



Badan Siber dan Sandi Negara Republik Indonesia
National Cyber and Cryptography Agency (BSSN) of Indonesia
Jl. Raya Muchtar No.70, Bojongsari Lama,
Kec. Bojongsari, Kota Depok,
Jawa Barat 16516,
Indonesia

14 March 2025

Dear sir/madam,

Re: Feedback on the Draft Law on Cyber Security and Resilience (RUU KKS)

The Coalition for Cybersecurity in Asia Pacific (CCAPAC) is a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building.

We understand that the BSSN is drafting a Law on Cyber Security and Resilience (RUU KKS). We applaud Indonesia for developing the law, which will help strengthen Indonesia's digital security and increase national resilience to the increasingly complex cyber threat landscape.

In view of the upcoming law, we wish to make a number of observations and recommendations, to ensure that the Law on Cybersecurity and Resilience balances the need for cybersecurity governance while still promoting innovation, trade, and economic growth in Indonesia.

- 1. The use of international standards for infrastructure provision, and for cybersecurity products and services.** We would like to encourage the BSSN to consider utilising international standards such as those from the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and other international industry standard approaches, for Indonesia. Using international standards - rather than developing national domestic standards or certifications for cybersecurity products and services - help businesses of any size and sector reduce costs, increase productivity, and also help local firms access new markets easily when their products are easily-identifiable as meeting international quality checks.
- 2. Encouraging trade and commerce through reduction of non-tariff barriers, such as data localization requirements.** We encourage BSSN to consider ensuring that there are no data localization requirements in the Law on Cyber Security and Resilience, as this can increase costs for businesses which may be passed to consumers, reduce innovation and productivity if cross-border data flows are impacted, and hinder global trade and economic growth. We recommend a nuanced approach towards concerns around international data transfers, such as creating mechanisms to enable such transfers, and/or frameworks such as the APEC Cross-Border Privacy Rules (CBPR) system.
- 3. Dialogue, capacity-building, and training with the private sector.** We understand that there may be other areas of concern for Indonesia's cyber landscape, and we would encourage a strong dialogue with the private sector to address other concerns in consultation, while

policymakers draft this important law. CCAPAC members stand ready to discuss issues such as critical infrastructure management, data governance and classification, supply chain security, and also offer up possible capacity-building and training programmes for the public sector, to increase government staff capabilities and resilience in cyber security matters.

We believe that these approaches can help achieve the goals of developing a strong cybersecurity regulatory landscape, while promoting innovation, trade, and economic growth. **We would like to suggest an online meeting on 10 April 2025 at 4pm (Indonesia time) for an informal discussion on these suggestions from the CCAPAC, and next steps.**

We look forward to hearing from you on this engagement, and would be happy to have the opportunity to discuss these suggestions further and collaborate with the BSSN to develop a balanced and effective cybersecurity framework for Indonesia.

Sincerely,

Lim May-Ann
Director
Coalition for Cybersecurity in Asia Pacific
ccapac@accesspartnership.com