July 26, 2024

Mr. Budi Arie Setiadi
Minister

Ministry of Communications and Informatics
Jl. Medan Merdeka Barat No. 9
Jakarta Pusat

BSA COMMENTS ON NATIONAL DATA CENTER ISSUES

Dear Pak Budi:

On behalf of BSA | The Software Alliance (**BSA**),[1] we send you our sincere regards. BSA has been actively participating in the developments related to the National Data Center. BSA provided comments to the Ministry of Communication and Informatics (**KOMINFO**) on the Draft Regulation Concerning Public Scope Electronic System Operators.[2] We also joined a Multi-Association Input Letter on the Public Electronic Service Providers Draft Regulation.[3] Most recently, BSA co-organized the event "Advancing Indonesia's Digital Ecosystem: US–Indonesia Commercial Discussion" on May 8, 2024, with the US Embassy in Jakarta and KOMINFO, where Indonesian and US government officials and industry representatives discussed a variety of issues including the National Data Center project.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create business-to-business technologies that help other businesses innovate and grow. For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, cybersecurity services, and collaboration systems. BSA offers our extensive global experience in technology policy to serve as a resource and we hope that our comments in this letter will be helpful to KOMINFO.

We would like to express our concern regarding the recent cybersecurity attack on the National Data Center.[4] This incident highlights the growing threat of cyber-attacks and the urgent need to enhance our collective defenses to protect sensitive information and maintain public trust. We understand the sensitive nature of this issue and commend KOMINFO for the swift action you have taken to address

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Cohere, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc

[2] See https://www.bsa.org/policy-filings/indonesia-comments-on-draft-regulation-of-the-minister-of-communications-and-informatics-concerning-public-scope-electronic-system-operators, 16 October 2023.

[3] See https://www.bsa.org/policy-filings/indonesia-joint-association-input-letter-on-public-electronic-service-providers-draft-regulation, 23 May 2023.

[4] See https://www.channelnewsasia.com/asia/cyberattack-hits-indonesia-data-centre-demands-us-8-million-ransom-lockbit-russia-4434191, 25 June 2024.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

the situation. In light of this event, we would like to extend our support and offer some suggestions to improve the policies surrounding the National Data Center and to improve their cybersecurity.

Data Localization Undermines Cybersecurity

As discussed in our previous comments,[5] current provisions in the Draft Regulation on Public Electronic Service Operators (**ESOs**) essentially require Public ESOs to locate their data within the National Data Center, a form of *de facto* data localization. Such data localization mandates create security, logistical, and operational challenges for many cloud service providers that store, process, and backup data in regional data centers outside of Indonesia and consequently are a barrier to the Indonesian government and Indonesian businesses harnessing the full potential of cloud services. Requiring data localization, whether formally or *de facto*, distorts the market for cybersecurity solutions by placing undue value on which companies are best at complying with data localization requirements rather than on which companies are best at providing the best functioning and most secure solutions. Cloud security laws and policies should recognize that security is not inherently linked to data location but rather to the security controls that a cloud service provider or user applies to data, such as identity and credential access management. When governments restrict a company's ability to move data, they may create unnecessary obstacles to data security. Locally hosted data is not free from cybersecurity risks; it is subject to the same types of cyberattacks as cloud services, because locally hosted data is also connected to the larger Internet. Local data storage depots, however, must combat these attacks without ready access to multinational cloud service providers' resources and security measures, which are a major focus for those providers. Additionally, depending on the locale, locally hosted data may be subject to greater physical risks of disruption – e.g., typhoons, earthquakes or other natural disasters that can compromise data integrity and continuing of services.

Cross-border data transfers are an important cybersecurity tool for several reasons. Such transfers enhance capabilities to protect against physical access and create redundancy, increase resiliency, and reduce latency. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. In the context of the recent cybersecurity incident, the ability to use offshore data centers to ensure redundancy and backup is very valuable. Data stored in physically remote data centers can be used to recover from data center outages, whether from cybersecurity incidents or natural disasters. On the other hand, when governments put in place data localization requirements or restrict the ability to transfer and analyze global data in real-time, they may create unintended vulnerabilities, reduce resilience and recovery capabilities, and deny their countries access to the latest global threat information.

Cutting Edge Cybersecurity Solutions from the Private Sector

As you consider how to develop and implement policies applicable to the National Data Center, we ask that you consider how these solutions fit within the broader technology products and services landscape. Approaching cybersecurity regulations horizontally enhances the security of all products and services, not just cloud services, promotes greater cross-ecosystem consistency, and fosters risk-based approaches that not only evolve with changing technology but encourage their continued improvement.

The starting point for laws and policies that support innovation while also improving security is recognizing that cloud security is not categorically different than cybersecurity in general. Both begin with a foundation of effective risk management. Although cloud services pose unique challenges, those challenges are still best confronted from a risk management, outcomes-based posture focused on establishing and implementing best practices.

---

[5] See https://www.bsa.org/policy-filings/indonesia-comments-on-draft-regulation-of-the-minister-of-communications-and-informatics-concerning-public-scope-electronic-system-operators, 16 October 2023.

Requiring Public ESOs to use only the National Data Center prevents them from using services provided by global cloud service providers, even when those services provide better functionality, competitive pricing, and superior security.. As the capabilities of malicious actors in cyberspace evolve, governments need to ensure that they have the best tools at their disposal to deal with emerging cyber threats. If companies that have developed effective cybersecurity solutions are not able to provide services to Public ESOs, Public ESOs will have both more limited and more costly options that cannot provide cutting-edge cybersecurity.

Taking advantage of readily available commercial solutions expedites digital transformation. We encourage KOMINFO to consider how policies that further facilitate the use of commercial solutions by Public ESOs would encourage improved cybersecurity and create positive spillover effects to strengthen the security of the entire ecosystem. This includes allowing Public ESOs to make use of private sector solutions such as cloud services on the public cloud. Further information is available in BSA's Principles for Government Cloud Security Laws and Policies.[6]

Conclusion

BSA reiterates our support to KOMINFO and our wish to act as a resource on international developments and best practices for technology policy. We stand ready to support the Indonesian government and hope that our comments will assist in improving the policies related to the Indonesia's National Data Center project. **Additionally, we would like to offer an introductory call your incoming Director-General of APTIKA to continue the discussion.** Please do not hesitate to contact the undersigned at waisanw@bsa.org to make arrangements.

Yours faithfully,

Wong Wai San

Wong Wai San

Senior Manager, Policy – APAC

Cc:

Vice Minister

Ministry of Communication and Informatics

Director General, APTIKA

Ministry of Communications and Informatics

[6] See https://www.bsa.org/policy-filings/global-principles-for-government-cloud-security-laws-and-policies, 28 June, 2022,