LAB 45 — TELAAH KEBIJAKAN

No. 050 - 18 Mei 2026

Indonesia's Cyber Security and Resilience Bill: Progress, Setbacks, and What Remains Unresolved

Christian Guntur Lebang
Koordinator Analis, Laboratorium Indonesia 2045

When President Prabowo Subianto's administration sent a Presidential Letter (Surpres No. R-07) to the House of Representatives on the Cyber Security and Resilience Bill (RUU KKS), formally confirmed in the DPR's 16th Plenary Session on 12 March 2026, it marked the opening of a legislative debate that will shape how Indonesia regulates cybersecurity for the foreseeable future (ANTARA, 2026). The bill has been designated a Prolegnas priority for 2026. Deliberation is now underway in earnest.

This piece examines the November 2025 draft, the most recent version circulated among researchers and policy experts, against the concerns raised when an earlier version first surfaced in early 2025. The picture is mixed. Several of the most visible problems have been addressed. But the deliberation process also introduced a new obligation that was not in the original draft and removed a safeguard that had briefly appeared. Understanding which changes are real and which are cosmetic matters now, before the text is locked in committee.

What the Academic Justification Gets Right and Leaves Unanswered

There is a genuine gap in Indonesia's legal architecture that the RUU KKS is trying to fill. The Electronic Information and Transactions Law (UU ITE) was built around individual conduct in digital spaces: content, transactions, defamation. The Criminal Code addresses crimes that happen to use digital tools. Neither was designed to protect critical information infrastructure as such, and the June 2024 ransomware attack on the National Data Centre, which knocked out immigration, education, and other services across more than 200 government agencies, made that gap impossible to ignore.

The problem is not the case for legislating. Indonesia's existing framework under Presidential Regulation No. 82 of 2022 (Perpres 82/2022) established incident reporting timelines and tiered response structures, but as a presidential regulation it carries no enforcement sanctions: operators face no legal consequence for non-compliance. That gap is a legitimate reason for a law. What the Academic Paper

does not explain is why closing that enforcement gap requires mandatory real-time connectivity with the national security operations centre, rather than simply attaching sanctions to the obligations that already exist.

What Has Changed in the Draft: Reading the Trajectory

The inter-ministerial committee process between February and November 2025 produced real changes. BSSN's authority to filter online content (Article 69g) was gone by October. TNI personnel as designated cybercrime investigators appeared in the October draft (Article 56(1)(d)) and were removed in the Final following public pushback (DW Indonesia, 2025). BSSN's autonomous investigative powers, which in February extended to search, seizure, and asset forfeiture (Article 82), were stripped entirely from the Final, with criminal investigation authority returned to the general criminal procedure framework.

The treatment of artificial intelligence also evolved. The February draft gave BSSN exclusive authority over AI use within critical information infrastructure (Article 43), directly conflicting with Kemkomdigi's 2023 AI ethics circular. Article 36(2) in the Final assigns AI governance to "the Government" broadly without specifying which ministry, recreating the conditions for inter-agency disputes. But Article 35(4) adds an explicit requirement that AI use "remain under human control and supervision," absent from all earlier versions. That is a meaningful addition.

Table 1. Key changes across three draft versions of the RUU KKS (February, October, and November 2025)

Issue	February 2025	October 2025	Final (November 2025)
Content filtering by BSSN	Present (Art. 69g)	Removed	Absent
Military as cybercrime investigators	Absent	Present (Art. 56(1)(d))	Removed
BSSN autonomous investigative powers	Broad (Art. 82)	Retained	Stripped entirely
NSOC real-time integration	Absent	Introduced (Art. 15(c))	Retained
Judicial oversight for access restriction	Absent	Present (Art. 56(3))	Removed
PDED enforcement sanctions	Present (Art. 10(5), Feb.)	Present (Art. 57(3))	Removed
AI regulatory authority	BSSN-exclusive over IIK (Art. 43)	Reformulated: "Government" broadly (Art. 36(2))	Retained — human-in-the-loop safeguard added (Art. 35(4))

Source: Author's own compilation.

What the table reveals is a pattern that deserves scrutiny. The provisions removed were all politically legible: content filtering, military investigators, BSSN acting as police. The provisions that moved in the other direction are technically dense: NSOC integration was quietly added in October and never removed; judicial oversight for access restriction measures briefly appeared and was quietly removed. What left quietly is more consequential than what left publicly.

The NSOC Mandate: A New Obligation Without a Model

Article 15(c) of the November 2025 draft requires all Critical Information Infrastructure (IIK) operators, government agencies and private companies alike, to connect their security monitoring systems to BSSN's National Security Operations Centre (NSOC) in real time. This obligation was introduced in October and survived into the Final unchanged; it was not in the February 2025 draft.

None of the major comparative frameworks reviewed for this piece use standing connectivity as the baseline obligation. Singapore requires incident reporting within defined windows for designated critical infrastructure operators, not continuous access to network telemetry (Hogan Lovells, 2025). The EU's NIS2 Directive operates on 24-hour early warnings and 72-hour full reports, triggered by specific incidents (NIS2 Directive, Article 23). Australia's Security of Critical Infrastructure Act uses tiered, incident-triggered information-sharing rather than a standing connection (SOCI Act 2018). The United States maintains a statutory wall between cybersecurity data collection and law enforcement use, requiring separate authorisation to cross it (PPD-41, 2016).

What makes the Indonesian provision difficult to defend is the absence of any legal architecture around what happens to the data that flows into NSOC. The Final draft is silent on retention limits, purpose restrictions, and the rights of private sector entities whose network telemetry flows into the centre. Article 9(2)(g)'s data protection requirement governs operators, not BSSN.

Jurisdictions that expand government access to security data generally embed legal protections in the same legislation. Australia's Cyber Security Act 2024 prohibits using incident-related disclosures as evidence in civil or criminal proceedings (Australian Cyber Security Act 2024). The Indonesian draft contains nothing equivalent.

Against this, consider what Indonesia already has. Perpres 82/2022 (Articles 12–13) requires incident reporting within 24 hours and gives BSSN a coordinating rather than a monitoring role. The shift to permanent real-time integration is a qualitative change in the relationship between the state and private infrastructure operators, and neither the Academic Paper nor the draft text offers a rationale for why it is necessary.

PDED: The Wrong Borrowing at the Wrong Time

The chapters on "Products with Digital Elements" (PDED) in Articles 30–38 are taken from the EU's Cyber Resilience Act framework; Article 1(14)'s definition is functionally identical to the EU CRA text, and Article 32(1) reproduces its eleven-point compliance checklist for producers of network-facing hardware and software (EU Regulation 2024/2847).

The EU CRA is designed to function within a specific institutional ecology: independent conformity assessment bodies, explicit carve-outs for open-source software and small enterprises, confidentiality protections for software bills of materials, and safe harbour provisions for security researchers. Indonesia's draft addresses some of these elements but only partially. A certification requirement appears in the Elucidation of Article 30(5) rather than the statute's operative text, with no detail on institutional structure. Small enterprises receive no exemptions or transition periods, SBOM-equivalent documentation is mandated under Article 32(1)(c) without any confidentiality protection for what it contains, and security researcher immunity under Article 60 is limited to authorised testing of critical infrastructure rather than independent research on commercial products.

There is also a timing problem. The EU's November 2025 Digital Omnibus, targeting nearly €12 billion in administrative cost reduction, was a direct acknowledgement that the CRA's compliance burden had become unworkable (European Commission, 2025). Indonesia is codifying a model the jurisdiction that designed it is actively walking back.

No ASEAN peer has taken the same path. Singapore, Japan, and Malaysia have all chosen operator-side obligations or voluntary labelling schemes rather than producer mandates, and Indonesia would be the only country in the region to have explicitly imported the CRA's producer-side construct (CSA Singapore; METI Japan, 2025).

The Final draft's treatment of PDED enforcement compounds the concern. The October version included mandatory product recalls as a sanction (Article 57(3)); the Final removes this entirely, leaving only written warnings and fines. A regulatory regime that cannot compel a non-compliant product off the market has no credible enforcement mechanism.

A Law That May Not Be Operational When It Passes

What happens after the RUU KKS is enacted has received less attention than it deserves. The bill shifts terminology from IIV (the term used in Perpres 82/2022) to IIK, but Article 62's transitional provision handles the relationship to existing law in a single generic clause: prior regulations "shall remain in force insofar as they do not conflict" with the new law. Perpres 82/2022 is not named. Whether its event-based reporting model "conflicts" with Article 15(c)'s real-time integration mandate is left to whoever reads the statute first, and that institution will almost certainly be BSSN, without any review mechanism.

Article 63 gives the government two years to issue all implementing regulations, with no sequencing by provision and no consequence for missing the deadline. This is not an abstract concern. The Personal Data Protection Law (UU PDP) entered full legal force in October 2024 after its own two-year transition, and as of mid-2025 not a single implementing PP had been issued and the supervisory body had not been established (Hukumonline, 2025). That is a governance failure; for a cybersecurity law, it would also be a security risk.

Recommendations

First, the NSOC obligation needs to be restructured, not just monitored. Article 15(c) in its current form is an open-ended data collection mandate dressed as a cybersecurity provision. Connectivity requirements should activate on incident thresholds, consistent with how Singapore, NIS2, and Australia approach the problem, and data use limitations covering retention, sharing, and purpose need to be in the statute, not left to a future implementing regulation.

Second, BSSN's expanded authority requires a matching accountability framework. The Final draft increases BSSN's reach over network monitoring, PDED compliance, and IIK designation, while the agency still reports only to the President based on Perpres 28/2021. Parliamentary reporting, independent review of decisions that significantly affect private entities, and an administrative appeals process should be written into the statute. Accountability of this scale, over both public and private infrastructure, requires it.

Third, the PDED chapter should be separated from the core law. Protecting critical infrastructure does not require regulating who can manufacture what. The chapter

should be developed separately, once Indonesia has the conformity assessment and market surveillance capacity the framework requires.

Fourth, the transitional provisions need to be specific. Article 62's savings clause creates an interpretive vacuum over the relationship with Perpres 82/2022 that BSSN will fill by default; it should be stated explicitly. Article 63's uniform two-year deadline should be disaggregated: regulations governing what BSSN can do with NSOC data must exist before Article 15(c) takes operational effect. The UU PDP has been formally in force since October 2024 and still has no implementing regulations or supervisory body. That is what a two-year deadline without sequencing produces.

Conclusion

The RUU KKS has improved since it first circulated. Content filtering authority is gone. Military investigators were added and then removed. BSSN's autonomous investigative powers did not survive the drafting process. A human-in-the-loop requirement for AI systems was added where none existed before. A legislative process capable of responding to serious public criticism is not nothing, and it would be unfair not to say so.

But the changes that carry the most long-term consequence moved in the other direction, and they moved quietly. NSOC real-time integration was not in the February draft. It appeared in October, drew less public attention than the provisions that were being removed, and is now in the Final. Judicial oversight for access restriction measures had a brief appearance in October and was gone by November. The PDED framework retains its ambitions without its enforcement teeth.

The draft that reaches committee is improvable. Whether it will be improved is a different question, one that depends, in the end, on whether the deliberation is open enough for the public to see what is actually being decided. Recent legislative processes in Indonesia have not always met that standard, and the people who will live under this law deserve better than to find out what is in it after it passes.

Referensi

ANTARA (2026). DPR terima Surpres RUU PSDK hingga RUU Keamanan dan Ketahanan Siber. *ANTARA*. https://www.antaranews.com/berita/5469723/dpr-terima-surpres-ruu-psdk-hingga-ruu-keamanan-dan-ketahanan-siber

Australian Cyber Security Act 2024. https://www.legislation.gov.au/Series/C2024A00098

CSA Singapore (n.d.). Cybersecurity Labelling Scheme. *CSA Singapore*. https://www.csa.gov.sg/our-programmes/technology-trust-safety/cybersecurity-labelling

DW Indonesia (2025). Draf RUU KKS: Peran TNI sebagai Penyidik Siber Tuai Kritik. *DW Indonesia*. https://www.dw.com/id/draf-ruu-kks-peran-tni-sebagai-penyidik-siber-tuai-kritik/a-74257750

EU Regulation 2024/2847 (Cyber Resilience Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

European Commission (2025). Digital Omnibus Press Release. *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718

Hogan Lovells (2025). Provisions in Singapore's Cybersecurity (Amendment) Act came into force on 31 October 2025. *Hogan Lovells*. https://www.hoganlovells.com/en/publications/provisions-in-singapores-cybersecurity-amendment-act-came-into-force-on-31-october-2025

Hukumonline (2025). Menanti Disahkannya Aturan Turunan UU PDP. *Hukumonline*. https://www.hukumonline.com/berita/a/menanti-disahkannya-aturan-turunan-uu-pdp-lt68fae7fbe057d

METI Japan (2025). JC-STAR Scheme Launch. *METI*. https://www.meti.go.jp/press/2024/03/20250331004/20250331004.html

NIS2 Directive (EU) 2022/2555. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Peraturan Presiden No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. https://peraturan.bpk.go.id/Details/163476/perpres-no-28-tahun-2021

Peraturan Presiden No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. https://peraturan.bpk.go.id/Details/208947

PPD-41 (2016). United States Cyber Incident Coordination. *The White House*. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Security of Critical Infrastructure Act 2018 (Australia). https://www.legislation.gov.au/Series/C2018A00029

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Jalan Mabes Hankam No. T65, Bambu Apus, Cilangkap, DKI Jakarta 13890
Email: lab45@lab45.id | Telpon: +62811452045

Silahkan hubungi tim editorial untuk pertanyaan melalui
lab45@lab45.id