant repercussions from cyber incidents. The proposed penalties only serve to exacerbate the impact to the victims of attacks, undermining recovery and further incentivizing malicious cyber actors.

The Chamber advocates strongly against local provider and local content requirements. As drafted, the law states that cyber insurance can only be supplied by Indonesian companies, which could be interpreted to mean that foreign-invested insurers cannot supply cyber insurance. If that is the intention, such a requirement would disincentivize companies from taking out cyber insurance policies, undermining an effective risk mitigation tool. Requiring local content on security devices and products only limits the range of choices of technology and solutions that are available to protect Indonesia and does not help Indonesia build its cybersecurity industry if there is not access to the best available technology globally.

We have out outlined our recommendations in more detail below. We thank you in advance for your consideration of our comments.

The Chamber firmly believes that a well-crafted cybersecurity strategy is the basis upon which sustainable digital growth can be built. We look forward to working with you to implement such a strategy, which will facilitate further growth in Indonesia-U.S. trade ties.

Should you have any questions or comments regarding the submission, please contact either Sean Heather (sheather@uschamber.com) or John Goyer (jgoyer@uschamber.com) at your convenience.

Sincerely,

Sean Heather
Senior Vice President
International Regulatory Affairs
U.S. Chamber of Commerce

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

Lin Neumann
Managing Director
AmCham Indonesia

Detailed Comments on Indonesia's Draft Law Concerning Cyber Security and Resilience

Issue of Concern	Articles	Proposed Solution
The definitions throughout Articles 1 and 11 and too vague and could lead to misinterpretation of the law. Specifically: 1(1): The definition of "cyber" is vague. The vagueness makes the scope of the draft law unclear. 1(2): The definitions of "cyber security" and "resilience" are too broad for a national cybersecurity law. 1(3): The definition of "Indonesia's cyber interests" is too broad. "Ideology" and "socio-culture" are not areas that should be addressed by a cybersecurity law, as they do not pertain to the resilience of digital systems. 1(5) and (6): The draft law does not sufficiently differentiate between a Cyber Incident and Cyber Attack. 1(12): The use of "existing" in the definition of countermeasure is not necessary.	1 & 11	We recommend aligning the definitions sections with internationally utilized definitions, such as those laid out in the U.S. National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. Critical Infrastructure: "Systems and assets, whether physical or virtual, so vital to the [country] that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters." Cybersecurity: "The process of protecting information by preventing, detecting, and responding to attacks." Cybersecurity Event: "A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)." Cybersecurity Incident: "A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery."
The word "public" is not well defined in Article 4 nor Article 8. Obligations in Articles 4, 6 and 8 refer to implementation of Cyber Security and Resilience by "the public" as well as various	4, 6 & 8	We recommend that the definitions be adjusted to distinguish between the obligations of: • Governments (including State Agencies, Central Government and Regional Governments)

government entities. The current definition fails to adequately define the "the public" and their obligations under the draft law.		• Private sector (Critical Infrastructure and non-Critical Infrastructure) • Public (individuals)
The national cyber infrastructure that government aims to protect is broadly defined in Article 10, with the responsibility to determine an authoritative list delegated to Badan Siber dan Sandi Negara ("BSSN"). If the cybersecurity law is to be effective, it is important that BSSN narrowly define this list, to ensure that government and private sector resources are allocated appropriately.	10	We recommend that national cyber infrastructures be clearly defined to include infrastructure that is most crucial to the government, such as government websites and e-government applications, and critical privately owned digital systems and infrastructure. Furthermore, the owners of critical infrastructure systems should have the ability to appeal their designation to BSSN. If the list of critical systems is too broadly defined, it may result in finite government and private sector resources being allocated away from protecting the most critical systems.
Article 11(2)(d) – the inclusion of "content" runs counter to the other definitions in 11(2), which are network directed malicious activities.	11	"Content" should be removed and be separately dealt with in separate legislation.
The criteria for mitigating a Cyber Threat risk in 12(2) are overly prescriptive, preventing the use of risk assessments to allocate resources and determine appropriate mitigation activities, in line with international best practices. It is effectively impossible to determine future cyber threats and the appropriate mitigation activities today. Attempts to do so not only constrain companies' ability to respond to evolving cyber risks, they may inadvertently create a	12	The law should state general best practices, which are not overly prescriptive, that are consistent with international best practices to ensure consistency. Article 12 (2) should be replaced with a call for providers to conduct cyber risk management activities in line with international standards and best practices, such as the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. In doing so, they can better ensure that cyber risks are identified, protected against, detected, responded to, and recovered from.

roadmap for malicious cyber actors. It is for this reason that cyber risk management is the preferred approach of governments such as the U.S., EU, Japan, Singapore, and many others.		
Articles 13(1), 16 and 44 state that designated actors will be required to conduct mitigation efforts "according to the specific standards set by BSSN". In developing new standards at the national level, Indonesia will waste valuable resources, as high quality international standards already exist. Moreover, where national standards diverge from international standards, they will create *de facto* trade barriers and undermine cybersecurity by preventing multinational entities from scaling best practices across borders.	13, 16 & 44	We recommend that BSSN be directed to leverage international standards and best practices for Cyber Threat risk management, which have proven to be effective, rather than developing new standards at a national level. Such risk-based, future-proof international standards and best practices include the ISO/IEC 27000 series standards and the U.S. National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.
Article 13 (2) states that "BSSN shall govern and assess the conformity of the Cyber Threat risk mitigation as referred to in paragraph (1)." BSSN focusing on conformance with their risk mitigation 'best practices' is burdensome and will direct finite cyber resources towards compliance, rather than risk mitigation activities.	13	We recommend that this provision be removed from the law.
Article 14 requires that all cyber incidents be reported to BSSN. Reporting all cyber incidents that could *potentially* affect consumers is overly broad. This would result in a slew of low priority information for BSSN to	14	We recommend that Articles 14(2) d., e., f., and g. are removed from the law. We recommend making incident reporting voluntary, such that experts operating within critical infrastructure entities can

assess, directing finite resources away time from higher priority incidents. Additionally, it would lead to consumers being overloaded with notifications that would create fatigue and not illicit reactions when actions by consumers is needed to protect data.		determine what information is of greatest relevance to report. This information can be shared both with government entities and within private sector information sharing bodies. In order to guide critical infrastructure entities, BSSN may wish to leverage existing international approaches to segmenting incidents by their severity, such as those in the United Kingdom, as indicated in Article 15. Tiers should remain *indicative,* rather than legally binding, however, as the same threat may have different implications on different systems.
Article 16 creates barriers to the deployment of international practices across borders by multinational entities. In doing so, it not only establishes a *de facto* trade barrier, it inhibits the ability of such entities to ensure the adequate protection of digital systems.	16	In Article 16(1), we recommend that BSSN leverage existing international standards and not create local standards that deviate from international best practices. Consistency of practices is essential to ensure good cyber protection. In Article 16(2), we recommend BSSN should recognize existing international accreditation schemes that validate standards and not require local and duplicated testing and certification.
Cyber device is not clearly defined and can be interpreted too broadly, layering unnecessary costs and regulatory burdens onto those devices that are not associated with sufficient risk to require certification. The standards against which certifications are measured should emanate from international standards setting bodies (according to TBT principles) and third party organizations should be utilized for conformity testing.	17	The law should clearly define what constitutes a cyber device and leverage existing approaches for determining the risk of a such devices. Only those devices which carry a high risk should be considered for certification. BSSN should utilize existing international standards, as well as those in development, rather than recreate them at the national level. International consistency is essential to the deployment of best practices. The law should not require that BSSN is the only body that can issue certification. Such an approach is cumbersome and will

The certification of devices should be used sparingly, and should be recommended based upon factors such as the risk of a device, its use case, and whether it is managed or unmanaged.		prevent operators from using the most current and innovative solutions to deal with fast evolving threats. BSSN should recognize existing international accreditation schemes that validate standards and not require local and duplicated testing and certification.
A licensing regime for individuals that conduct cyber system management, penetration testing, or cryptographic algorithm development is cumbersome to implement and delays access to effective solutions against fast evolving threats.. It raises the cost of conducting such activities in a legitimate fashion, prohibits many international experts from supporting Indonesian businesses and does nothing to disincentivize those international actors who conduct such activities maliciously.	18	We recommend removing this Article in its entirety.
Article 19 requires that those who are employed in cybersecurity roles have "competency" as determined by BSSN standards. Critical infrastructure owners and operators have significant incentives to hire qualified personnel, making such provisions unnecessary. Conversely, such provisions may inhibit their ability to leverage international personnel that have sufficient competency but not an accreditation from BSSN.	19, 20 & 21	We recommend removing these Articles in their entirety.
Article 22 outlines a number of administrative sanctions that may be imposed upon providers that do not meet the appropriate cybersecurity standards.	22	We recommend that Indonesia provide further clarification regarding the "clearance" referenced in c. and d.

These are in some cases unclear, in others counter-productive, and all are unnecessary. c. and d. reference the suspension or permanent revocation of "clearance". It is unclear what clearance this refers to. g. and h. reference the suspension or permanent termination of electronic system operations. If the purpose of this law is to ensure the uninterrupted operation of critical digital systems, a government 'takedown' of such systems would clearly be counter-productive. Were BSSN to avail itself of this option, moreover, it would represent a significant violation against the property rights of the owners of such infrastructure. This would be a severe disincentive for investment in Indonesia. Critical infrastructure operators already experience significant repercussions from cyber incidents in the form of direct costs from damage caused and remedies, loss of customer and partner confidence, and negative impacts on their valuation. Government penalties only serve to exacerbate the impact to the victims of attacks, undermining recovery and further incentivizing malicious cyber actors.		We strongly recommend that g. and h. be removed from the law, given the concerning implications if these were ever to be utilized by the government. We urge the government to utilize any remaining administrative sanctions with significant restraint, to ensure that they do not inhibit cyber incident response and recovery, or further incentivize malicious cyber activity.
Articles 23-26 reference the suspension or permanent termination of electronic system operations. If the purpose of this law is to ensure the uninterrupted operation of critical digital systems, a government 'takedown' of such systems would clearly be counter-productive. Were BSSN to avail	23, 24, 25 & 26	We strongly recommend that c. and d. in articles 23-26 be removed from the law, given the concerning implications if these were ever to be utilized by the government. We urge the government to utilize any remaining administrative sanctions with significant restraint, to ensure that they do not

itself of this option, moreover, it would represent a significant violation against the property rights of the owners of such infrastructure. This would be a severe disincentive for investment in Indonesia. Critical infrastructure operators already experience significant repercussions from cyber incidents in the form of direct costs from damage caused and remedies, loss of customer and partner confidence, and negative impacts on their valuation. Government penalties only serve to exacerbate the impact, undermining recovery and further incentivizing malicious cyber actors.		inhibit cyber incident response and recovery, or further incentivize malicious cyber activity.
This is a notably positive provision of the law. Yet the process to be taken by a person negatively impacted by a cyber crime is unclear. It is also unclear who is responsible for the cost of such rehabilitation, compensation and restitution.	28	Article 28 should define the process someone would take who has been a victim of cyber crime and who would be responsible for any appropriate restitutions.
Article 29 (2) requires that Cyber insurance services be provided by an Indonesian insurance provider. As drafted, this provision could be interpreted to mean that foreign-invested insurers cannot supply cyber insurance. If that is the intention, such a requirement would concentrate undue risk in the Indonesian financial sector and disincentivize companies from taking out cyber insurance policies, undermining an effective risk mitigation tool. In addition, a nationality-based requirement appears to be inconsistent with Indonesia's obligations under the General Agreement on Trade in Services, which could expose Indonesia to litigation under the World Trade Organization.	29	We recommend that Article 29 (2) be removed in its entirety.

Local provider requirements will reduce the economic competitiveness of Indonesia, without meaningfully contributing to improving cybersecurity outcomes.		
Similar to Article 19, Article 30 (2) has a certification requirement for cybersecurity employees to have a certification from BSSN. Again, it is a concern that the law assigns BSSN to set a standard for who might be employed in a cybersecurity role.	30	We suggest that Article 30 (3) and (4) be removed.
Article 31 (2) requires that Cyber Security and Resilience operations centers of larger companies need to be connected to the national Cyber Security and Resilience operations center. It is unclear what benefits would be derived from such an approach. It would, however, increase cyber risk by establishing unnecessary connectivity with the national center, which could be exploited by malicious actors. Moreover, without the appropriate filtering of information by those collecting it, the national center will be overwhelmed by the volume of information, inhibiting its ability to identify and respond to the most serious threats. Threat information sharing is best conducted in an environment of trust, which is best facilitated by a [mandatory] *[do we mean voluntary here?]* approach to information sharing.	31	We recommend that Article 31 (2) be removed. We encourage the Government of Indonesia to explore how they can leverage existing voluntary, cross-border information sharing mechanisms, such as the system of sectoral ISACs and existing CERT-to-CERT information sharing bodies.

The requirements for developing a cyber culture in Article 35 are unnecessarily prescriptive and are not proven to bring about the intended outcomes.	35	We suggest that Article 35 be removed.
As the law currently mandates, BSSN has the power to conduct contents and electronic apps filtering. These actions may overlap with the Ministry of Communication and Informatics (MoCI)'s authority to filter and takedown contents. If the law is passed in its current form, this will an unnecessary hurdle and complication for industry, given that BSSN may have very different views on responsibility of social media platforms as compared to MoCI.	38	We recommend delete "negative content" from the scope of things that BSSN may have jurisdiction over in Articles 11 and 38. This should be left under the purview of MoCI so there is clear overview regulator.
Both Articles 39 and 40 give the power to BSSN to prosecute a person proven to have committed a cyber crime. This will create a disincentive for information sharing to protect citizens and for following best practices in combating cybercrime. Additionally, this will also create a disincentive to follow the provisions required in Article 31.	39 & 40	We suggest that Articles 39 and 40 be removed. Related to the comment at Article 45 below, cybercrime provisions should be established in a separate legislation that empowers law enforcement with investigation and prosecution powers to pursue criminals, and not here in the cybersecurity law which deals with protecting the infrastructure essential to Indonesia.
While we express no opinion on whether BSSN or another part of the government should be the lead, provisions a., b., d. and e. are concerning for the reasons outlined in comments above. In Article 44 g. the power is given to BSSN to perform assessment, testing and penetration of electronic systems. This power is too general and if carried out, must be paired with legal guidelines for BSSN's actions. Article 44 encompasses many of the problems identified with the law as a whole.	44	We suggest strict guidelines be placed around BSSN's ability to conduct the activities outlined in 44 g. We suggested that a., b., d. and e. be amended or removed according to the suggested changes outlined above.

Article 45 expands upon Articles 39 and 40 to give BSSN further jurisdiction over the law enforcement process. Criminal law enforcement should be the responsibility of police and the court process, not BSSN. This is not only to preserve the integrity of the rule of law, but to ensure that BSSN is viewed as a trusted partner by industry and the public. If they are viewed as a prosecutorial organization, this would likely create a chilling effect on cooperation and information sharing.	45	We recommend that the functions outlined in Article 45 not be allocated to the same authority that leads cyber risk assessment, mitigation and remediation activities.
Article 47 f. and 48 f. grants the authority to BSSN to authorize activities of research and testing in the cyber space. Research and development should be encouraged, not hindered, by BSSN and should not require pre-authorization. This would hinder innovation.	47 & 48	We suggest Article 47 f. and 48 f. be removed from the law.
The overarching control and governance of cryptographic algorithms described in Article 29 is concerning. We suggest looking to international best practices on cryptographic algorithms before mandating BSSN's governance of them.	49	We suggest that Article 49 a. be removed from the law.
The local content requirements in Article 66 are contradictory to the objective of improving competitiveness and innovation (Article 3 b). It is impractical to require such a high percentage at	66	We suggest Article 66 be removed.

50% and will likely rule out access to the most current and innovative solutions available globally, putting Indonesia at even greater risk because it is not able to leverage the must current defences.		