May 16, 2019

Mr. Djoko Setiadi
Head of National Cyber and Encryption Agency
National Cyber and Encryption Agency
Jl. Harsono RM 70 Ragunan, Pasar Minggu
Jakarta Selatan, Indonesia 12550

Dear Pak Djoko,

US-ASEAN BUSINESS COUNCIL AND BSA | THE SOFTWARE ALLIANCE COMMENTS ON DRAFT BSSN REGULATION ON INFORMATION SECURITY MANAGEMENT SYSTEMS

The US-ASEAN Business Council (**US-ABC**)[1] and BSA | The Software Alliance (**BSA**)[2] greatly appreciate the opportunity to provide comments to the National Cyber and Encryption Agency (Ba*dan Siber dan Sandi Negara*; **BSSN**) on the draft regulation on Information Security Management Systems (*Sistem Manajemen Pengamanan Informasi;* **SMPI**) recently issued by BSSN for public comment (**SMPI Regulation**).[3]

Our members are at the forefront of data-driven innovation, developing and offering essential software, security tools, communications devices, servers, and computers that drive the global information economy and improve our daily lives. Our members earn users' confidence by providing essential security technologies to protect them from cyber threats. These threats may be posed by a broad range of malicious actors, including those who would steal our identities, harm our loved ones, steal commercially valuable secrets, or pose immediate danger to our nation's security.

US-ABC and BSA have worked closely with governments around ASEAN and the world in relation to the development of national security policies and legislation. In doing so, we have witnessed first-hand the potential for such policy and legislation to effectively deter and manage security threats whilst still protecting the privacy and civil liberties of citizens.

[1] For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations ("ASEAN"). Worldwide, the council's 150-plus membership generates over $6 trillion in revenue and employs more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The council has offices in Washington, DC; New York, New York; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

[2] BSA (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[3] As made available at this webpage: https://bssn.go.id/permohonan-tanggapan-publik-mengenai-peraturan-badan-siber-dan-sandi-negara-tentang-sistem-manajemen-pengamanan-informasi-smpi/

We thus have a significant interest in the BSSN's plans to introduce an SMPI Regulation. After a thorough review of the draft regulation, we would like to propose BSSN not to issue this draft regulation due to potential inconsistencies with existing Indonesian laws and regulations. However, in the event that BSSN believes the regulation should be pursued, we would like to offer the following comments and recommendations for your consideration.

GENERAL COMMENTS

1. Ensure the Alignment of Draft SMPI Regulation with the Draft GR 82 Amendment and Draft Personal Data Protection Bill

We recommend that the draft SMPI Regulation should be put on hold until the issuance of the finalized amendments to Indonesia Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (**GR82**) and the finalized Personal Data Protection Bill (**PDP Bill**), as well as with other existing regulations, for clarity and consistency.

For instance, the definition of "Personal Data" is different in the draft SMPI Regulation and the current draft PDP Bill. These definitions should be aligned. Moreover, having two separate regulators (the Ministry of Communications and Informatics (**KOMINFO**) and BSSN) requiring electronic system providers to obtain similar certifications under separate pieces of legislation creates confusion and duplication, which places significant burden on the industry, including micro-, small-, and medium-sized enterprises (**MSMEs**). The confusion can arise from (i) the government agency responsible for managing compliance with those obligations and (ii) uncertainty of the implementation of other regulations. The draft regulation should shed light on how it is intended to be implement in conjunction with KOMINFO Regulation No. 4 of 2016 and clearly delineate responsibilities between BSSN and KOMINFO. We also note, in particular, that the draft amendment to GR82 is intended to implement the "Strategic", "High", and "Low" categorization scheme for electronic systems.[4] Putting the SMPI Regulation on hold until the GR82 categorization scheme is settled would therefore avoid conflicting definitions and approaches for "Strategic", "High", and "Low" electronic systems.

2. The Definition of "Public Service" and the Entities and Electronic Systems Covered should be made Consistent with Other Existing Regulations

We recommend that the draft SMPI Regulation should align the definition of "public service" under the draft SMPI Regulation with other existing legislation, including Law No. 25 of 2009 regarding Public Services (**Law 25**) and GR82, which we understand the draft SMPI Regulation is intended to implement.

Existing legislation limits the definition of "public service" to activities which are performed by entities **established by law solely** for the purpose of providing public service activities:

- Law 25 defines "Public Service Provider" as "every state administrator institution, corporation, and independent institution **established on the basis of law** to undertake activities of public service and other legal entities **solely** established to undertake activities of public service"
- Article 2 of KOMINFO Regulation No. 7 of 2013 regarding the Guidelines for the Implementation of Inter-Operability of Office Documents for Electronic System Provider for Public Services also states that *"[e]lectronic system providers for public service is any state administrative institution,*

[4] US-ABC and BSA had also provided comments to KOMINFO, in March 2018, on the draft amendment to GR82, including on the categorization scheme. Our comments are available at https://www.bsa.org/sites/default/files/2019-03/03012018BSAJointSubmissionOnGR82Amendment.pdf

*corporation, independent institution **established pursuant to the Law** for public service activities, and other legal entities established **solely for the purpose** of public services providing, managing, and/or operating an electronic system separately or jointly to the electronic system used for its own purpose and/or for the purposes of other parties.*"

We similarly recommend that the draft SMPI Regulation should revise its definition of "Public Service" to align the scope of entities covered to existing legislation. In this regard, the mandatory obligations under GR82 are confined to electronic systems operators for public service. Subject to our comments below on removing all requirements for mandatory certification, the SMPI Regulation should adopt a similar approach in that only electronic systems operators for public service should be subject to any mandatory obligation under the SMPI Regulation.

In addition, the concept of "Electronic System Operator" does not make any distinction between the "owner" of the electronic system, who is the Public Service provider and has management and control over the electronic system, and third-party service providers in relation to aspects of the electronic system who may not necessarily have management and control over the whole electronic system. To ensure accountability over the electronic system, there should only be one "owner" which is the Public Service provider, with applicable requirements passed on as appropriate to third-party service providers of the Public Service provider through contractual business-to-business relationships between the Public Service provider and the third-party service providers.

The application of the draft SMPI Regulation should also be limited to electronic system located in Indonesia only. Electronic systems located outside Indonesia should not be covered by the draft regulations as: (a) it would be challenging to administer the requirements for offshore electronic systems; and (b) there will be conflicts with the legal and regulatory regimes in other countries.

3. Promote Voluntary Market-Driven Certification and Reliance on Internationally-Recognized Standards and Certifications

The draft SMPI Regulation imposes various mandatory requirements on electronic system operators including the following:

- A requirement for operators to perform a yearly assessment and self-categorization of their electronic systems into "Strategic", "High", and "Low" and to submit a yearly report accordingly to the BSSN, who will then verify the self-categorization and award a certificate to operators whose systems meet the requirements of Indonesia's Information Security Index (i.e., the KAMI Index).[5]
- A requirement for operators of "Strategic" and "High" electronic systems to undergo an SMPI certification against the Indonesian National Standard version of ISO/IEC 27001. For operators of "Strategic" electronic systems, the SMPI certification will also be against additional standards that have yet to be specified.[6] The SMPI certification must be done by a certification agency domiciled in Indonesia.[7] If awarded, the SMPI certificate will be valid for three years, but there is a further requirement for annual surveillance audits to be carried out.

Voluntary Market-Driven Certification

We recommend that the draft SMPI Regulation be amended to remove all requirements for mandatory certification (in respect of both the KAMI Index and the SMPI certification). Instead, the

[5] See Articles 10, 11, and 12 of the draft SMPI Regulation.

[6] See Articles 7 and 13.

[7] See Article 15.

focus should be on voluntary self-assessment and certification. In our experience, certification schemes may be effective measures to drive stronger cybersecurity, but they must be structured in a way that reflects market demands for both continuing innovation and broad diversity of product types and configurations. Market-driven incentives, such as tax incentives and safe harbours, for adopting any certification standards are preferable to other alternatives. Requiring adoption through legislation may have the unintended result of impeding flexible, outcome-oriented standards and eroding innovation as well as discourage investors and unicorns from establishing businesses and/or investing in Indonesia.

We also recommend that the draft SMPI Regulation should be streamlined to eliminate unnecessary reporting and audit requirements. The certification requirements described above, which contemplate two sets of certifications and reporting (one for the KAMI Index certificate and another for the SMPI certificate) will be extremely burdensome and will consume a great deal of time, energy and resources. MSMEs would be particularly impacted given their lack of financial, legal, compliance, and other resources. The following are a few ways in which BSSN could streamline the draft SMPI Regulation:

- Remove all provisions and requirements relating to the KAMI Index. It is unclear why there needs to be a separate KAMI Index certification or verification by BSSN, as compared with the ISO/ IEC 27001-based SMPI certification issued by a certification body acknowledged by BSSN. Removing potentially confusing elements of the certification framework would also be consistent with a voluntary market-driven certification approach, where electronic system operators would be left to self-assess/categorize their electronic systems, and to determine the best certificates to obtain, based on market demands and their own resourcing constraints.
- Align all certification/re-certification, reporting, and audit cycles to three years, which we note is the validity period indicated in Article 14(2) of the draft SMPI Regulation in respect of SMPI certificates.[8]

We further recommend that the draft SMPI Regulation should be amended to clarify that it is up to the electronic system operator to choose its certification agency, and to remove the requirement that the certification agency must be domiciled in Indonesia. This would allow for greater market competition in Indonesia among certification agencies, which would lead to lower certification fees overall. Recognizing certifications obtained outside of Indonesia, in line with our comments below, will also avoid duplicative in-country testing. All this would lower the cost burden for electronic system operators in Indonesia, including domestic MSMEs and as the cost savings can be passed on, would ultimately lead to lower costs to consumers of the electronic system operators' products and/or services.

Reliance on Internationally-Recognized Standards, Certifications, and Reports

We recommend that the standards to be referenced for the certification should all be internationally-recognized ones, and that the draft SMPI Regulation should be amended to recognize the validity of certifications and audit reports obtained from internationally-accredited testing/ auditing entities or laboratories for purposes of any domestic certification requirements, to avoid duplicative, costly and time-consuming in-country testing.

Reliance on internationally-recognized standards and certifications ensures interoperability for both businesses and government agencies with international counterparts, facilitating both economic development and operational collaboration against security threats. While we note that the draft

[8] We note, in relation to this, that Article 14(2) of the draft SMPI Regulation already provides for a 3-year effective period for SMPI certificates.

SMPI Regulation places some reliance on ISO/IEC 27001, it also references the KAMI Index and other yet-to-be-specified standards, which may represent a deviation from global standards. This may ultimately undermine the benefits associated with reliance on internationally-recognized standards.

Deviating from global standards in national implementation can have negative consequences. *First*, it will raise costs to governments by eliminating the economies of scale in production that allow governments to procure the highest quality products at lower prices. *Second*, government-imposed indigenous standards inconsistent with globally accepted best practices and standards, rather than bolstering security, tend to freeze innovation and force consumers and businesses into using products that might not suit their needs. *Third*, indigenous standards tend to harm the global competitiveness of MSMEs. Forcing domestic enterprises to build to national standards to win domestic contracts will render such enterprises unable to easily compete globally, where compliance with internationally-recognized standards is desired and will facilitate market entry in other countries.

4. Ensure that Sensitive and Proprietary Information is Protected

In the course of a certification audit, the auditor/certification agencies will likely gain or be able to gain access to sensitive and proprietary information of the electronic system operators. However, the draft SMPI Regulation currently does not contain any measures to protect such information. We accordingly recommend amending the draft SMPI Regulation to include protections for such information. Such protections could include, for example, provisions to ensure that auditors/certification agencies:

- should rely on audit reports and findings made on electronic system operators produced by independent third-party auditors (rather than needing to perform another separate inspection/audit on the electronic system);
- do not gain unnecessary access to source code, intellectual property and other sensitive and proprietary information;
- sign a non-disclosure agreement prior to any audit/inspection; and
- put in place appropriate protection/security measures to protect, against unauthorized access and use, any information that they gain access to in the course of the audit/inspection.

SPECIFIC COMMENTS

In addition to the general comments above, we have the following comments on specific provisions of the draft SMPI Regulation:

- **Article 1 –** The definitions used in the draft SMPI Regulation should be made consistent with the source regulations that it is intended to implement, e.g., GR82, Law 25, and Law No. 11 of 2008 on Electronic Information and Transactions (as amended by Law No. 19 of 2016).

- **Article 1(4)** – In line with our comments above, the definition of "Public Service" should be made consistent with other existing regulations. One possible approach would be for the SMPI Regulation to incorporate the definition in Law 25 by reference.[9]

- **Article 1(6)** – Information Security is usually defined as the triad of confidentiality, integrity and availability of information**.** The reference to originality ("keaslian") should be removed as it is not an understood term in the context of information security.

[9] For example, the SMPI Regulation could state that "*"Public Service" has the same meaning as in Law No. 25 of 2009.*"

- **Article 1(7)** – In line with our comments above, the definition of "Personal Data" should be made consistent with the definition of personal data in the draft PDP Bill. The use of two separate definitions would cause unnecessary confusion to the public.[10]

- **Article 3** – It is unclear what an "Operator Task Force" comprises and what "Missions of the State" means. There should be definitions for these terms. Based on Law 25, private entities carrying state mission(s) are those private entities running government programs and initiatives (e.g., government funded hospitals and schools participating in national curriculum), and not private commercial entities. Therefore, we suggest that BSSN clarify the scope of "state mission" to be consistent with the Law 25.

- **Articles 4(2) and 4(3)** – What is considered "serious" versus "limited" impact is vague and open to interpretation. Additional guidance and clarity should be provided in the draft SMPI regulation on what is considered "serious" versus "limited" impact.

- **Article 7(1) –** Instead of limiting the reference standards to the ISO27001 framework, we suggest that the government should consider allowing organizations to choose the relevant cybersecurity framework they should align to depending on their needs/ exposure/ environment. This also accords with our recommendation above to focus on voluntary market-driven certification.

- **Articles 7(3), 7(4), 10, 11, and 12** – In line with our comments above to remove references to the KAMI index, in order to streamline the draft SMPI Regulation and eliminate unnecessary reporting and audit requirements, we recommend the deletion of these references to the KAMI Index assessment. In the event that BSSN decides to retain these KAMI Index assessment, we recommend:
    - deleting Article 7(3), which unnecessarily duplicates the requirements in Article 10(3); and
    - amending the assessment and reporting cycle such that the assessment and reporting need only be made once every three years.

- **Article 8(3) –** We recommend amending this article as follows to allow multinational companies to use their own global teams for compliance:

    "*For the implementation of the standard as set out in Article 7 paragraph (1) for a strategic Electronic System, the Electronic System Operator should employ an Expert of Indonesian nationality where applicable*".

- **Article 11(2)** – Subject to our comments above on the removal of the KAMI Index requirements, as on-site assessments are likely to be disruptive to operations of electronic system operator, the Article should clarify that such assessment will be carried out at a time to be mutually agreed between the electronic system operator and BSSN.

- **Article 12(2)** – The reference to "paragraph (2)" appears to be a typographical error. We believe this should refer to "paragraph (1)" instead.

[10] The draft of PDP Bill defines "personal data" as "any data about a person whether identified and/ or can be identified separately or in combination with other information, directly or indirectly, through electronic and/ or non-electronic system". Again, a possible approach for aligning the definitions would be for the SMPI Regulation to state that "*"Personal Data" has the same meaning as in the [Personal Data Protection Law].*"

- **Article 13** – This Article states that the SMPI certificate is optional for "Low" electronic systems. However, Article 7.3 says the KAMI Index guidelines must be implemented by the electronic system operator and must report the results of its self-assessment to BSSN every year. Subject to our comments above on the removal of the KAMI Index requirements, if the intention is for certification of "Low" electronic systems to be voluntary/optional, then Article 7.3 should be amended for consistency to state that the implementation of the KAMI Index is voluntary.

- **Article 15** – We recommend including a requirement for BSSN to publish the list of entities that BSSN acknowledges and that can provide certification under the draft SMPI Regulation.

- **Article 20(1)** – Rather than the certification agency submitting results to BSSN directly, the process should be that the certification agency submits the results to the electronic system operator for the operator to then forward it to BSSN. This will give the electronic system operator an opportunity to correct any shortcomings or deficiency to be able to obtain the relevant certification. This would also be consistent with a certification framework where the electronic system operator has the discretion to choose its certification agency (as recommended in our general comments above)

- **Articles 20(2) and 21** – The certification agency is required to submit the report at least twice per year and carry out a surveillance audit at least once every year, although the Information Security Management System Certificates itself will be valid for three years as stipulated in Article 14(2). It is unclear why there is a need to conduct such frequent reporting and surveillance audit. In line with our comments above, we recommend aligning all certification/re-certification, reporting, and audit cycles to three years in line with Article 14(2).

- **Article 22** – We would like to seek clarification on what would be the consequence(s) of a revocation of certification, as contemplated under this Article.

- **Schedule 1.7** – The definitions of "very confidential", "confidential", and "normal" are not clear. The terms may require further clarification to determine which systems should be identified as "Strategic", "High", and "Low".

- **Sample Format 1** – We recommend that there should be weightages assigned to the respective criteria, as not every criterion listed is of equal importance. For example, criteria 1,9 on "Impact of Electronic System failure" would be a much more important consideration than the criteria 1,1 on "Investment value of installed electronic system". Moreover, we recommend that criteria 1.1 and 1.2 should be removed as these criteria penalize organizations with high capital and operational expenditure, which are not necessarily indications of the strategic nature of the organization's systems. For example, foreign airlines have high capital and operational expenditure, and have made significant investments in operating and maintaining planes, ticketing, booking, flight tracking and customer management systems. The criteria in 1.1 and 1.2 of Sample Format 1 would have the consequence of classifying foreign airlines as a strategic electronic system provider, and the consequence (under GR82) that data of individuals in Indonesia will not be able to be transferred out of Indonesia (which would not be realistic in the context of international air travel).

CONCLUSION

We thank you again for conducting an open and transparent consultation process as you seek to further develop an effective regulatory approach to information security systems management. We believe that there are great opportunities for industry and the Government of Indonesia to work together on developing and implementing such an approach.

Our organizations and our respective members stand ready to work with BSSN to further improve the draft SMPI Regulation. We hope that our input will be useful to improve the current draft SMPI Regulation and we would welcome a meeting with BSSN to further discuss our concerns.

We thank you for considering our views.

Sincerely,

Alexander C. Feldman
President & CEO
U.S.-ASEAN Business Council

Darryn F. Lim
Director, Policy – APAC
BSA | The Software Alliance

cc: Critical Information Infrastructure Directorate, National Cyber and Encryption Agency
Amb. Joseph R. Donovan Jr., Ambassador of the United States to the Republic of Indonesia
Amb. Mahendra Siregar, Ambassador of the Republic of Indonesia to the United States