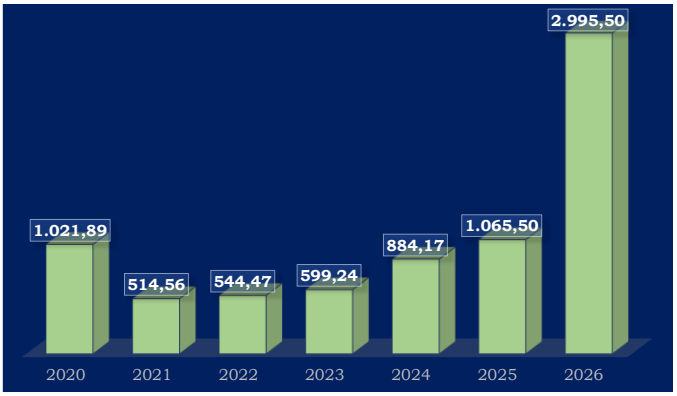
Analisis
PAGU ANGGARAN
2025

ANGGARAN BADAN SIBER DAN SANDI NEGARA TAHUN 2026: HARUS MAMPU MENJAWAB BERBAGAI TANTANGAN KETAHANAN DAN KEAMANAN SIBER KE DEPAN

www.bkd.dpr.go.id

Realisasi anggaran Badan Siber dan Sandi Negara (BSSN) sepanjang 2020 hingga 2024 berfluktuasi. Realisasi anggaran pada 2021 mengalami penurunan tajam dibanding 2020, yakni 49,65%. Setelah itu, mengalami peningkatan setiap tahun sepanjang 2022-2024, dengan rata-rata pertumbuhan sebesar 21,14% (Gambar 1). Realisasi anggaran tersebut mayoritas dialokasi pada Program Keamanan dan Ketahanan Siber dan Sandi Negara (Program K2S2).



Gambar 1. Perkembangan Anggaran BSSN 2020-2026 (Miliar Rp)
Sumber: Nota Keuangan APBN Berbagai Tahun dan Badan Pemeriksa Keuangan, 2025 (diolah)

Outlook alokasi anggaran dalam APBN 2025 mencapai Rp1.065,50 miliar, meningkat 20,51% dibanding realisasi 2024. Pada 2026, alokasi pagu anggaran BSSN sebesar Rp2.995,5 miliar, meningkat 181,14% dibanding *outlook* alokasi dalam APBN 2025. Alokasi pagu anggaran 2026 tersebut dimanfaatkan untuk mendukung prioritas nasional antara lain melalui kegiatan penguatan ekosistem keamanan siber dan sandi di Indonesia yang pendanaannya bersumber dari pinjaman luar negeri (Nota Keuangan RAPBN 2026). Selain itu, alokasi pagu anggaran tersebut juga akan dimanfaatkan untuk penguatan ekosistem keamanan siber di Indonesia dan pemeliharaan operasional perangkat keamanan siber/sandi secara berkelanjutan.

Dalam konteks Rencana Pembangunan Jangka Menengah Nasional Tahun 2025-2029 (RPJMN 2025-2029), alokasi anggaran BSSN 2026 ditujukan untuk mendukung program prioritas nasional "Keamanan Siber, Sandi, dan Sinyal", dengan sasaran "Terwujudnya interaksi dan transaksi siber, persandian, dan sinyal yang aman". Ketercapaian sasaran tersebut diukur dengan Indeks Keamanan dan Ketahanan Siber, yang ditargetkan sebesar 0,84 pada 2029.

Critical Notes: Alokasi 2026 Harus Mampu Menjawab Berbagai Tantangan Ketahanan dan Keamanan Siber

Ketahanan dan keamanan siber merupakan salah satu faktor penting dalam memperkuat daya saing perekonomian suatu negara. Saat ini, Pemerintah, masyarakat dan perusahaan sebagai pelaku ekonomi sudah semakin mengandalkan teknologi untuk mengelola segala hal mulai dari layanan publik hingga proses bisnis, bahkan belanja kebutuhan sehari-hari. Kondisi ini berimplikasi pada meluasnya ketergantungan pada sistem digital.

Dalam konteks ketergantungan yang meluas pada sistem digital yang semakin kompleks, ancaman siber yang semakin meningkat melampaui kemampuan masyarakat untuk mencegah dan mengelolanya secara efektif. World Economic Forum (2023) menyebutkan serangan siber merupakan salah satu dari sepuluh risiko terbesar terhadap perekonomian global dalam lima tahun ke depan, khususnya karena dapat melumpuhkan layanan penting (termasuk layanan publik) dan aktivitas perdagangan.

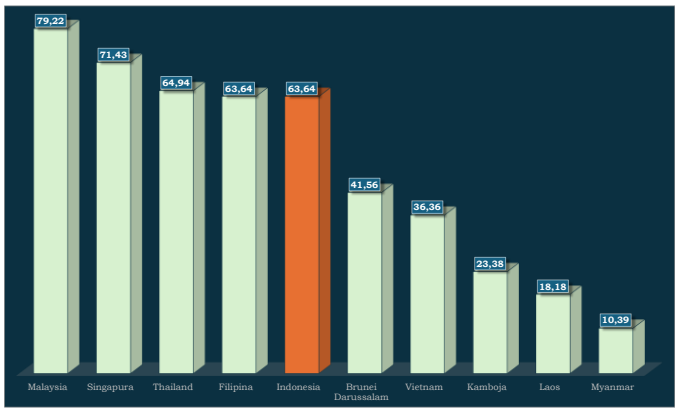
Negara yang tidak memiliki ketahanan siber yang memadai akan menghadapi tantangan besar dalam menjaga kelangsungan layanan publik, transaksi bisnis, serta daya tarik investasi asing. OECD (2022) menyebutkan *digital security* sebagai aspek ekonomi dan sosial dari *cybersecurity* diperlukan untuk membangun kepercayaan dalam ekonomi yang semakin bergantung pada teknologi digital. Dengan demikian, ketahanan dan keamanan siber bukan hanya isu teknis, melainkan juga bagian integral dari kebijakan ekonomi dan strategi pembangunan nasional. Ketika sistem digital rentan dan tidak aman terhadap serangan, hal ini dapat menurunkan kepercayaan investor dan pelaku usaha, mengguncang stabilitas ekonomi, serta menghambat pertumbuhan. Oleh karena itu, negara yang memiliki keamanan siber yang mumpuni memiliki keunggulan kompetitif dalam menjaga keandalan layanan, stabilitas perekonomian dan menarik investasi.

Apabila merujuk pada keterkaitan erat antara keamanan dan ketahanan siber terhadap kinerja dan daya saing perekonomian, Komisi I DPR RI perlu mendorong agar alokasi anggaran BSSN tahun 2026 diarahkan untuk menjawab berbagai tantangan keamanan dan ketahanan siber. **Pertama, ancaman siber yang meningkat seiring dengan peningkatan jumlah pengguna internet**. Jumlah pengguna internet di Indonesia telah mencapai 221,6 juta penduduk atau tingkat penetrasinya telah menyentuh angka 79,5% (Kementerian Komunikasi dan Digital, 2025; Haryanto, 2024). Peningkatan pengguna internet tersebut berimplikasi peningkatan volume data dan peningkatan perangkat terhubung, baik milik individu, perusahaan, maupun sektor publik. Kondisi ini membuka celah bagi berbagai ancaman dan serangan siber, seperti *malware*, *ransomware*, dan aktivitas peretasan yang menyasar data sensitif. Berdasarkan laporan dari perusahaan keamanan siber global seperti Kaspersky, Indonesia termasuk dalam 10 besar negara yang menjadi sasaran serangan siber global, dengan jenis serangan yang paling sering terjadi meliputi DDoS (*Distributed Denial of Service*), *ransomware*, dan *phishing* (Salwa, 2024). Celah ancaman siber tersebut berdampak pada pengawasan dan perlindungan terhadap infrastruktur kritikal negara semakin kompleks (Salwa, 2024). Terlebih lagi, perkembangan tren teknologi baru seperti *Internet of Things* (IoT) dan kecerdasan buatan turut memperluas vektor serangan yang harus diantisipasi. Dengan demikian, kecepatan BSSN dalam mendeteksi, merespons dan mengatasi kondisi ini sangat diperlukan guna menjaga sistem siber nasional.

Kedua, rendahnya kesadaran dan budaya masyarakat atas keamanan siber. Kesadaran dan budaya keamanan siber masyarakat sangat menentukan potensi dan eskalasi ancaman siber. Rendahnya kesadaran, kemampuan dan budaya untuk mengenali tautan berbahaya, menggunakan sandi yang kuat, atau membedakan informasi valid dan hoaks membuat individu rentan terhadap serangan seperti *phishing*, *ransomware*, dan *social engineering*. Kondisi ini tidak hanya terbatas berdampak pada masyarakat secara personal, namun juga berpotensi berdampak dan menjalar pihak lain dan infrastruktur kritikal ketika individu masyarakat terhubung langsung atau tidak langsung dengan sistem yang lebih luas. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada 2023 mengungkap 74,59% masyarakat Indonesia tidak menyadari atau merasa belum pernah mengalami peretasan siber, 66,82% tidak pernah mengganti kata sandi akun pribadi, dan 36,4% masih menggunakan kombinasi angka sebagai metode penguncian ponsel (Salwa, 2024). Angka-angka tersebut menunjukkan masih banyak masyarakat di Indonesia yang belum sepenuhnya memahami pentingnya kata sandi dalam melindungi akun dan perangkat mereka. Hal ini juga dipertegas BSSN yang menyebutkan budaya keamanan siber di masyarakat masih menjadi tantangan ke depan seiring perkembangan teknologi informasi (Badan Siber dan Sandi Negara, 2025). Dengan demikian, BSSN perlu melakukan upaya peningkatan kesadaran dan budaya keamanan siber di masyarakat.

Ketiga, percepatan pemenuhan kuantitas dan pengembangan kualitas Sumber Daya Manusia (SDM) di bidang keamanan siber. Ketersediaan SDM di bidang keamanan siber yang mendeteksi, mencegah, dan merespons ancaman siber secara efektif memiliki peran vital dalam menjaga keamanan dan ketahanan siber nasional. Ketersediaan SDM tersebut juga dibutuhkan guna memperkuat ekosistem dan transformasi digital nasional. Secara umum, Indonesia menghadapi kekurangan talenta di bidang keamanan siber, baik dari segi jumlah maupun kualitas, yang menyebabkan banyak organisasi kesulitan dalam merekrut atau mempertahankan personel dengan keahlian teknis untuk mendeteksi, merespons, dan memulihkan diri dari insiden siber (Badan Siber dan Sandi Negara, 2025; Nugraha, 2025; Vincha & Satrio, 2024). Spesifik pada instansi pemerintah daerah, kekurangan SDM dan kapabilitas teknis dalam mengidentifikasi, mengevaluasi, dan mengelola kerentanan secara efektif juga masih menjadi masalah di pemerintah daerah, sehingga menimbulkan celah keamanan yang dapat dieksploitasi oleh pelaku ancaman siber (Nurhidayat et.al, 2024).

Keempat, perlu upaya percepatan mengejar ketertinggalan keamanan siber dengan negara satu kawasan. Ketahanan dan keamanan siber sebuah negara sangat berpengaruh terhadap kepercayaan investor dan pelaku usaha, sehingga akan berdampak pada daya saing investasi dan perekonomian sebuah negara. Nilai *National Cyber Security Index* Indonesia pada 2023 sebesar 63,64 poin. Angka tersebut masih lebih rendah dibanding Malaysia, Singapura dan Thailand (Gambar 2). Apabila menelusuri indikator dan sub-indikator pembentuk indeks, terdapat beberapa hal yang perlu menjadi perhatian BSSN, antara lain:



Gambar 2. Perbandingan *National Cyber Security Index* Indonesia Dengan Negara Kawasan ASEAN Tahun 2023
Sumber: E-Governance Academy Foundation, 2025 (diolah)

a. strategi keamanan siber tingkat nasional atau dokumen setara lainnya;
b. analisis situasi ancaman siber strategis nasional dilakukan entitas khusus;
c. pengawasan penyedia layanan digital publik dan swasta terkait penerapan persyaratan keamanan siber/informasi;
d. penyusunan dan penetapan rencana manajemen krisis untuk insiden siber berskala besar;
e. integrasi kompetensi keselamatan siber/keselamatan komputer dalam kurikulum pendidikan dasar dan menengah;
f. penyedia layanan digital sektor publik harus menerapkan persyaratan keamanan siber/TIK atau standar keamanan yang diakui luas, serta
g. koordinasi keamanan siber internasional.

Daftar Pustaka

Badan Siber dan Sandi Negara. 2025. Laporan Kinerja BSSN 2024. Jakarta: BSSN.

E-Governance Academy Foundation. 2025. National Cyber Security Index. Diakses dari https://ncsi.ega.ee/country/id_2022/?allData=1, pada 4 Agustus 2025.

Haryanto, A.T. 2024. APJII: Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. Diakses dari https://inet.detik.com/cyberlife/d-7169749/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang, pada 5 Agustus 2025.

Kementerian Komunikasi dan Digital. 2025. Transformasi Digital Bersama Kementerian Komdigi. Diakses dari https://www.komdigi.go.id/transformasi-digital, pada 5 Agustus 2025.

Nurhidayat., et.al. 2024. Kajian Ketahanan Siber: Manajamen Kerentanan. Bogor: Politeknik Siber dan Sandi Negara.

Nugraha, A. 2025. Kesiapan Keamanan Siber Indonesia Masih Rendah. Diakses dari https://csirt.hulusungaiselatankab.go.id/posts/kesiapan-keamanan-siber-indonesia-masih-rendah, pada 6 Agustus 2025.

OECD. 2022. OECD Policy Framework on Digital Security. Paris: OECD.

Salwa, N.D.K. 2024. Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia. Diakses dari https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn, pada 5 Agustus 2025.

Susapto, L.W. 2024. BSSN Ungkap Indonesia Kekurangan SDM Keamanan Siber. Diakses dari https://validnews.id/nasional/bssn-ungkap-indonesia-kekurangan-sdm-keamanan-siber, pada 6 Agustus 2025.

Vincha, C., & Satrio, J. 2024. Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber Indonesia. Jurnal Ketahanan Nasional. Vol. 30, No. 2, 222-242.

World Economic Forum. 2023. Global Risks Report 2023. Geneva: World Economic Forum.

Pengarah

Plt. Kepala Badan Keahlian DPR

Dr. Lidya Suryani Widayati, S.H., M.H.

Penanggung Jawab

Kepala Pusat Analis Anggaran dan Akuntabilitas Keuangan Negara

Dr. Furcony Putri Syakura, S.H., M.H., M.Kn., QGIA, QHIA., QIA, PQIA

Penulis

Robby Alexander Sirait, S.E., M.E., C.L.D

Leo Iskandar, S.E., M.Sc.

Analisis PAGU ANGGARAN 2025

BADAN KEAHLIAN DPR RI

PUSAT ANALISIS ANGGARAN DAN AKUNTABILITAS KEUANGAN NEGARA

BADAN KEAHLIAN, SEKRETARIAT JENDERAL DPR RI

Gedung Sekretariat Jenderal DPR RI Lantai 6
Jl. Jend. Gatot Subroto, Senayan, Jakarta Pusat 10270
www.bk.dpr.go.id