PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2025
TENTANG
RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2025-2029

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 19 ayat (2) Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional, Pasal 17 ayat (3) Peraturan Pemerintah Nomor 40 Tahun 2006 tentang Tata Cara Penyusunan Rencana Pembangunan Nasional, dan ketentuan Pasal 19 ayat (1) Peraturan Presiden Nomor 80 Tahun 2025 tentang Penyusunan Rencana Strategis dan Rencana Kerja Kementerian/Lembaga, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2025-2029;

Mengingat : 1. Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 104, Tambahan Lembaran Negara Republik Indonesia Nomor 4421);
2. Undang-Undang Nomor 59 Tahun 2024 tentang Rencana Pembangunan Jangka Panjang Nasional Tahun 2025-2045 (lembaran Negara Republik Indonesia Tahun 2024 Nomor 194, Tambahan Iembaran Negara Republik Indonesia Nomor 6987);
3. Peraturan Pemerintah Nomor 40 Tahun 2006 tentang Tata Cara Penyusunan Rencana Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 97, Tambahan Lembaran Negara Republik Indonesia Nomor 4664);

4. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
5. Peraturan Presiden Nomor 12 Tahun 2025 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2025-2029 (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 19);
6. Peraturan Presiden Nomor 80 Tahun 2025 tentang Penyusunan Rencana Strategis dan Rencana Kerja Kementerian/Lembaga (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 114);
7. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2025-2029.

Pasal 1

Rencana Strategis Badan Siber dan Sandi Negara Tahun 2025-2029 yang selanjutnya disebut Renstra BSSN merupakan dokumen perencanaan Badan Siber dan Sandi Negara untuk periode 5 (lima) tahun terhitung sejak tahun 2025 sampai dengan tahun 2029.

Pasal 2

(1) Renstra BSSN sebagaimana dimaksud dalam Pasal 1 memuat:
    a. visi, misi, tujuan, dan sasaran strategis;
    b. arah kebijakan, strategi, kerangka regulasi, dan kerangka kelembagaan; dan
    c. target kinerja dan kerangka pendanaan.
(2) Ketentuan mengenai Renstra BSSN sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 3

Data dan informasi kinerja Renstra BSSN yang termuat dalam sistem informasi KRISNA-RENSTRAKL merupakan bagian yang tidak terpisahkan dari dokumen Renstra BSSN sebagaimana dimaksud dalam Pasal 2.

Pasal 4

Pada saat Peraturan Badan ini mulai berlaku, Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 (Berita Negara Republik Indonesia Tahun 2020 Nomor 843) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2021 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 (Berita Negara Republik Indonesia Tahun 2021 Nomor 1461), dicabut dan dinyatakan tidak berlaku.

Pasal 5

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Badan ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 8 Oktober 2025

KEPALA BADAN SIBER DAN SANDI NEGARA,

Ditandatangani secara elektronik oleh:
Kepala Badan Siber dan Sandi Negara

Drs. NUGROHO SULISTYO BUDI, M.M., M.Han.
Letnan Jenderal TNI (Purn)

NUGROHO S. BUDI

Diundangkan di Jakarta
pada tanggal 5 November 2025

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2025 NOMOR 908

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2025
TENTANG
RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2025-2029

RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2025-2029

BAB I
PENDAHULUAN

1.1 Kondisi Umum

Penetrasi pengguna internet di Indonesia terus mengalami peningkatan dalam rentang waktu 5 (lima) tahun terakhir (Survei Penetrasi Internet APJII 2024). Hingga tahun 2024, tingkat penetrasi internet di Indonesia mencapai angka 79,50% dengan total penduduk terkoneksi internet per tahun 2024 sebesar 221.563.489 jiwa. Rata-rata penetrasi internet bertumbuh di angka 5,36% dari tahun 2018 – 2024. Penetrasi internet yang masif memberikan dampak positif berupa efisiensi waktu yang sangat terbantu dengan teknologi. Disisi lain, adanya ancaman mengenai keamanan dalam penggunaan internet yang juga menjadi perhatian di tingkat nasional.

Sejalan dengan pemanfaatan digital di tingkat individu, era Revolusi Industri 5.0 dan Society 5.0 ditandai dengan integrasi mendalam antara *machine learning* dan kecerdasan artifisial dalam kehidupan sehari-hari. Konektivitas antar komputer tidak hanya mentransformasi peran manusia dalam operasional manufaktur dan pengambilan keputusan, tetapi juga menciptakan ekosistem kolaboratif di mana teknologi menjadi mitra yang memperkuat kapabilitas manusia. Konektivitas yang menjadi kunci

interaksi ini dimungkinkan oleh perkembangan internet dan TIK yang semakin canggih.

Konektivitas antar individu maupun antar organisasi menciptakan ruang siber yang di dalamnya mencakup interaksi masif. Interaksi tersebut terdiri dari interaksi sosial oleh masing-masing individu, interaksi bisnis dari para pelaku usaha hingga interaksi dari penyelenggara pemerintahan. Gangguan terhadap ruang siber terhadap salah satu pengguna ruang siber dapat berdampak langsung terhadap stabilitas sebuah negara, baik dampak minor maupun mayor.

Berdasarkan National Institute and Standard Technology (NIST), ruang siber diartikan sebagai domain global dalam lingkungan informasi yang terdiri dari jaringan infrastruktur sistem informasi yang saling bergantung, termasuk internet, jaringan telekomunikasi, dan komputer. Peningkatan interaksi menarik atensi dari pihak-pihak tidak bertanggung jawab yang memanfaatkan celah keamanan untuk memperoleh keuntungan individu maupun kelompok. Celah yang dimaksud direpresentasikan dengan peningkatan *cybercrime, cyber-attack, cyber espionage* dan bahkan dapat terjadi hingga adanya operasi serangan yang akan mengancam pertahanan suatu negara *(cyber warfare).* Dalam beberapa tahun terakhir, masifnya serangan siber di tingkat nasional telah menyebabkan kerugian baik secara *tangible* hingga *intangible*. Kerugian *tangible* yang dimaksud adalah dampak ekonomi yang ditimbulkan karena efek serangan siber. Kerugian *intangible* yang dimaksud adalah menurunnya kepercayaan masyarakat terhadap inisiatif pemerintah di bidang siber, khususnya bidang keamanan siber.

Antisipasi berupa proteksi terhadap ruang siber sepatutnya menjadi perhatian dan atensi nasional saat ini. Badan Siber dan Sandi Negara (BSSN) merupakan Lembaga Pemerintah Non-Kementerian (LPNK) yang diberi mandat untuk menjaga keamanan ruang siber nasional. Tantangan

berat menanti BSSN dalam beberapa tahun ke depan dengan tren ancaman dan serangan siber yang belum menunjukkan penurunan, sebaliknya semakin variatif. Perencanaan yang efektif dan efisien dibutuhkan untuk mengantisipasi tantangan dengan melibatkan berbagai pemangku kepentingan sebagai bagian integral dalam menjaga ruang siber nasional.

Gangguan keamanan siber yang menjadi atensi nasional terjadi dalam beberapa tahun terakhir. *Ransomware Lockbit 3.0* menyerang sistem elektronik Bank Syariah Indonesia (BSI) pada tahun 2023 yang menyebabkan nasabah tidak dapat mengakses sistem elektronik perbankan BSI. Serangan *Ransomware* juga menyerang Pusat Data Nasional Sementara (PDNS) pada tahun 2024 ini yang menyebabkan beberapa layanan pemerintah terganggu, salah satunya adalah antrean panjang dalam layanan keimigrasian di Bandara. Hal ini tentunya sangat mempengaruhi citra Indonesia, baik di dalam negeri maupun di luar negeri. Tren serangan ini akan terus meningkat dalam beberapa tahun ke depan, baik serangan siber secara global maupun serangan siber di Indonesia.

Cybersecurity Ventures melaporkan bahwa terdapat 10 prediksi yang kemungkinan akan terjadi pada keamanan siber global, yaitu:

1. Kerugian akibat kejahatan dunia maya global diperkirakan mencapai US$10,5 triliun setiap tahunnya pada tahun 2025.

   Cybersecurity Ventures memperkirakan gangguan keamanan siber yang terjadi dapat menimbulkan kerugian hingga mencapai US$10,5 triliun setiap tahunnya pada tahun 2025. Potensi kerugian ini merupakan transfer kekayaan ekonomi terbesar dalam sejarah, mempertaruhkan insentif untuk inovasi dan investasi, dan secara eksponensial lebih besar daripada kerusakan yang disebabkan oleh bencana alam dalam setahun. Hal ini tentu perlu menjadi perhatian serius pemerintah, khususnya pemerintah Republik Indonesia, untuk meminimalisasi risiko kerugian akibat serangan siber yang berpotensi akan terjadi.

2. Belanja keamanan siber global akan melebihi US$1,75 triliun secara kumulatif dari tahun 2021-2025.

   Cybersecurity Ventures memproyeksikan biaya yang dibutuhkan dalam melindungi bisnis digital, peralatan *Internet of Things* (IoT) serta konsumen dari gangguan keamanan siber adalah sebesar US$1,75 triliun secara kumulatif dari tahun 2021-2025. Hal ini menjadi peluang pertumbuhan industri keamanan siber selama tahun 2021-2025.

3. Dunia akan memiliki 3,5 juta pekerjaan keamanan siber yang belum terisi pada tahun 2024.

   Cybersecurity Ventures memperkirakan akan ada 3,5 juta pekerjaan keamanan siber yang belum terisi pada tahun 2024. Hal ini tentunya menjadi peluang bagi BSSN untuk membentuk SDM keamanan siber nasional melalui kolaborasi dengan pemangku kepentingan terkait sehingga dapat mengisi kekosongan pekerjaan keamanan siber yang dibutuhkan tersebut.

4. Biaya kerusakan akibat *ransomware* global diperkirakan melebihi US$265 miliar pada tahun 2031.

   Menurut Cybersecurity Ventures, kerugian akibat *ransomware* global diperkirakan mencapai $20 miliar per tahun pada tahun 2021, naik dari $325 juta pada tahun 2015, yang merupakan peningkatan 57 kali lipat. Dalam delapan tahun dari sekarang, kerugiannya akan melebihi $265 miliar. Cybersecurity Ventures juga memperkirakan bahwa sebuah bisnis menjadi korban serangan *ransomware* setiap 11 detik pada tahun 2021, naik dari setiap 14 detik pada tahun 2019. Hal ini menjadikan *ransomware* sebagai jenis kejahatan dunia maya yang paling cepat berkembang. Frekuensi serangan *ransomware* pada pemerintah, bisnis, konsumen, dan perangkat akan terus meningkat selama 8 tahun ke depan dan mencapai setiap dua detik pada tahun 2031.

5. Dunia perlu melindungi 200 zettabyte data pada tahun 2025.

Total penyimpanan data global diproyeksikan akan melampaui 200 zettabyte pada tahun 2025. Ini termasuk data yang disimpan pada infrastruktur TI publik dan privat, pada infrastruktur utilitas, pada pusat data *cloud* publik dan privat, pada perangkat komputasi personal — PC, laptop, tablet, dan ponsel pintar — dan pada perangkat IoT (*Internet-of-Things*). Cybersecurity Ventures memperkirakan bahwa jumlah total data yang disimpan di *cloud* — yang mencakup *cloud* publik yang dioperasikan oleh vendor dan perusahaan media sosial (seperti Apple, Facebook, Google, Microsoft, Twitter, dll.), *cloud* milik pemerintah yang dapat diakses oleh warga negara dan bisnis, *cloud* privat yang dimiliki oleh perusahaan menengah hingga besar, dan penyedia penyimpanan *cloud* — akan mencapai 100 zettabyte pada tahun 2025, atau 50 persen dari data dunia pada saat itu, naik dari sekitar 25 persen yang disimpan di *cloud* pada tahun 2015. Peningkatan data yang tersimpan secara digital ini tentunya akan meningkatkan kebutuhan perlindungan dari berbagai gangguan keamanan siber di masa depan.

6. Pasar asuransi siber diprediksi mencapai US$14,8 miliar setiap tahunnya pada tahun 2025.

   Meningkatnya kebutuhan keamanan siber kedepan diiringi dengan potensi peningkatan serangan siber akan membuka peluang dalam permintaan jaminan asuransi keamanan siber. Cybersecurity Ventures memperkirakan pasar asuransi siber akan tumbuh dari sekitar US$8,5 miliar pada tahun 2021 menjadi US$14,8 miliar pada tahun 2025, dan melampaui US$34 miliar pada tahun 2031, berdasarkan *Compound Annual Growth Rate* (CAGR) sebesar 15 persen selama periode 11 tahun (2020 hingga 2031) yang dihitung.

7. Kejahatan mata uang kripto diprediksi akan merugikan dunia US$30 miliar setiap tahunnya pada tahun 2025.

   Pertumbuhan pesat dalam penggunaan layanan keuangan terdesentralisasi (*Decentralized Finance - DeFi*) menciptakan titik lemah

baru bagi sistem keuangan global, mendorong metode baru kejahatan kripto bagi penjahat dunia maya yang menurut prediksi Cybersecurity Ventures akan merugikan dunia sebesar US$30 miliar pada tahun 2025.Jumlah tersebut hampir dua kali lipat dari kerugian sebesar US$17,5 miliar pada tahun 2021 dan diperkirakan akan tumbuh sebesar 15 persen setiap tahunnya seiring pasar mata uang kripto terus berkembang dan akan memicu meningkatnya minat penjahat dunia maya untuk mencuri toko mata uang kripto. Perhatian penjahat dunia maya terhadap kripto terwujud dalam berbagai cara, termasuk peretasan bursa langsung dan penipuan yang dirancang untuk mengelabui orang agar menyerahkan kepemilikan mata uang kripto mereka untuk sejumlah tujuan palsu.

8. Perempuan diprediksi akan memegang 30 persen posisi keamanan siber secara global pada tahun 2025.

   Perkembangan keamanan siber global juga menimbulkan peluang pekerjaan khususnya bagi kaum perempuan. Cybersecurity Ventures memperkirakan perempuan akan memegang 30 persen posisi keamanan siber secara global pada tahun 2025. Prediksi ini melampaui pengamanan jaringan perusahaan dan mencakup keamanan IoT(*Internet of Things*), IIoT (*Industrial Internet of Things*), dan ICS (*Industrial Control Systems*), serta keamanan siber untuk medis, otomotif, penerbangan, pertahanan militer, dan lainnya.

9. 90 persen populasi manusia, berusia 6 tahun ke atas, akan terhubung dengan internet pada tahun 2030.

   Cybersecurity Ventures memprediksi sekitar satu juta orang lebih bergabung dengan internet setiap harinya. Ada sekitar 6 miliar orang yang terhubung ke internet dan berinteraksi dengan data pada tahun 2022, naik dari 5 miliar pada tahun 2020 — dan Cybersecurity Ventures memperkirakan akan ada lebih dari 7,5 miliar pengguna internet pada tahun 2030. Jika kejahatan jalanan meningkat seiring dengan

pertumbuhan populasi, maka kejahatan dunia maya juga akan meningkat.

Berdasarkan data yang dirilis APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), pada tahun 2024 pengguna internet di Indonesia telah mencapai 221,56 juta orang atau sebesar 79,5% dari total populasi 278,7 juta jiwa penduduk Indonesia tahun 2023. Jumlah tersebut mengalami peningkatan sebesar 2,8% dibandingkan periode sebelumnya yang sebanyak 215,63 juta pengguna. Peningkatan ini menandakan konsistensi grafik tren positif penetrasi internet Indonesia dalam lima tahun terakhir yang terus naik secara signifikan.

Penetrasi terbesar terjadi saat pandemi Covid-19, di mana di mana pembatasan aktivitas diberlakukan secara masif dan aktivitas dilakukan dalam jaringan (daring).

10. Dunia perlu mengamankan 338 miliar baris kode perangkat lunak baru pada tahun 2025.

    Cybersecurity Ventures memperkirakan dunia perlu mengamankan 338 miliar baris kode perangkat lunak baru pada tahun 2025, naik dari 111 miliar baris kode baru pada tahun 2017, berdasarkan pertumbuhan kode baru sebesar 15 persen dari tahun ke tahun. Statistik yang jarang diketahui ini telah menjadi salah satu yang paling penting bagi para profesional keamanan siber tingkat eksekutif untuk diperhatikan selama 5 tahun terakhir. Hal ini menunjukkan bahwa keamanan aplikasi menjadi salah satu hal penting yang perlu dilakukan dalam menjaga keamanan ruang siber maupun keamanan informasi.

    Keamanan siber dan sandi menjadi komponen penting dalam mewujudkan Indonesia Emas tahun 2045 melalui terwujudnya Visi Indonesia Digital (VID) tahun 2045. Keamanan siber dan sandi menjadi fondasi penting baik dalam mewujudkan pemerintah digital, masyarakat digital maupun ekonomi digital. Selain itu, Peraturan

Presiden nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) menjadi payung hukum yang kuat bagi terwujudnya pemerintah digital, di mana keamanan siber dan persandian menjadi hal krusial dalam pelaksanaan SPBE tersebut.

BSSN diberi mandat untuk menjaga keamanan ruang siber serta penerapan teknologi keamanan siber dan sandi dalam menjaga keamanan informasi nasional.

Peningkatan tren gangguan keamanan siber maupun penerapan kriptografi nasional yang menyerang Infrastruktur Informasi Kritis (IIV) maupun layanan publik menjadi tantangan tersendiri bagi BSSN untuk dapat mengatasinya. Untuk itu, BSSN telah menyusun Peraturan BSSN Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi Indonesia dan Penilaian Kesesuaian Keamanan Modul Kriptografi (PAKI dan PKKMK) yang telah diundangkan sejak 19 November 2024, sebagai salah satu penguatan peran BSSN yang sangat penting. Namun penguatan peran BSSN lainnya bidang kriptografi khususnya pada sektor pertahanan, keamanan, dan diplomasi masih perlu dilakukan agar keamanan ruang siber nasional dapat lebih terjamin dalam mewujudkan Visi Indonesia Digital 2045.

Untuk itu, maka dibutuhkan Rencana Strategis BSSN tahun 2025-2029 yang selaras dengan RPJMN 2025-2029 yang penyusunannya sesuai ketentuan pada Peraturan Menteri Perencanaan Pembangunan Nasional (Permen PPN) Nomor 10 Tahun 2023 tentang Tata Cara Penyusunan Rencana Strategis Kementerian/Lembaga 2025-2029 serta Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Permen PANRB) Nomor 89 Tahun 2021 tentang Penjenjangan Kinerja Instansi Pemerintah.

1.1.1 Capaian Renstra BSSN Periode 2020 – 2024

Capaian Rencana Strategis (Renstra) BSSN merupakan kinerja yang didapatkan berdasarkan perhitungan dari indikator kinerja yang telah disepakati pada periode 2020 – 2024. Capaian Renstra BSSN merupakan tolok ukur kinerja BSSN yang dapat menjadi *input* dalam perencanaan ke depan. Analisis terhadap capaian Renstra 2020 – 2024 untuk melihat sejauh mana perkembangan kinerja dan melihat upaya yang sudah dilakukan BSSN dalam perwujudan visi BSSN pada periode Renstra sebelumnya.

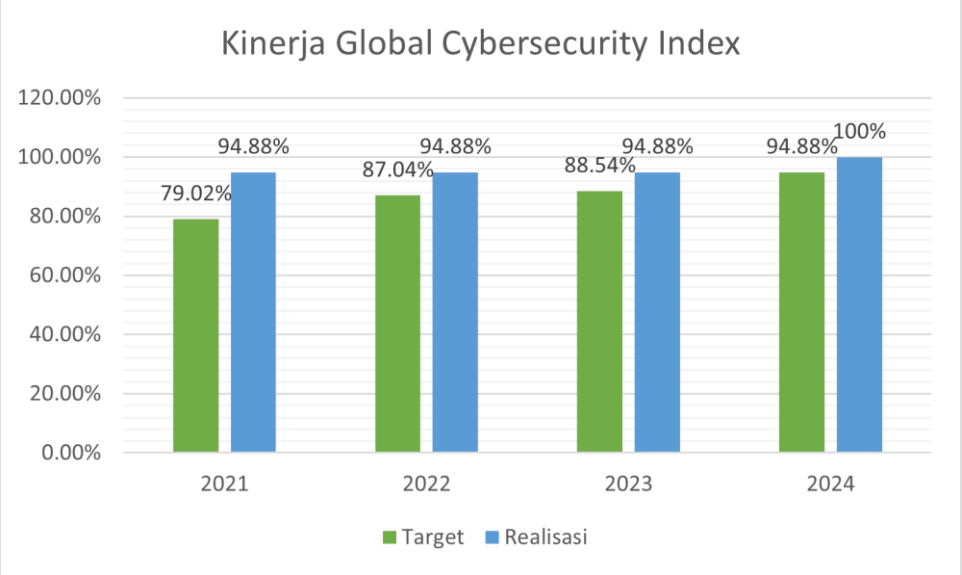
Pada periode 2020-2024, dilakukan penyesuaian terhadap Renstra BSSN 2020-2024 sebagai tindaklanjut perubahan organisasi dan tata kerja BSSN guna penguatan tugas dan fungsi dalam mencapai tujuan yang ditetapkan. Penyesuaian Renstra dimaksud dilakukan terhadap indikator kinerja sasaran strategis, sasaran program, dan sasaran kegiatan. Pada penyesuaian Renstra BSSN 2021-2024, BSSN memiliki 2 tujuan strategis yaitu (1) Terwujudnya kedaulatan keamanan siber Indonesia dan (2) Terwujudnya tata kelola pemerintahan yang baik. Kedua tujuan tersebut kemudian dijabarkan ke dalam 3 (tiga) Sasaran Strategis BSSN.

Dalam rangka penguatan akuntabilitas kinerja BSSN yang berpedoman pada Peraturan BSSN Nomor 14 Tahun 2019 tentang Pengelolaan Kinerja di BSSN, tujuan dan sasaran strategis tersebut selanjutnya dijabarkan ke dalam sejumlah sasaran strategis pada Peta Strategi BSSN 2021-2024. Lebih rinci mengenai capaian sasaran strategis BSSN dapat dilihat sebagai berikut.

Sasaran Strategis 1: Meningkatnya Keamanan Siber Indonesia

Sasaran pertama terkait peningkatan keamanan siber Indonesia diukur dengan indikator *Global Cybersecurity Index* (GCI). Indeks tersebut merepresentasikan komitmen Indonesia terhadap keamanan siber di

tingkat global. Penilaian dilakukan berdasarkan 5 (lima) pilar, yaitu *legal measures, technical measures, organizational measures, capacity development measures* dan *cooperation measures*. Kinerja GCI Indonesia dapat dilihat pada gambar berikut.



Gambar 1.1. Target dan Realisasi GCI

Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja GCI dapat dikatakan baik karena seluruh target capaian kinerja terwujud. Capaian kinerja tersebut tidak lepas dari beberapa upaya yang dilakukan BSSN sebagai berikut.

Tabel 1.1. Upaya Yang Dilakukan Untuk Mendukung Capaian GCI

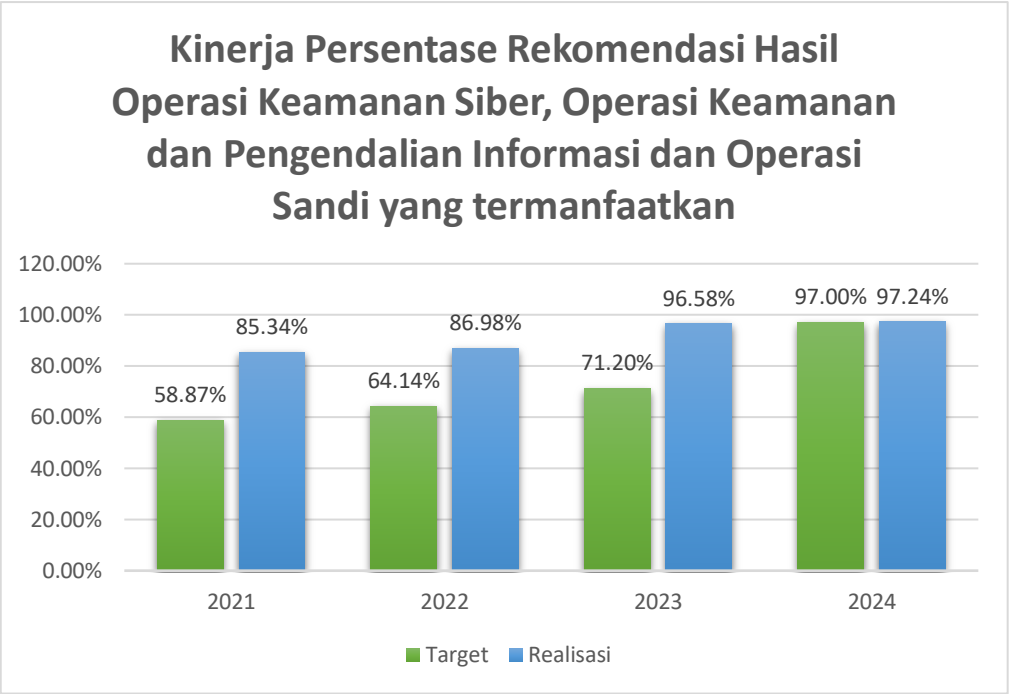
UPAYA YANG DILAKUKAN
2020
1. Menyusun indeks keamanan siber. 2. Penyusunan Strategi Keamanan Siber Nasional (SKSN). 3. Peningkatan Kerja Sama dan Kemitraan *(Bilateral* dan Forum). 4. Pembentukan CSIRT Instansi Pemerintah. 5. Registrasi CSIRT Sektoral oleh BSSN.
2021
1. Penyusunan RPerpres tentang Strategi Keamanan Siber Nasional (SKSN) dan RPerpres tentang Pelindungan Infrastruktur Informasi Vital (IIV).

UPAYA YANG DILAKUKAN
2. Peningkatan Kerja sama dan kemitraan dalam konteks *Conference Bulding Measures* (Bilateral, Regional, Multilateral Forum). 3. Kerja sama dengan Sektor Publik dan Privat. 4. Literasi kesadaran keamanan siber dalam rangka perlindungan anak di ruang siber. 5. Pembentukan Indonesia Women in Cyber Security (IWCS). 6. Pelaksanaan *cyber drill test*. 7. Pembentukan CSIRT Instansi Pemerintah. 8. Registrasi CSIRT Sektoral oleh BSSN.
2022
1. Terlibat dalam *workshop*/rapat Internasional Telecommunication Union (ITU) menghasilkan Resolusi 50 (*cybersecurity*) dan penunjukan *focal point* GCI (ITU). 2. Terlibat dalam kegiatan Tim *Expert* Group GCI menghasilkan penentuan *tools* GCIv5 (mengukur GCI 2023); Rekomendasi pembobotan survei GCIv5; Penentuan 3 *tier* model untuk GCIv5. 3. Terlibat dalam penyusunan peraturan keamanan siber: Rekomendasi UU 27/2022; menyusun Perpres 82/2022; dan menyusun draf RPerpres tentang SKSN.
2023
1. Penetapan 4 Peraturan BSSN yang merupakan turunan dari Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, yaitu : (1) Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi IIV, (2) Peraturan BSSN Nomor 8 Tahun 2023 tentang Kerangka Kerja IIV, (3) Peraturan BSSN Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas SDM Bidang Keamanan Siber dan Sandi, (4) Peraturan BSSN Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber. *2.* Pengembangan Kapasitas Keamanan Siber dan Sandi pada *stakeholder* 3. Pengelolaan National CSIRT, 4. Monitoring isu kekerasan anak pada *darknet* dan diseminasi kepada KemenPPPA terkait identifikasi ancaman *child abuse* pada *darknet*.
2024
1. Menetapkan Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber. 2. Menetapkan Peraturan BSSN Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber dan Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber. 3. Mengelola *National Computer Security Incident Response Team* (Nat-CSIRT). 4. Mengelola *Government Computer Security Incident Response Team* (Gov-CSIRT). 5. Melakukan monitoring isu kekerasan anak pada *darknet* dan melakukan diseminasi terkait identifikasi ancaman *child abuse* pada *darknet* di Indonesia. 6. Melaksanakan kegiatan literasi dalam rangka peningkatan budaya keamanan siber dan keamanan informasi. 7. Menyelenggarakan forum tingkat tinggi. 8. Mendorong pembentukan CSIRT Organisasi dan CSIRT Sektoral.

UPAYA YANG DILAKUKAN
9. Melaksanakan pengukuran kematangan keamanan siber dan penyusunan profil risiko pada sektor pemerintahan, sektor pembangunan manusia dan sektor perekonomian. 10. Memberikan pembinaan terhadap *stakeholder* pada setiap sektor melalui program *workshop*, audiensi, maupun bimbingan teknis. 11. Melakukan kerja sama dan kolaborasi terkait keamanan siber dengan stakeholder maupun komunitas. 12. Melakukan kerja sama bilateral dengan berbagai negara dan berperan aktif dalam berbagai forum internasional.

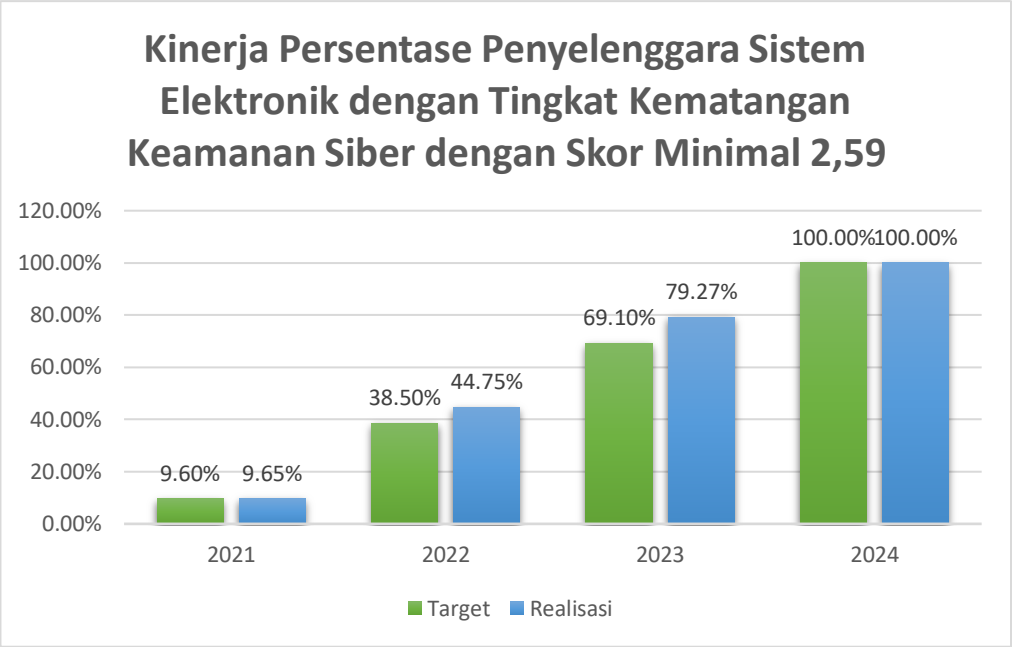
Sasaran Strategis 2: Meningkatnya Kapasitas Keamanan Siber dan Sandi

Sasaran kedua terkait peningkatan kapasitas keamanan siber dan sandi yang diukur dengan 2 (dua) indikator. Indikator pertama terkait persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan. Indikator kedua yaitu persentase penyelenggara sistem elektronik (PSE) dengan tingkat kematangan keamanan siber pada skor 2,59. Indikator tersebut merepresentasikan penyajian hasil analisis kepada pemangku kepentingan untuk merespons permasalahan sesuai dengan tugas dan fungsi BSSN terkait penyelenggaraan operasi keamanan siber dan sandi. Kinerja pemanfaatan rekomendasi dapat dilihat pada gambar berikut.



Gambar 1.2. Target dan Realisasi Pemanfaatan Rekomendasi

Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja pemanfaatan rekomendasi secara keseluruhan dapat dikatakan sangat baik karena selama 4 (empat) tahun berturut-turut capaian kinerja terwujud. Analisis terkait indikator kedua yaitu Persentase Penyelenggara Sistem Elektronik (PSE) dengan tingkat kematangan keamanan siber dengan skor minimal 2,59. Indikator ini pelaksanaan amanat Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). BSSN melakukan pembinaan kepada PSE sesuai tugas dan fungsi BSSN dalam mengkoordinasikan keamanan siber. Kinerja terkait pembinaan dapat dilihat pada gambar berikut.



Gambar 1.3. Target dan Realisasi Terkait Pembinaan PSE

Gambar di atas menunjukkan capaian kinerja pembinaan BSSN dalam meningkatkan maturitas Penyelenggaraan Sistem Elektronik (PSE) dengan skor minimal 2,59 selama periode 2021-2024. Dapat disimpulkan bahwa capaian kinerja pembinaan sangat memuaskan, ditandai dengan realisasi yang konsisten melebihi target setiap tahunnya. Terjadi peningkatan signifikan baik pada target maupun realisasi dari tahun ke tahun, dengan pencapaian paling mencolok pada 2023 di mana realisasi mencapai 79,27% melampaui target 69,10%. Keberhasilan program ini mencapai puncaknya pada tahun 2024 dengan tercapainya target dan realisasi 100%. Capaian kinerja tersebut tidak lepas dari beberapa upaya yang dilakukan BSSN sebagai berikut.

Tabel 1.2. Upaya Yang Dilakukan Terkait Pembinaan PSE

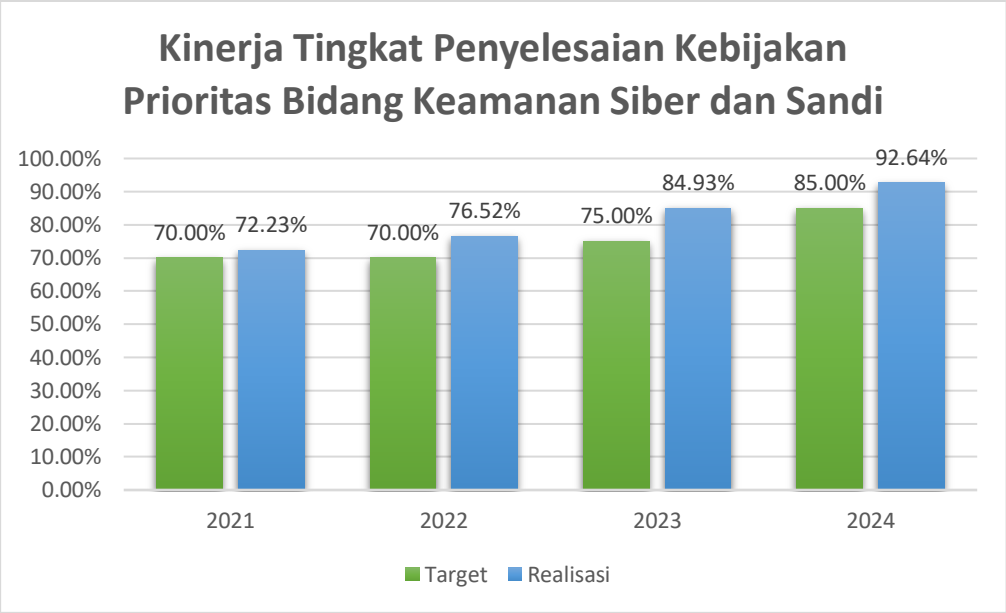
UPAYA YANG DILAKUKAN
Kinerja persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan
2021
1. Penyelenggaraan kegiatan respons JKSN dan Rakor JKSN sehingga terjadi kolaborasi dan sinergi antara BSSN dengan *stakeholders* dalam peningkatan peran persandian untuk pengamanan komunikasi. 2. Penyelenggaraan operasi deteksi sinyal yang berperan dalam pengambilan keputusan strategis *stakeholders* terkait wilayah operasi BDS Batam.
2022
1. Pemberian Layanan Sistem Penanganan Perkara Pidana Terpadu berbasis Teknologi Informasi (SPPT-TI) kepada *stakeholders*. 2. Pemberian layanan pengamanan TIK dalam proses pengadaan Calon Aparatur Sipil Negara (CASN) dengan memperhatikan prinsip-prinsip *Confidentiality, Scalability, Availability* dan *Non-Repudiation.* 3. Penyelenggaraan kegiatan Respons Jaring Komunikasi Sandi Nasional (JKSN). 4. Pembentukan *team helpdesk* yang bertugas 7x24 jam untuk menangani permasalahan penggunaan email sanapati dan beberapa aplikasi yang ter-*install* di server C3.
2023
1. Penyusunan dan penyampaian Laporan Analisis dan Rekomendasi kepada *stakeholder* yang disusun berdasarkan hasil monitoring tim pengendalian informasi, aduan masyarakat/publik dalam hal ini dari sektor publik dan sektor privat yang melaporkan aduan pada *email* bantuan70@bssn.go.id, serta memperhatikan arahan pimpinan. *2.* Peningkatan pemenuhan layanan implementasi Modul Kriptografi seiring dengan meningkatnya kesadaran keamanan informasi bagi ASN maupun masyarakat umum karena banyaknya serangan siber yang dapat menyebabkan *data breach.* 3. Pemenuhan Layanan Kontra Pengindraan sebagai upaya peningkatan keamanan informasi yang mendukung kegiatan pengamanan yang bersifat strategis baik pemantauan rutin berkala ataupun kegiatan yang bersifat insidental. 4. Pemenuhan kebutuhan keamanan informasi yang tinggi untuk memenuhi prinsip *Confidentiality, Scalability, Availability* dan *Non-Repudiation* pada kegiatan Seleksi Pengadaan CASN. 5. Pemanfaatan persandian untuk pengamanan komunikasi, seperti penggunaan email sanapati untuk kirim terima berita berklasifikasi. 6. Pembentukan tim *helpdesk monitoring Communication and Command Center* (C3) yang bertugas 7x24 jam dan Tim Respons Jaring Komunikasi Sandi Nasional (JKSN) untuk menangani permasalahan penggunaan email sanapati dan beberapa aplikasi yang ter-*install* di server C3. 7. Melakukan kegiatan operasi deteksi sinyal oleh Balai Deteksi Sinyal dalam rangka pembebasan Pilot Susi Air yang disandera oleh Tentara Pembebasan Nasional Papua Barat- Organisasi Papua Merdeka (TPNPB-OPM).

UPAYA YANG DILAKUKAN
2024
1. Adanya dukungan dan komitmen kuat dari pimpinan dalam memastikan setiap operasi berjalan dengan optimal. 2. Adanya kompetensi SDM yang mumpuni dalam bidang operasi keamanan siber dan sandi; 3. Penggunaan sistem deteksi konten yang mempermudah pengguna dalam mendeteksi ancaman siber sosial maupun konten negatif sehingga dapat segera dilaporkan dan ditindaklanjuti. 4. Adanya pemantauan dan evaluasi berkala selama tahun 2024 untuk memastikan rekomendasi yang dihasilkan dapat bermanfaat bagi *stakeholder*. 5. Penggunaan survei *online* yang mempermudah pengumpulan data dari *stakeholder* yang tersebar luas. 6. Adanya kolaborasi dan sinergi yang baik di lingkungan internal dan eksternal BSSN, baik antar individu, tim kerja, maupun dengan pihak *stakeholder*.
Persentase Penyelenggara Sistem Elektronik (PSE) dengan tingkat kematangan keamanan siber dengan skor minimal 2,59
2021
1. Melakukan penjajakan kerja sama terkait upaya peningkatan keamanan siber. 2. Melakukan diseminasi informasi untuk meningkatkan pemahaman mengenai urgensi keamanan siber di level Pimpinan PSE. 3. Memberikan asistensi penerapan keamanan siber. 4. Mengadakan seminar, *webinar*, *workshop* dan diskusi tentang *cyber security awareness*.
2022
1. Melakukan pembinaan dan pelayanan keamanan siber dan sandi: asistensi, konsultasi, bimbingan teknis, sosialisasi dan diskusi aktif dengan *stakeholder* terkait pentingnya proteksi keamanan siber. 2. Memberikan saran dan rekomendasi penerapan tata kelola, rencana implementasi aplikasi/ sistem, program peningkatan kompetensi personel terkait proteksi keamanan siber di lingkungan *stakeholders*. 3. Pelaksanaan amanat Perpres Nomor 82/2022 tentang IIV menjadi landasan dalam pengukuran maturitas siber paling sedikit 1 (satu) kali dalam 1 (satu) tahun. 4. Melakukan pendekatan personal kepada *top level management* para *stakeholders* agar berkomitmen dan memberi dukungan terhadap program keamanan siber dan lingkungannya.
2023
1. Menyelenggarakan Bimtek Pengukuran Tingkat Kematangan Keamanan Siber pada tanggal 5- 6 Juli 2023 bersama dengan Kemenkes sebagai bentuk kolaborasi untuk memenuhi mandat Perpres Nomor 28 Tahun 2022 tentang Perlindungan IIV khususnya Pengukuran Tingkat Kematangan Siber.

UPAYA YANG DILAKUKAN
2. Menyelenggarakan *Workshop* Manajemen Risiko *Cyber Security Maturity* Sektor Industri yang dilaksanakan pada tanggal 13 Maret 2023. 3. Menyelenggarakan *Workshop* Persiapan Implementasi Tata Kelola Keamanan Siber dan Penyusunan Profil Risiko Sektor ESDA pada tanggal 20 - 24 Februari 2023. 4. Melakukan pendampingan kegiatan pengukuran penilaian tingkat kematangan keamanan siber dan sandi sampai dengan verifikasi hasil pengukuran serta pemberian rekomendasi berdasarkan hasil verifikasi.
2024
1. Penilaian kematangan keamanan siber dilakukan dengan beberapa tahapan, meliputi sosialisasi dan bimbingan teknis pengisian instrumen, verifikasi hasil pengukuran dan penyampaian rekomendasi hasil verifikasi. 2. Terjalinnya kerja sama yang baik antara BSSN dengan *stakeholder* terkait. 3. Telah terbentuknya *security awareness* yang baik di lingkungan *stakeholder*. 4. Melakukan pendekatan personal ke top level manajemen *stakeholder*. 5. Melakukan penjajakan dan diskusi dengan PSE untuk mendapatkan informasi atau kebutuhan PSE dalam peningkatan kapasitas keamanan siber. 6. Melakukan asistensi penerapan keamanan siber sebagai tindak lanjut hasil pengukuran kematangan keamanan siber.

Sasaran Strategis 3: Terwujudnya Kebijakan Keamanan Siber dan Sandi yang Berkualitas

Sasaran ketiga terkait terwujudnya kebijakan keamanan siber dan sandi yang berkualitas dengan indikator Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi. Penyelesaian kebijakan merupakan upaya BSSN untuk menyediakan kebijakan keamanan siber yang menjadi acuan bagi *stakeholders* dalam mengimplementasikan pengelolaan keamanan siber di organisasi maupun sektor di Indonesia. Kinerja terkait tingkat penyelesaian kebijakan dapat dilihat pada gambar berikut.



Gambar 1.4. Target dan Realisasi Kinerja Tingkat Penyelesaian Kebijakan

Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja penyelesaian kebijakan secara keseluruhan dapat dikatakan sangat baik karena selama 4 (empat) tahun berturut-turut capaian kinerja terwujud. Capaian kinerja tersebut tidak lepas dari beberapa upaya yang dilakukan BSSN sebagai berikut.

Tabel 1.3. Upaya yang dilakukan terkait kualitas kebijakan

UPAYA YANG DILAKUKAN
2021
1. Menyusun instrumen penilaian kualitas kebijakan lingkup BSSN (Adopsi konsep LAN). 2. Melakukan *self-assessment* terhadap 5 UKE 1 (4 Deputi dan Sekretariat Utama), Inspektorat, 3 Pusat di bawah Kepala BSSN dan 1 Politeknik. 3. Kesamaan persepsi dari *stakeholders* terhadap urgensi regulasi yang akan dibuat. 4. Melakukan koordinasi dengan *stakeholders* untuk menggali kebutuhan dan harapan *stakeholders* terhadap kebijakan yang akan dibuat. 5. Diskusi dengan pakar untuk memperluas perspektif materi muatan kebijakan dan memberikan solusi efektif dalam menciptakan keharmonisan kebijakan yang akan dibuat. 6. Meningkatkan kompetensi teknis dan manajerial keamanan siber dan sandi, penyusunan kebijakan dan manajemen risiko. 7. Menciptakan komunikasi dan kolaborasi yang baik dengan pihak eksternal yang berwenang dalam proses perumusan dan penetapan kebijakan.

UPAYA YANG DILAKUKAN
2022
1. Kesamaan persepsi dengan Kementerian/Lembaga terhadap urgensi regulasi yang akan dibuat. 2. Kolaborasi dan komunikasi intensif dan efektif dengan seluruh *stakeholders* mempercepat proses penyusunan dan pengesahan regulasi. 3. Telah dilakukan studi dan kajian terhadap *best practice* terkait penerapan peraturan keamanan siber dan sandi. 4. Melakukan peningkatan pemahaman penyusun kebijakan dengan Risk Impact Analysis (RIA) dengan K/L sehingga risiko kebijakan yang disusun dapat diantisipasi sejak dini.
2023
1. Adanya persepsi yang sama dari setiap K/L terhadap urgensi peraturan yang akan dibuat khususnya dalam penyusunan RPP yang memerlukan Panitia Antara K/L sehingga seluruh stakeholder yang terlibat memahami urgensi peraturan tersebut 2. Adanya kolaborasi dan komunikasi yang intens dan efektif dengan seluruh stakeholder sehingga dapat mempercepat proses penyusunan dan pengesahan peraturan. 3. Terlaksananya diskusi dengan para pakar di berbagai bidang untuk memberikan perspektif yang luas terhadap suatu materi muatan kebijakan, dan memberikan solusi efektif dalam menciptakan keharmonisan dalam kebijakan yang dibuat. 4. Telah dilakukannya studi dan kajian terhadap *best practice* penerapan peraturan tentang keamanan siber dan sandi. 5. Terselenggaranya peningkatan kompetensi teknis dan manajerial terkait keamanan siber dan sandi, penyusunan kebijakan, dan manajemen risiko untuk meningkatkan wawasan dan kompetensi dalam menyusun substansi kebijakan
2024
1. Adanya Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028 yang mengamanatkan perumusan kebijakan keamanan siber. 2. Proses penyusunan kebijakan yang terstruktur mulai dari penyusunan, pengajuan tanggapan hukum hingga pengesahan kebijakan; 3. Kesamaan persepsi dari setiap Kementerian atau Lembaga terhadap urgensi kebijakan yang akan dibuat, terutama pada kebijakan terkait rencana aksi nasional keamanan siber. 4. Komunikasi dan kolaborasi yang intens dan efektif dengan elemen internal BSSN maupun stakeholder terkait, sehingga mempercepat proses penyusunan kebijakan. 5. Respons cepat dan koordinasi yang baik dengan berbagai pihak yang memperlancar proses penyempurnaan rancangan kebijakan.

Sasaran Strategis 4: Terpenuhinya Kerja Sama Keamanan Siber dan Sandi

Sasaran keempat terkait kerja sama bidang keamanan siber dan sandi yang diukur dengan indikator persentase pencapaian kerja sama keamanan siber internasional. Keamanan siber dan sandi merupakan upaya kolektif internasional yang melibatkan banyak negara. Kerja sama internasional bertujuan untuk mendorong penggunaan ruang siber yang terbuka, aman, stabil, dapat diakses dan damai sehingga dapat melindungi keamanan nasional dan mempromosikan stabilitas internasional. Kinerja terkait kerja sama internasional dapat dilihat pada gambar berikut.

Gambar 1.5. Target dan Realisasi Kerja Sama Internasional

Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja kerja sama internasional menunjukkan hasil yang sangat memuaskan. Pada tahun 2021 dan 2022, realisasi bahkan melampaui target secara signifikan dengan pencapaian 200% dan 250%. Sementara pada tahun 2023 dan 2024, realisasi mencapai 100% sesuai dengan target yang ditetapkan. Capaian kinerja tersebut didukung oleh beberapa upaya yang dilakukan sebagai berikut.

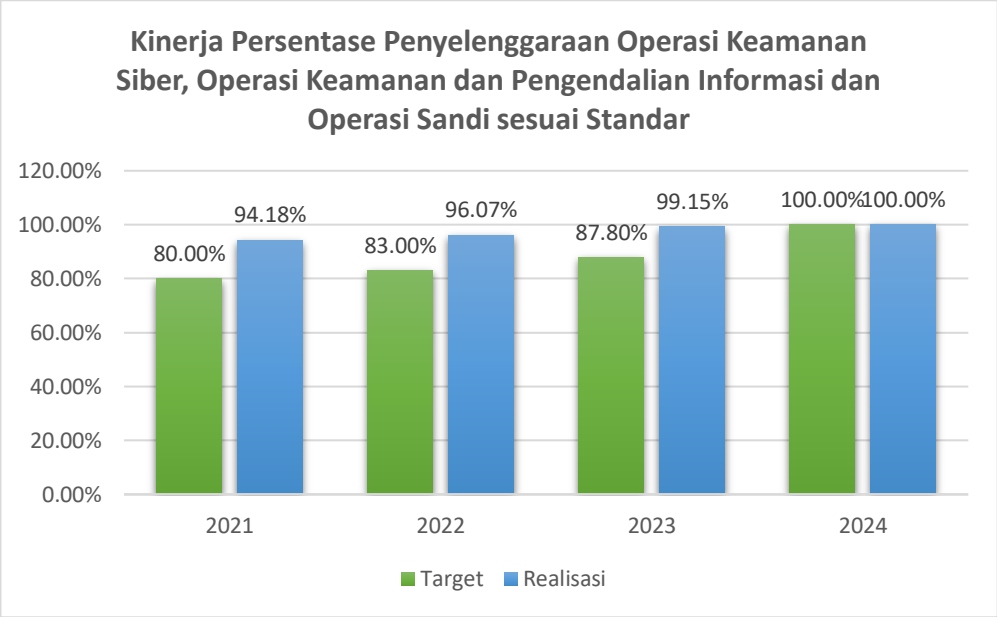
Tabel 1.4. Upaya yang dilakukan terkait kerja sama internasional

UPAYA YANG DILAKUKAN
2021
1. *Memorandum of Understanding* antara Pemerintah Australia tentang Kerja Sama Bidang Siber dan Teknologi Siber Berkembang 2. Pernyataan Kehendak (LoI) antara Pemerintah Republik Indonesia dan Pemerintah Amerika Serikat tentang Memajukan Kerja Sama Ruang Siber yang Erat 3. Persetujuan *(agreement)* antara Pemerintah Republik Indonesia dengan Federasi Rusia mengenai Kerja Sama dalam Bidang Keamanan Informasi Internasional
2022
1. *Memorandum of Understanding* (MoU) antara BSSN RI dengan KISA (Korea Information Security Agency) tentang Kerja Sama Peningkatan Kapasitas Keamanan Siber 2. *Memorandum of Understanding* antara BSSN RI dan Otoritas Keamanan Siber Nasional (NCA – National Cybersecurity Authority) Kerajaan Arab Saudi tentang Kerja Sama Keamanan Siber 3. *Memorandum of Understanding* antara BSSN RI dan Dewan Keamanan Siber (CSC Cyber Security Council) Uni Emirat tentang Kerja sama Keamanan Siber 4. *Plan of Action* (POA) 2022-2024 sebagai Implementasi MoU antara BSSN RI dan Administrasi Ruang Siber RRT tentang Kerja Sama Pengembangan Kapasitas Keamanan Siber dan Teknologi 5. Rencana untuk mengimplementasikan ruang lingkup kerja sama antara Indonesia dan Rusia di bidang jaminan keamanan informasi Internasional tahun 2022 - 2025
2023
1. Meningkatnya prioritas kebutuhan dari kedua belah pihak sehingga berpengaruh dalam percepatan proses kesepakatan dan penandatanganan dokumen kerja sama. 2. Pelaksanaan pembahasan kerja sama yang sudah dimudahkan dengan adanya platform *video conference*, sehingga tidak lagi ada keterbatasan harus dengan kehadiran fisik dari kedua belah pihak untuk dapat melaksanakan pembahasan rencana kerja sama. 3. Adanya komitmen penuh dari pimpinan dalam hal keterlibatan dan koordinasi langsung saat proses kesepakatan dan penandatanganan kesepakatan kerja sama.
2024
1. Adanya Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028 yang mengamanatkan peningkatan kerja sama internasional. 2. Meningkatnya prioritas kebutuhan dari kedua belah pihak sehingga berpengaruh dalam percepatan proses kesepakatan dan penandatanganan dokumen kerja sama. 3. Adanya komitmen penuh dari pimpinan untuk melaksanakan kerja sama di bidang keamanan siber dan sandi.

Sasaran Strategis 5: Meningkatnya Operasi Keamanan Siber dan Sandi

Sasaran kelima terkait operasi keamanan siber dan sandi yang diukur dengan indikator persentase penyelenggaraan operasi keamanan siber, operasi keamanan dan pengendalian informasi dan operasi sandi sesuai standar. Hal tersebut merupakan upaya BSSN dalam mengukur kepatuhan penyelenggaraan operasi sehingga diharapkan dapat meningkatkan kualitas operasi keamanan siber dan sandi di masa mendatang. Kinerja terkait penyelenggaraan operasi sesuai standar dapat dilihat pada gambar berikut.

Gambar 1.6. Target dan realisasi terkait penyelenggaraan operasi sesuai standar



Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja penyelenggaraan operasi sesuai standar secara keseluruhan menunjukkan hasil yang memuaskan. Realisasi konsisten melampaui target setiap tahunnya, dengan persentase pencapaian yang terus meningkat dari 94,18% pada tahun 2021, 96,07% pada tahun 2022, hingga 99,15% pada tahun 2023. Pada tahun 2024, target dan realisasi

sama-sama mencapai 100%. Capaian kinerja tersebut tidak lepas dari beberapa upaya yang dilakukan BSSN sebagai berikut.

Tabel 1.5. Upaya yang dilakukan terkait penyelenggaraan operasi sesuai standar

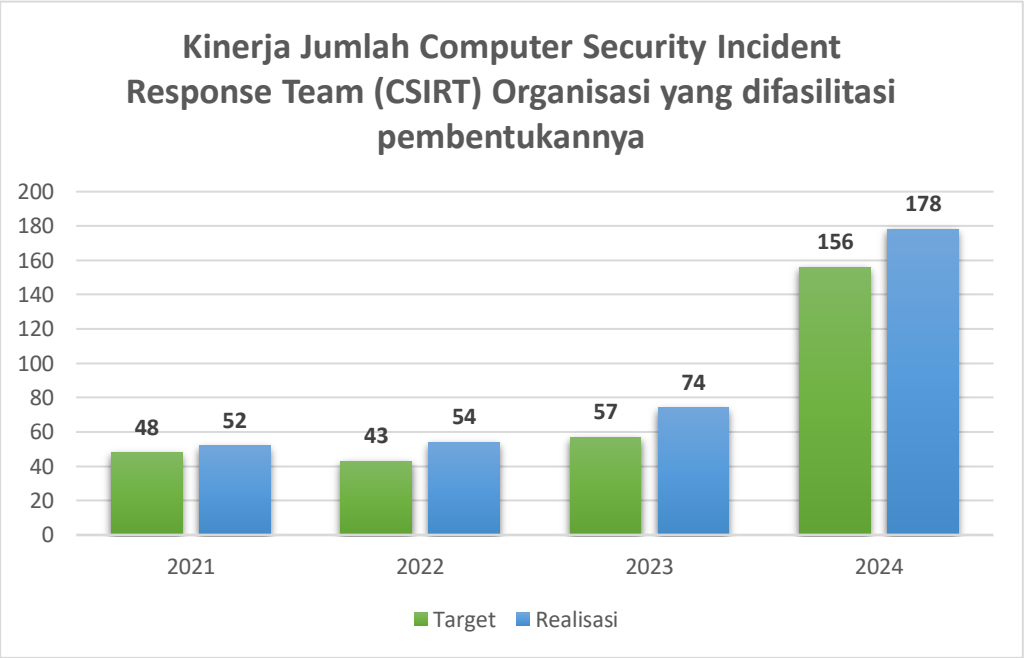
UPAYA YANG DILAKUKAN
2021
1. Ruang lingkup yang sudah jelas karena sebagian besar merupakan kegiatan rutin yang dilaksanakan BSSN sejak tahun-tahun sebelumnya 2. Komunikasi dengan *stakeholders* sudah terjalin dengan baik 3. SOP telah disusun setelah kegiatan berjalan dan terus dievaluasi implementasinya secara berkala
2022
1. Norma, Standar, Prosedur, dan kriteria (NSPK) dalam bentuk SOP disusun setelah kegiatan berjalan dan dievaluasi implementasinya secara berkala; 2. Ruang lingkup kegiatan yang sudah jelas dan sebagian besar merupakan operasi yang telah lama dilaksanakan semenjak tahun-tahun sebelumnya sehingga komunikasi dengan *stakeholder* telah terjalin dan kegiatan dapat diselenggarakan tanpa hambatan yang berarti.
2023
1. Melakukan perbaikan (*services maintenance*) terhadap beberapa perangkat penunjang operasi Deteksi Sinyal yang mengalami kerusakan 2. Melakukan evaluasi terhadap penggunaan *tools* yang digunakan dalam proses analisis hasil operasi deteksi sinyal 3. Menjaga hubungan koordinasi dengan *stakeholder* dan berkolaborasi secara intensif agar pelaksanaan kegiatan operasi berjalan sesuai dengan perencanaan. 4. Melanjutkan pelaksanaan evaluasi terhadap SOP yang sudah ada dan menyelesaikan SOP pelaksanaan operasinya, sehingga penyelenggaraan operasi dapat berjalan optimal
2024
1. Norma, Standar, Prosedur, dan Kriteria (NSPK) baik dalam bentuk SOP maupun pedoman telah disusun dan dilakukan evaluasi atas pelaksanaan dan implementasi kegiatan secara berkala. 2. Ruang lingkup kegiatan sudah jelas dan sebagian besar merupakan operasi yang telah rutin dilaksanakan, sehingga telah terjalin komunikasi dengan *stakeholder* dan kegiatan dapat diselenggarakan dengan baik.

Sasaran Strategis 6: Meningkatnya Kualitas Hasil Pembinaan Keamanan Siber dan Sandi

Kinerja pembinaan keamanan siber dan sandi diukur dengan indikator Jumlah *Computer Security Incident Response Team* (CSIRT)

Organisasi yang difasilitasi pembentukannya. Fasilitasi pembentukan yang diberikan BSSN kepada sektor pemerintahan dan pembangunan manusia serta fasilitasi CSIRT di sektor perekonomian. Kinerja terkait fasilitasi pembentukan CSIRT dapat dilihat pada gambar berikut.

Gambar 1.7. Target dan realisasi terkait fasilitasi pembentukan CSIRT



Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja penyelenggaraan fasilitasi pembentukan CSIRT secara keseluruhan dapat dikatakan sangat baik karena selama 4 (empat) tahun berturut-turut capaian kinerja terwujud. Capaian kinerja tersebut tidak lepas dari beberapa upaya yang dilakukan BSSN sebagai berikut.

Tabel 1.6. Upaya yang dilakukan terkait fasilitasi pembentukan CSIRT

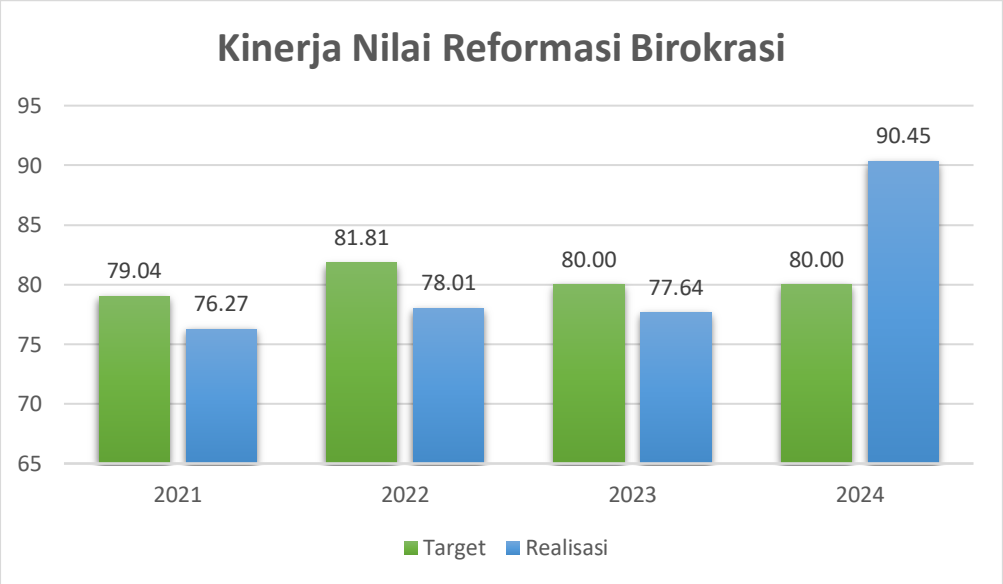
UPAYA YANG DILAKUKAN
Persentase penyelenggaraan pembinaan keamanan siber dan sandi kepada pemangku kepentingan sesuai standar
2021
1. Melaksanakan kegiatan asistensi kepada instansi terkait untuk meningkatkan pemahaman dan membangun kesadaran akan pentingnya CSIRT bagi keberlanjutan operasional TI organisasi yang diharapkan dapat mendorong komitmen pembentukan CSIRT. 2. Melaksanakan penilaian maturitas penanganan insiden keamanan siber menggunakan *tools* TMPI.

UPAYA YANG DILAKUKAN
3. Melaksanakan pembinaan atau pembekalan kepada CSIRT instansi terkait pengelolaan CSIRT agar mandiri dan efektif dalam menjalankan fungsi. 4. Melaksanakan evaluasi penyelenggaraan CSIRT instansi dan pemerintah rekomendasi sebagai bahan perbaikan.
2022
1. Melaksanakan kegiatan asistensi kepada *stakeholders* untuk meningkatkan pemahaman tentang CSIRT dan apa saja yang harus dipersiapkan untuk pembentukan CSIRT. 2. Melaksanakan penilaian maturitas penanganan insiden keamanan siber menggunakan *tools* TMPI. 3. Melaksanakan *workshop* untuk membangun kesadaran dan pembekalan Tim Teknis di organisasi yang menjalankan fungsi CSIRT.
2023
1. Adanya peraturan dan regulasi yang dapat mendorong dan mempercepat pembentukan CSIRT organisasi pada beberapa *stakeholder*. 2. Adanya *stakeholder* yang telah memiliki fungsi CSIRT namun belum teregistrasi, sehingga memudahkan untuk mendorong *stakeholder* tersebut untuk dapat meregistrasikan CSIRT-nya ke dalam Nat CSIRT. 3. Adanya sikap proaktif melalui koordinasi intens dengan *stakeholder* untuk membangun kesadaran akan pentingnya CSIRT bagi keberlanjutan bisnis dan operasional teknologi informasi organisasi sehingga dapat mendorong komitmen *stakeholder* dalam pembentukan CSIRT dalam melakukan kolaborasi lebih lanjut. 4. Adanya peluang skema *cost-sharing* dengan *stakeholder* untuk pelaksanaan asistensi pembentukan CSIRT.
2024
1. Adanya Peraturan Presiden No 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV), pasal 11-12 yang menyatakan bahwa penyelenggara IIV membentuk CSIRT, telah menjadi faktor pendorong stakeholder untuk segera membentuk dan meregistrasikan CSIRT-nya ke IDSIRTII/CC. 2. Adanya Peraturan BSSN Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028 yang mengamanatkan peningkatan kesiapsiagaan dan ketahanan siber melalui pembentukan CSIRT. 3. Diseminasi Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber yang dilakukan kepada Institusi Pembina Sektor, Asosiasi dan *Stakeholder*. 4. Adanya peraturan instansi pembina/induk stakeholder yang mempermudah dalam mendorong pembentukan dan pendaftaran CSIRT. 5. Melaksanakan pertemuan dengan pimpinan institusi sehingga dapat membangun kesadaran dan pentingnya CSIRT bagi keberlanjutan bisnis dan operasional TI organisasi, serta mendapatkan komitmen pembentukan CSIRT. 6. Melaksanakan kegiatan *workshop* membangun kesadaran dan pentingnya CSIRT bagi keberlanjutan bisnis dan operasional TI organisasi, serta mendapatkan komitmen pembentukan CSIRT. 7. Mendorong organisasi/ *stakeholder* yang telah memiliki fungsi CSIRT namun belum teregistrasi, untuk meregistrasikan CSIRT-nya ke IDSIRTII/CC. 8. Penyampaian hasil kegiatan pengukuran tingkat kematangan keamanan siber menjadi faktor pendorong kesadaran PSE untuk membentuk dan meregistrasikan CSIRT-nya ke IDSIRTII/CC. 9. Adanya fasilitasi layanan secara daring guna meningkatkan sasaran dalam sosialisasi dan asistensi pembentukan CSIRT untuk mengatasi permasalahan dalam penjadwalan kegiatan secara luring.

UPAYA YANG DILAKUKAN
10. Terdapat skema *sharing cost* dengan *stakeholder* pada saat pelaksanaan asistensi pembentukan CSIRT. 11. Adanya Surat Kepala BSSN Nomor T.1341/BSSN/PS.02.02/08/2024 tanggal 10 Agustus 2024 tentang Percepatan Pembentukan Tim Tanggap Insiden Siber Kabupaten/Kota di Indonesia.

Sasaran Strategis 7: Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien Dan Berorientasi Pada Pelayanan Publik

Sasaran ketujuh terkait perbaikan birokrasi BSSN yang diukur dengan 1 (satu) indikator yaitu terkait implementasi reformasi birokrasi. Nilai reformasi birokrasi BSSN merepresentasikan kualitas perbaikan tata kelola BSSN sehingga dapat berkontribusi dalam pembangunan nasional dan melayani masyarakat. Kinerja implementasi reformasi birokrasi dapat dilihat pada gambar berikut.



Gambar 1.8. Target dan realisasi Nilai Reformasi Birokrasi BSSN

Berdasarkan gambar di atas, dapat dilihat bahwa pada tiga tahun pertama (2021-2023), realisasi nilai RB berada sedikit di bawah target yang ditetapkan. Pada tahun 2021, realisasi mencapai 76,27 dari target 79,04, tahun 2022 mencapai 78,01 dari target 81,81, dan tahun 2023

mencapai 77,64 dari target 80,00. Penurunan pada tahun 2021 dipengaruhi oleh perubahan format implementasi RB Nasional. Namun terjadi peningkatan signifikan pada tahun 2024 di mana realisasi mencapai 90,45, jauh melampaui target yang ditetapkan sebesar 80,00. Hal ini menunjukkan adanya perbaikan substansial dalam implementasi reformasi birokrasi di BSSN. Capaian kinerja RB tidak lepas dari beberapa upaya yang dilakukan BSSN sebagai berikut.

Tabel 1.7. Upaya peningkatan birokrasi BSSN yang bersih, akuntabel, berkinerja tinggi, efektif, efisien dan berorientasi pada pelayanan publik

UPAYA YANG DILAKUKAN
Nilai RB BSSN
2021
1. Penyesuaian Renstra berdasarkan SOTK 2. Perbaikan Peraturan BSSN 6/2020: RB BSSN 3. Menyusun Peraturan BSSN tentang penanganan benturan kepentingan 4. Menyusun Peraturan BSSN tentang Sistem Penanganan Pengaduan melalui WBS 5. Perencanaan dan monev regulasi BSSN 6. Pemetaan, evaluasi, sinkronisasi dan harmonisasi Perka LSN dan/atau Perka BSSN 7. Penilaian risiko organisasi dan unit kerja 8. Percepatan penyusunan proses bisnis 9. Pengembangan ALMA: pengintegrasian dan modernisasi pelayanan publik BSSN 10. Asistensi penyusunan pohon kinerja 11. Pendampingan Tim RB 12. Sosialisasi tentang Koordinator dan Subkoordinator 13. Pemberian layanan konsultasi dan *remote assessment* RB 14. Diseminasi informasi RB
2022
1. Mengukur indeks PINTAR (83 pegawai) 2. Survei pemahaman RB ke seluruh pegawai 3. Diseminasi informasi RB 4. Pelaksanaan forum NGOPI RB 5. Rakor pengembangan dan penguatan *change agent, role model* dan BSSN Muda 6. *Open recruitment* dan penetapan BSSN Muda

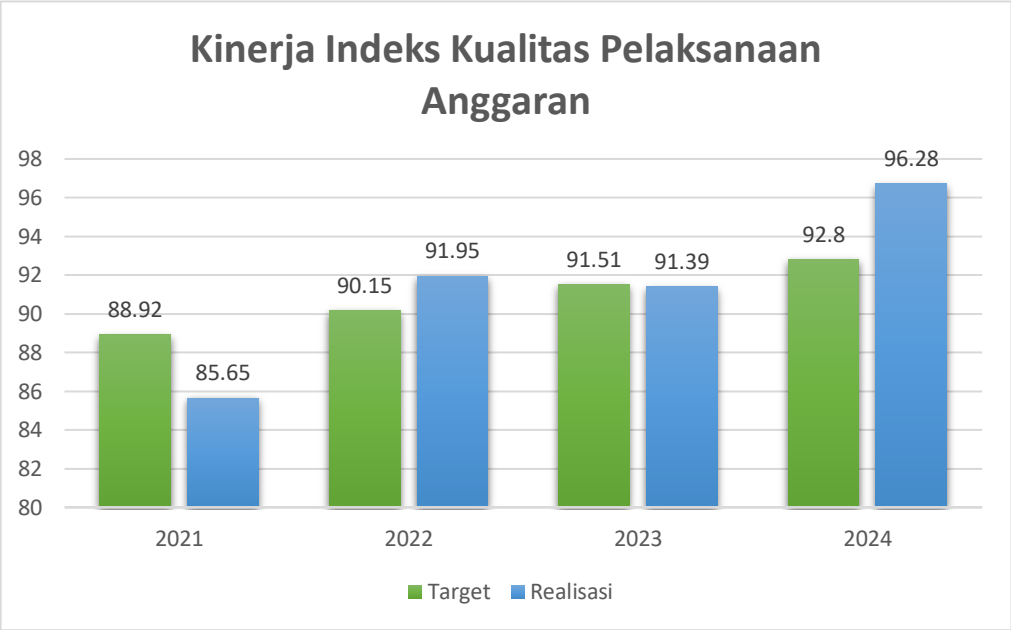
UPAYA YANG DILAKUKAN
7. Menyusun *roadmap* implementasi Core Values ASN 8. Menyusun rencana aksi penerapan kualitas kebijakan 9. Mengubah/Merevisi Peraturan BSSN 1/2021: Pembentukan Peraturan Per-UU dan Peraturan Internal BSSN 10. Menyusun perubahan BSSN 6/2021 Tentang OTK BSSN 11. Menyusun peraturan internal tentang sistem kerja di BSSN (Implementasi PermenPAN RB 7/2022: Sistem Kerja Instansi Pemerintah) 12. Menetapkan peta proses bisnis BSSN (Kep Kepala BSSN 248/2022) 13. Menyusun *enterprise architecture* SPBE BSSN 14. Menyusun instrumen penilaian serta *talent pool* 15. Menyusun analisis kebutuhan kompetensi (AKPK) individu untuk beberapa unit kerja *piloting* 16. Penyempurnaan fitur pemetaan potensi aplikasi SIABANG 17. Menyusun dan menindaklanjuti RATL rekomendasi hasil evaluasi SAKIP BSSN 18. Melakukan asistensi Zona Integritas terhadap Museum Sandi 19. Asistensi penilaian risiko BSSN dan Unit Kerja untuk membangun SPIP 20. Melakukan penilaian SPIP terintegrasi BSSN 21. Melakukan survei kepuasan pengguna layanan terkait aplikasi pelayanan publik yang sudah digunakan 22. Melakukan survei IKM setiap semester terhadap pengguna layanan dan melakukan analisa untuk bahan evaluasi guna meningkatkan kualitas layanan publik
2023
1. Melaksanakan pencerahan terkait penajaman *Roadmap* Reformasi Birokrasi Nasional kepada personil BSSN. 2. Penyusunan Rencana Aksi Reformasi Birokrasi General Tahun 2023. 3. Melakukan penataan organisasi BSSN (Peraturan BSSN No 4/2023), UPT BDS (Peraturan BSSN No 5/2023), dan UPT Museum Sandi (Peraturan BSSN No 6/2023). 4. Melakukan penyederhanaan administrasi di lingkungan BSSN yang sebelumnya terdapat 133 jabatan, menjadi 31 jabatan administrasi. 5. Melakukan evaluasi kelembagaan dan telah di verifikasi oleh Kemen PAN RB. 6. Melakukan penetapan dan sosialisasi Surat Edaran No 5/2023 tentang Mekanisme Kerja di Lingkungan BSSN. 7. Melakukan penyesuaian SOP dan Proses Bisnis Unit Kerja sesuai Mekanisme Kerja Baru. 8. Melakukan monitoring pembentukan tim kerja tahun 2023 dengan pembentukan *squad team*. 9. Melanjutkan penyempurnaan penjenjangan kinerja pada level Kementerian dan seluruh unit kerja. 10. Menyusun pedoman teknis perencanaan kinerja dalam bentuk surat edaran No. 16/2023 tentang Penyusunan Perencanaan Program dan Anggaran di Lingkungan BSSN. 11. Menyusun pedoman pengukuran kinerja atas pelaksanaan program dan anggaran (Surat Edaran No. 12/2023 tentang Tata Cara Pengukuran Nilai Kinerja Program dan Anggaran (NKPA) dan Nilai Kinerja Kegiatan dan Anggaran (NKKA) di Lingkungan BSSN. 12. Melakukan sosialisasi RB dengan cara NGOPI RB, BSSN, Reform Gathering, RB Expo dan optimalisasi media informasi. 13. Melakukan assurance terhadap Governance, Risk and Compliance (GRC).

UPAYA YANG DILAKUKAN
2024
1. Penyusunan rencana aksi RB tahun 2024 telah mengacu pada Keputusan Menteri PANRB Nomor 739 tahun 2023 tentang Petunjuk Teknis Evaluasi Reformasi Birokrasi Tahun 2023. 2. Penajaman rencana aksi RB BSSN tahun 2024 untuk dapat menjawab sasaran dari setiap kegiatan utama. 3. Penetapan target atas kegiatan utama pada rencana aksi RB BSSN tahun 2024 telah merujuk pada target RB nasional. 4. Penajaman indikator *output* atas rencana aksi RB BSSN tahun 2024 agar relevan dan menggambarkan sasaran yang ingin diwujudkan. 5. Inspektorat telah melaksanakan evaluasi internal tahap perencanaan (ex-ante) dengan tujuan untuk memastikan *roadmap* dan rencana aksi RB BSSN memiliki kualitas yang baik dan layak menjadi pedoman dalam pelaksanaan RB, serta berisi solusi terkait isu dan pemerintahan. 6. BSSN telah mengajukan permohonan kepada Kementerian PANRB perihal penataan organisasi Balai Sertifikasi Elektronik. 7. BSSN telah menerbitkan Peraturan BSSN Nomor 6 Tahun 2024 tentang Organisasi dan Tata Kerja Balai Besar Sertifikasi Elektronik. 8. Telah dilaksanakan pemenuhan dan monitoring pembentukan tim kerja tahun 2024 dengan pembentukan squad team dalam bentuk Keputusan Kepala BSSN di seluruh unit kerja di lingkungan BSSN. 9. Mendorong unit kerja untuk melakukan pembaruan dokumen SOP untuk mengakomodasi mekanisme sistem kerja baru. 10. Melakukan percepatan penyelesaian pembangunan aplikasi e-spip. 11. Melaksanakan *updating* register risiko level BSSN. 12. Melaksanakan monitoring penyelesaian Rencana Tindak Pengendalian (RTP) Unit Kerja. 13. Melaksanakan audit kinerja tahun 2024. 14. Melakukan asistensi dan pendampingan pada Biro OSDM dalam proses pembangunan zona integritas. 15. Melakukan identifikasi unit kerja yang siap membangun zona integritas. 16. Melakukan monitoring kepada unit kerja yang telah berpredikat WBK agar dapat secara aktif bersinergi mendorong implementasi zona integritas pada unit kerja lainnya. 17. Melakukan identifikasi potensi terjadinya *crosscutting* kinerja secara menyeluruh terhadap kinerja organisasi BSSN. 18. Melakukan reviu dan perbaikan kualitas dokumen perencanaan agar lebih berorientasi pada hasil.

Sasaran Strategis 8: Meningkatnya Pengelolaan Keuangan BSSN yang Akuntabel

Sasaran Strategis Meningkatnya Pengelolaan Keuangan BSSN yang Akuntabel diukur melalui dua indikator yaitu (1) Indeks Kualitas Pelaksanaan Anggaran (IKPA) dan (2) Opini Badan Pemeriksa Keuangan (Opini BPK). IKPA merupakan indeks yang mengukur kualitas kinerja

pelaksanaan anggaran belanja Kementerian/Lembaga dari sisi kesesuaian terhadap perencanaan, efektivitas pelaksanaan anggaran, efisiensi pelaksanaan anggaran, dan kepatuhan terhadap regulasi. Kinerja terkait IKPA dapat dilihat pada gambar di bawah ini.



Gambar 1.9 Capaian Kinerja Indeks Kualitas Pelaksanaan Anggaran

Berdasarkan aplikasi OM-SPAN Kementerian Keuangan, pada tahun 2021, nilai IKPA BSSN mengalami penurunan dikarenakan terdapat perubahan parameter pengukuran indeks terkait capaian rincian *output* (RO). Capaian IKPA BSSN tahun 2022 dan 2023 adalah sebesar 91,95 dan 91,39 dengan kategori "Baik". Pada tahun 2024, nilai IKPA BSSN mengalami kenaikan yang cukup signifikan menjadi 96,72 dengan kategori "Sangat Baik". Terdapat beberapa hal yang telah dilakukan BSSN sehingga mendapatkan nilai tersebut, antara lain:

1) Melakukan percepatan belanja kontraktual dengan pelaksanaan kontrak pra DIPA untuk indikator Kontraktual;
2) Melakukan pendaftaran kontrak ke KPPN sebelum batas akhir waktu pendaftaran kontrak untuk indikator belanja kontraktual;

3) Melakukan pendaftaran UP Tunai secara rasional sesuai kebutuhan bulanan untuk indikator pengelolaan UP dan TUP;
4) Melakukan pengisian data capaian *output* bulanan secara akurat dan disiplin secara tepat waktu sebelum 5 (lima) hari kerja setiap awal bulan, karena ketepatan waktu merupakan salah satu komponen penilaian untuk indikator Capaian *Output*;
5) Melakukan reviu dan memperbaiki/ Menyusun kembali Rencana Penarikan Dana (RPD) setiap awal triwulan untuk indikator Deviasi Rencana Penarikan Dana.

Analisis terkait indikator kedua yaitu opini BPK atas laporan keuangan BSSN. Indikator tersebut menilai kewajaran pelaporan keuangan BSSN berdasarkan hasil audit yang diselenggarakan BPK. Kinerja terkait pelaporan keuangan BSSN dapat dilihat pada gambar berikut.

Gambar 1.10. Tren Kinerja Nilai Opini BPK atas Laporan Keuangan BSSN

Berdasarkan gambar di atas, dapat disimpulkan bahwa capaian kinerja kewajaran pelaporan keuangan BSSN secara keseluruhan dapat dikatakan sangat baik karena selama 4 (empat) tahun berturut-turut capaian kinerja terwujud. Capaian Opini BPK tidak lepas dari beberapa upaya yang dilakukan BSSN dalam 3 (tiga) tahun terakhir sebagai berikut.

Tabel 1.8. Upaya Peningkatan Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien dan Berorientasi Pada Pelayanan Publik

UPAYA YANG DILAKUKAN
Indeks Kualitas Pelaksanaan Anggaran
1. Memperbaiki perencanaan dan eksekusi kegiatan secara relevan dan terjadwal, sehingga tidak menumpuk realisasi penyerapan anggaran pada periode triwulan IV. 2. Melakukan percepatan belanja, khususnya untuk belanja barang dan jasa. 3. Mengoptimalkan penyerapan anggaran secara proporsional setiap bulan berdasarkan target, rencana kegiatan, dan rencana penarikan dana yang telah disusun. 4. Memastikan setiap pelaporan capaian *output* sudah di input dengan akurat, teliti, dan disiplin waktu, sebelum 5 (lima) hari kerja setiap awal bulan, karena ketepatan waktu merupakan salah satu komponen penilaian. 5. Meningkatkan koordinasi antar pengelola anggaran, dan PPK dengan unit kerja pengelola kegiatan, dalam melakukan pengawasan, perhitungan, dan pelaporan data capaian *output*.
Nilai Opini BPK
2021
1. Menindaklanjuti temuan BPK sebanyak 207 rekomendasi (99,52%) 2. Sebanyak 1 (satu) rekomendasi yang belum ditindaklanjuti dengan nominal temuan Rp.0
2022
1. Menindaklanjuti temuan BPK sebanyak 228 rekomendasi (97,85%) 2. Sebanyak 5 (lima) rekomendasi yang belum selesai ditindaklanjuti dengan nominal temuan Rp.142.860.559,88 3. Melakukan kegiatan pemantauan tindak lanjut atas rekomendasi LHP BPK 4. Memastikan kesesuaian dengan standar akuntansi pemerintahan, kecukupan pengungkapan, kepatuhan terhadap Peraturan Perundang-Undangan, dan efektivitas SPIP.
2023
1. Melaksanakan pemantauan secara intensif terhadap pelaksanaan tindak lanjut atas rekomendasi LHP yang disampaikan oleh BPK. 2. Melakukan peningkatan terhadap upaya pengendalian *intern* khususnya yang berkaitan dengan pelaporan keuangan. 3. Melakukan peningkatan kualitas sumber daya manusia yang menangani pengelolaan anggaran melalui pelatihan/bimtek/*workshop*/sosialisasi terkait pengelolaan anggaran dan pengadaan barang/jasa pemerintah.
2024
1. Melakukan reviu atas Laporan Keuangan BSSN minimal dilakukan 2 (dua) semester dalam setiap tahun anggaran. 2. Meningkatkan upaya pengendalian intern atas pelaporan keuangan. 3. Melakukan kegiatan pemantauan tindak lanjut atas rekomendasi LHP BPK secara berkala. 4. Melakukan pemantauan penyelesaian kerugian negara. 5. Melakukan pengawasan atas Penerimaan Negara Bukan Pajak (PNBP).

UPAYA YANG DILAKUKAN
6. Kerja sama tim penyusun Laporan Keuangan BSSN dan tim reviu Laporan Keuangan BSSN. 7. Dukungan unit kerja dalam penyediaan data pendukung pemeriksaan audit laporan keuangan dan tindak lanjut hasil pemeriksaan. 8. Perhatian pimpinan dalam setiap kegiatan baik dari entry meeting dengan BPK hingga *exit meeting* dengan BPK atas audit laporan keuangan.

1.1.2 Aspirasi Masyarakat

Aspirasi masyarakat merupakan harapan masyarakat terkait pemenuhan kebutuhan barang publik, layanan publik, dan regulasi dalam lingkup kewenangan BSSN 2020 – 2024. Berdasarkan Peraturan Menteri PPN Nomor 10 Tahun 2023, penjaringan aspirasi masyarakat didapatkan melalui wadah dan mekanisme yang akuntabel seperti forum konsultasi, forum diskusi kelompok terarah *(focus group discussion),* media cetak dan media elektronik, situs web *(website)*, dan sebagainya. Berdasarkan hasil analisis, aspirasi masyarakat terhadap layanan publik didapatkan dari aplikasi Sistem Pengelolaan Pelayanan Publik Nasional – Layanan Aspirasi dan Pengaduan Online Rakyat (SP4N-LAPOR) dan Survei Kepuasan Masyarakat.

Pertama, aspirasi masyarakat yang berasal dari SP4N LAPOR BSSN. Secara garis besar terdapat 5 (lima) aspirasi sebagai berikut.

1. Komunikasi, Informasi dan Edukasi (KIE)
    a. Perlu adanya sosialisasi dan diseminasi terkait prosedur untuk mendapatkan layanan Sistem Manajemen Pengamanan Informasi (SMPI).
    b. Masyarakat menghendaki adanya aplikasi lapor BSSN yang independen, terpisah dari aplikasi SP4N LAPOR.
2. Celah/kejadian keamanan siber
    a. BSSN perlu melakukan langkah-langkah pencegahan dan penanggulangan keamanan siber untuk *website* Pemerintah,

mengingat banyaknya *website* Pemerintah yang disusupi spam seperti judi *online*.

b. BSSN perlu meminimalisasi celah keamanan yang termasuk kategori fatal pada *website* Pemerintah karena saat ini masyarakat melakukan *penetration tester* seperti pada *website* kki.go.id dan kemenkopmk.go.id.

3. Sinergi BSSN dengan KPU dalam memanfaatkan sistem berbasis *blockchain* yang digunakan pada sistem perhitungan suara di pemilihan umum. Adanya sistem *blockchain* membuat data yang disajikan semakin transparan dengan kemungkinan manipulasi data yang kecil.
4. Seleksi ASN BSSN
   a. Masyarakat menghendaki transparansi dalam penerimaan Pegawai Pemerintah dengan Perjanjian Kerja (PPPK).
   b. Masyarakat menghendaki proses seleksi PPPK yang profesional dengan mal administrasi yang minimal.
5. Pemanfaatan Tanda Tangan Elektronik (TTE) tidak hanya pada institusi pemerintah melainkan pada institusi swasta, khususnya pada bidang pendidikan.

Kedua, aspirasi masyarakat yang didapatkan dari Survei Kepuasan Masyarakat (SKM) yang dilakukan oleh penyelenggara pelayanan publik BSSN. Secara garis besar terdapat 6 (enam) aspirasi sebagai berikut.

1. Perlu adanya pendidikan dalam bidang keamanan siber sejak dini guna membentuk kesadaran keamanan siber masyarakat.
2. Perlu peningkatan kreativitas, inovasi dalam bidang keamanan siber dalam meningkatkan keamanan siber.
3. Perlu adanya inovasi pelayanan publik BSSN agar memudahkan masyarakat.
4. Perlu adanya pusat pengaduan masyarakat *(call center)* terkait layanan publik BSSN agar memudahkan masyarakat.

5. Perlu adanya peningkatan SDM pemberi layanan serta sarana dan prasarana layanan publik BSSN dalam meningkatkan kualitas layanan publik BSSN, dan
6. Perlu ada sinergi dengan TNI dan Polri dalam mewujudkan kedaulatan ruang siber.

Ketiga, aspirasi yang dijaring oleh UKE 1. Secara garis besar terdapat 4 (empat) aspirasi yang terjaring sebagai berikut.

1. Komunikasi, Informasi dan Edukasi (KIE)
    a. BSSN melakukan asistensi terhadap instansi pemerintah, khususnya di Pemerintah Daerah untuk melihat kesiapan keamanan siber di wilayah tersebut. Beberapa Pemerintah Daerah melihat keamanan siber sebagai hal penting yang perlu mendapatkan atensi.
    b. Dalam melakukan bimbingan teknis, BSSN sebaiknya didahului dengan pemetaan kemampuan peserta karena maturitas dari setiap peserta tidak sama. Sebaiknya materi juga lebih banyak pada aspek implementasi agar pemanfaatan dapat berjalan efektif dan efisien dalam pelaksanaan tugas dan fungsi instansi peserta.
    c. BSSN memberikan edukasi kepada instansi dan masyarakat mengenai keamanan siber sehingga dapat mendorong kesadaran masyarakat untuk berinteraksi dengan tepat dan aman.
    d. BSSN menyebarluaskan mengenai regulasi mengenai siber dan sandi nasional kepada para pemangku kepentingan untuk dapat mencegah munculnya insiden dan bagaimana mengatasi ancaman keamanan siber.
    e. Sektor siber dan sandi memerlukan dukungan SDM yang kompeten di bidangnya dan sebaiknya penugasan SDM tidak

hanya dilakukan di Pemerintah Pusat namun menyentuh instansi Pemerintah Daerah.

f. Belum banyaknya masyarakat yang mengetahui tugas dan fungsi serta layanan yang diberikan BSSN kepada masyarakat sehingga BSSN perlu melakukan *branding* untuk mempertegas *positioning* BSSN di tingkat nasional.

2. Evaluasi dan umpan balik
    a. BSSN diharapkan dapat mengevaluasi implementasi keamanan siber dengan melakukan kunjungan langsung ke organisasi *stakeholders* untuk melihat bagaimana implementasi keamanan siber di organisasi tersebut.
    b. BSSN memberikan umpan balik mengenai implementasi keamanan siber pada organisasi *stakeholders* untuk meningkatkan kualitas implementasi keamanan siber *stakeholders*.
3. Regulasi: BSSN diharapkan dapat mendorong munculnya regulasi terkait keamanan siber untuk menjamin penyelenggaraan keamanan siber memiliki payung regulasi yang tepat.
4. Kolaborasi: BSSN mendorong kerja sama nasional dan internasional terkait siber dan sandi untuk mengantisipasi hingga penanggulangan permasalahan siber dan sandi nasional.

1.1.3 Studi Banding dengan Instansi Sejenis

Studi banding dengan instansi bertujuan untuk membandingkan antara BSSN dengan beberapa instansi yang memiliki tugas dan fungsi yang tidak jauh berbeda dengan BSSN. Instansi yang memiliki fungsi dan tugas sejenis yang digunakan sebagai acuan pada proyek ini adalah Cybersecurity and Infrastructure Security Agency (CISA) dari Amerika Serikat dan National Cyber Strategy Centre (NCSC) dari Inggris.

1. Cybersecurity and Infrastructure Security Agency (CISA) – Amerika Serikat

Cybersecurity and Infrastructure Security Agency (CISA) sebagai instansi keamanan siber di Amerika Serikat memiliki fokus pada peningkatan keamanan siber di dalam negeri dengan melibatkan banyak pihak baik swasta maupun pemerintah. CISA memiliki tanggung jawab untuk melindungi infrastruktur vital seperti keuangan, energi, dan transportasi. Meskipun memiliki kesamaan dengan BSSN, CISA lebih berfokus untuk menciptakan sistem keamanan siber untuk melindungi infrastruktur vital di Amerika Serikat.

2. National Cyber Strategy Centre (NCSC) - Inggris

   National Cyber Strategy Centre memiliki fokus pada lingkup keamanan siber di tingkat nasional, dengan penekanan pada peningkatan kesadaran terhadap keamanan siber bagi masyarakat Inggris. Selain itu, NCSC telah aktif untuk membangun sistem keamanan dasar untuk layanan berbasis elektronik yang beroperasi di Inggris. Meskipun memiliki tujuan yang tidak jauh berbeda, NCSC memiliki fokus untuk memberikan pencerdasan ke masyarakat inggris maupun UMKM terkait pentingnya keamanan siber.

1.2 Potensi dan Permasalahan

Dalam rangka menyusun rencana strategis BSSN, organisasi perlu melakukan analisis lingkungan strategis yang meliputi identifikasi potensi dan permasalahan yang dihadapi. Potensi adalah segala sesuatu yang dapat dimanfaatkan oleh organisasi untuk mencapai tujuan dan sasaran yang diinginkan. Permasalahan adalah segala sesuatu yang menghambat atau mengancam pencapaian tujuan dan sasaran organisasi. Analisis potensi dan permasalahan bertujuan untuk mengetahui kekuatan, kelemahan, peluang, dan ancaman yang ada dalam lingkungan internal dan eksternal organisasi.

Dengan melakukan analisis potensi dan permasalahan, organisasi dapat menentukan strategi yang tepat untuk memaksimalkan potensi yang

ada dan meminimalkan permasalahan yang muncul. Strategi ini dapat berupa penguatan, pengembangan, peningkatan, perbaikan, pemecahan, pencegahan, atau mitigasi terhadap potensi dan permasalahan yang teridentifikasi. Strategi ini kemudian dijabarkan menjadi program, kegiatan, indikator, target, dan anggaran yang menjadi bagian dari rencana strategis organisasi. Berikut adalah analisis potensi dan masalah BSSN melalui analisis terhadap faktor eksternal organisasi, seperti: politik, ekonomi, sosial, teknologi, dan lingkungan hidup (PESTEL).

1.2.1 Politik dan Hukum

Analisis lingkungan politik dan hukum merupakan analisis lingkungan makro dan meso untuk melihat pengaruh kebijakan politik dan regulasi terhadap penyelenggaraan keamanan siber nasional serta dampaknya terhadap BSSN. Dampak dari analisis terbagi menjadi 2 (dua) yaitu potensi (P) atau tantangan (T). Lebih detail mengenai analisis perubahan politik dan hukum dapat dilihat pada tabel berikut.

Tabel 1.9. Hasil Analisis Perubahan Lingkungan Politik dan Hukum

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
1	Adanya kebijakan tentang perencanaan, persiapan, pemindahan dan penyelenggaraan Ibu Kota Nusantara (IKN)	Pemindahan kedudukan lembaga negara dan ASN yang ditentukan ke IKN	Pimpinan dan ASN BSSN akan dipindah ke IKN	P
			Kantor pusat BSSN akan berpindah ke IKN	P
			BSSN perlu menata ulang sarana dan prasarana sandi dan keamanan siber di IKN	P
			BSSN perlu menyusun perencanaan dan anggaran terkait pemindahan BSSN dan ASN BSSN ke IKN	T
2	Diundangkannya Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)	Sistem pemerintahan berbasis elektronik dapat memudahkan aktivitas masyarakat saat	Data masyarakat dan pemerintah perlu disimpan dan dikelola dengan baik. Serta memastikan data masyarakat dan pemerintah berada	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
		mengurus berkas dengan kementerian atau lembaga terkait.	dalam kondisi aman dari peretasan.	
			Penerapan pemberian imbalan kepada peretas topi putih dapat diterapkan guna membangun kolaborasi antara pemerintah dan peretas topi putih dalam mendesain sistem keamanan data.	P
			BSSN perlu membuat regulasi terkait dokumen yang boleh dipublikasikan ke masyarakat dan dokumen yang tidak boleh dipublikasi ke masyarakat.	T
		Sistem pemerintahan berbasis elektronik dapat meningkatkan transparansi pemerintah ke masyarakat.	BSSN dapat mengoordinasikan pelaksanaan Strategi Keamanan Siber dan Nasional (SKSN) serta Manajemen Krisis Siber (MKS) secara nasional	P
			SKSN) serta MKS secara detail dapat direncanakan dan dilaksanakan dengan baik	P
			Dalam pelaksanaan SKSN dan MKS, BSSN berperan dalam: 1. mengoordinasikan pelaksanaan; 2. memantau pelaksanaan; 3. mengevaluasi pelaksanaan 4. melaporkan hasil pelaksanaan.	P
			BSSN berpotensi menjadi *leading sector* dalam Pengelolaan Keamanan Siber serta Manajemen Keamanan Siber	P
			BSSN perlu menyusun peraturan perundang-	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
			undangan (Peraturan Badan) yang merupakan turunan dari Perpres SKSN dan MKN	
3	Diundangkannya Peraturan Presiden nomor 82 tahun 2022 tentang Pelindungan Infrastruktur IIV	Pelindungan IIV telah memiliki payung hukum dan dapat dikoordinasikan di seluruh K/L	BSSN menjadi *leading sector* dalam mengkoordinasikan pelindungan IIV khususnya di sektor administrasi pemerintahan	P
			Pelaksanaan pelindungan IIV dilaksanakan sektoral dengan koordinator pada masing-masing sektor, sehingga pelaksanaan lebih komprehensif	P
4	Geopolitik: Beberapa negara saat ini tengah mengembangkan kapabilitas siber baik ofensif dan defensif: - Amerika Serikat melalui NSA dan US *Cyber Command*, terlibat aktif dalam operasi siber global - China (RRT) dituduh melakukan spionase siber terhadap sektor industri dan pemerintahan negara lain - Rusia terlibat dalam operasi disinformasi dan serangan siber, termasuk terhadap infrastruktur penting negara lain - Iran dan Korea Utara dikenal menggunakan serangan siber untuk spionase dan sabotase	Indonesia dapat menjadi target serangan siber oleh negara lain sebagai aktor siber, khususnya yang memiliki kepentingan yang berbeda dengan Indonesia	Adanya ancaman serangan siber dari negara lain, khususnya terhadap Infrastruktur Informasi Vital (IIV) Indonesia	T
5	Geopolitik: Peningkatan serangan siber terhadap	Serangan siber terhadap infrastruktur	Serangan siber terhadap infrastruktur kritis akan semakin masif	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
	infrastruktur kritis seperti listrik, air, transportasi, perbankan, layanan kesehatan dan lain-lain Contoh: *Colonial Pipeline* di AS tahun 2021, serangan siber terhadap pemerintahan dan energi Ukraina, serangan terhadap Bank Syariah Indonesia (BSI), dan lain-lain	kritis berpotensi akan tetap terjadi di Indonesia	menyerang layanan publik dan data pribadi	
			Masyarakat akan semakin sadar akan pentingnya keamanan siber, khususnya bagi masyarakat yang telah mengalami serangan siber	P
6	Geopolitik: Saat ini negara-negara sedang berlomba-lomba dalam membangun "*cyber arsenal*", baik untuk menyerang sistem lawan (*cyber offense*), melindungi diri dari serangan lawan (*cyber defense*) maupun menguasai ruang informasi (*cyber influence*).	Indonesia dapat membangun "*cyber arsenal*" sendiri, minimal untuk melindungi diri dari serangan lawan (*cyber defense*)	Mendorong penelitian dan pengembangan siber dan sandi di BSSN dalam menciptakan "*cyber arsenal*" sendiri	P
7	Adanya beberapa perjanjian dan diplomasi siber internasional: - Tallinn Manual: panduan hukum internasional dalam perang (operasional) siber. - Norma PBB yaitu *Group of Government Expert* (UN GGE) & *Open-Ended Working Group* (OEWG): membahas norma perilaku negara dalam ruang siber	Penegasan posisi Indonesia dalam tata kelola siber melalui peran aktif Indonesia dalam UN OEWG	Penegasan posisi Indonesia dalam tata kelola siber melalui peran aktif Indonesia dalam UN OEWG	P
		Indonesia dapat menggunakan Tallin Manual maupun norma PBB sebagai salah satu referensi dalam menyusun strategi dan kebijakan pertahanan siber	Indonesia dapat menggunakan Tallin Manual maupun norma PBB sebagai salah satu referensi dalam menyusun strategi dan kebijakan pertahanan siber	P
		Perjanjian dan diplomasi	BSSN dapat memanfaatkan	P

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
		internasional dapat membantu pelindungan infrastruktur kritis di Indonesia	perjanjian dan diplomasi internasional dalam melindungi infrastruktur kritis di Indonesia	
		Terbukanya peluang kerja sama siber regional maupun bilateral	BSSN dapat memperluas kerja sama siber regional maupun bilateral dalam meningkatkan ketahanan siber Indonesia.	P
		Regulasi di Indonesia belum sepenuhnya mengadopsi kerangka normatif internasional.	Regulasi di Indonesia belum sepenuhnya mengadopsi kerangka normatif internasional.	T
8	Munculnya kelompok-kelompok kriminal seperti kelompok Lazarus (Korea Utara) yang dikenal melakukan berbagai serangan siber untuk mendukung kepentingan negara	Indonesia berpotensi terkena serangan siber dari kelompok-kelompok kriminal seperti kelompok Lazarus (Korea Utara) ini	Indonesia berpotensi terkena serangan siber dari kelompok-kelompok kriminal seperti kelompok Lazarus (Korea Utara) ini	T
			BSSN dapat membaca pola kerja dan serangan kelompok-kelompok kriminal, sehingga dapat mengantisipasi dan mengatasi jika terjadi serangan	P
9	Beberapa negara menerapkan kedaulatan digital dan fragmentasi internet - *Great Firewall China*: Sistem yang digunakan China (RRT) untuk mengontrol akses internet domestik - *RuNet Rusia*: Upaya Rusia untuk menciptakan internet domestik yang terpisah dari jaringan global	Indonesia dapat menerapkan kebijakan kedaulatan digital dan fragmentasi internet, khususnya dari aplikasi maupun informasi yang berpotensi merusak generasi muda Indonesia	BSSN dapat menerapkan kebijakan kedaulatan digital dan fragmentasi internet, khususnya dari aplikasi maupun informasi yang berpotensi merusak generasi muda Indonesia	P

Berdasarkan tabel di atas, terdapat 9 (sembilan) fakta makro dengan 14 dampak nasional. Berdasarkan hasil analisis, seluruh faktor makro dan dampak nasional memiliki 26 dampak terhadap BSSN yang terdiri dari 18 peluang dan 8 (delapan) tantangan bagi BSSN yang berhasil teridentifikasi dari perubahan lingkungan politik dan hukum, termasuk perkembangan geopolitik internasional.

1.2.2 Ekonomi

Analisis ekonomi merupakan faktor eksternal yang sangat penting untuk diperhatikan. Tujuan dari analisis ekonomi ini adalah untuk mengidentifikasi fakta-fakta terkait ekonomi dan dampaknya pada skala nasional serta dampaknya terhadap BSSN. Dari analisis dampak perubahan ekonomi tersebut, akan ditentukan apakah fakta-fakta yang terjadi tersebut menjadi potensi (P) atau tantangan (T) bagi BSSN. Berikut adalah hasil analisis fakta-fakta ekonomi dan dampaknya dalam skala nasional dan terhadap BSSN.

Tabel 1.10. Analisis Ekonomi

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
1	Nilai ekonomi data telah meningkat secara signifikan. Dengan makin meningkatnya digitalisasi, data menjadi aset yang sangat berharga. Data dapat digunakan untuk berbagai tujuan, mulai dari analisis bisnis hingga penargetan iklan.	Seiring dengan peningkatan nilai data ini, motivasi ekonomi untuk melakukan serangan siber juga meningkat. Para pelaku serangan dapat mencuri data dan menjualnya di pasar gelap atau menggunakan informasi tersebut untuk mendapatkan keuntungan finansial melalui penipuan atau pemerasan (seperti *ransomware*).	• BSSN perlu meningkatkan upaya deteksi dan pencegahan serangan terhadap masyarakat dan instansi dalam melindungi data secara nasional baik BSSN maupun di luar BSSN. Hal ini melibatkan peningkatan investasi dalam teknologi dan sumber daya manusia, serta peningkatan kerja sama dengan lembaga lain baik di dalam maupun luar negeri. • BSSN perlu meningkatkan *information sharing* dengan BSSN dan	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
			stakeholder atau antar *stakeholder*. • BSSN perlu mengembangkan dan menerapkan kebijakan baru untuk menangani peningkatan ancaman berkaitan dengan data. • BSSN perlu melakukan edukasi kepada masyarakat dan instansi pemerintah tentang pentingnya keamanan siber dan bagaimana melindungi data.	
2	Kerugian ekonomi dari kejahatan siber. Kejahatan siber dapat menyebabkan kerugian ekonomi yang signifikan. Hal ini bisa berupa kerugian langsung seperti pencurian uang atau data, serta kerugian tidak langsung seperti kerusakan reputasi, penurunan kepercayaan, dan biaya pemulihan dari serangan.	Kejahatan siber dapat memiliki dampak ekonomi yang luas terhadap negara Indonesia. • Kepercayaan publik dan internasional terhadap infrastruktur digital Indonesia bisa berkurang, yang bisa berdampak pada investasi dan kerja sama internasional.	Kerugian ekonomi dari kejahatan siber memperlihatkan pentingnya peran BSSN dalam melindungi ruang siber Indonesia. Dengan meningkatnya kejahatan siber, BSSN diharapkan untuk lebih meningkatkan upaya dalam melindungi siber. Ini bisa berarti BSSN perlu melakukan: • Peningkatan dana dan kompetensi SDM BSSN • Peningkatan kerja sama dengan entitas lain (contoh: *managed service*, asuransi siber, dll). • Perubahan strategi atau kebijakan. • Memastikan bahwa masyarakat dan organisasi di Indonesia dapat memahami dan menanggapi risiko kejahatan siber. • Meningkatkan mitigasi dan	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
			recovery untuk keamanan siber.	
3	Berdasarkan laporan terbaru International Monetary Fund (IMF), ekonomi global mengalami perlambatan yang signifikan. Proyeksi pertumbuhan ekonomi global (Global GDP Growth) telah direvisi turun dari 3,3% menjadi 2,8% untuk tahun 2025. Tren penurunan ini terlihat jelas dari data historis yang menunjukkan perlambatan dari 6% pada 2021 menjadi 3,5% pada 2022, kemudian 3,2% pada 2023, dan konsisten di angka 3,2% pada 2024. Faktor utama penyebab perlambatan ini adalah meningkatnya ketegangan perdagangan global dan ketidakpastian kebijakan ekonomi antar negara.	Perlambatan ekonomi global pada tahun 2025 semakin dirasakan dampaknya oleh Indonesia melalui beberapa indikator ekonomi utama. Neraca perdagangan yang sebelumnya surplus mulai menunjukkan tekanan, investasi asing cenderung melambat, dan daya beli masyarakat mengalami penurunan.	Perlambatan ekonomi berdampak langsung pada pengurangan alokasi anggaran untuk keamanan siber, sementara ancaman siber justru meningkat. BSSN perlu mengembangkan strategi yang lebih efisien dan inovatif untuk melindungi infrastruktur digital nasional dengan sumber daya yang terbatas. Diperlukan pendekatan berbasis prioritas risiko, peningkatan kerja sama dengan sektor swasta, dan optimalisasi teknologi automasi untuk efisiensi operasional. Selain itu, BSSN perlu memperkuat kapasitas mitigasi dan pemulihan (recovery) untuk mengantisipasi meningkatnya celah keamanan siber akibat keterbatasan ekonomi dan menanggulangi berbagai bentuk kejahatan siber yang muncul dalam situasi ekonomi yang menantang.	T
		Situasi ini berpotensi meningkatkan kejahatan siber karena keterbatasan ekonomi mendorong aktivitas ilegal di ruang digital, yang dapat merugikan individu, sektor bisnis, dan instansi	Munculnya berbagai celah keamanan siber akibat peningkatan potensi kejahatan siber.	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
		pemerintah. Perusahaan dan lembaga publik cenderung mengurangi anggaran untuk keamanan siber ketika menghadapi tekanan ekonomi.		
4	Pasar Asuransi Siber. Pertumbuhan pasar asuransi siber menunjukkan peningkatan kesadaran tentang risiko siber dan kebutuhan untuk perlindungan finansial terhadap serangan tersebut. Asuransi ini dapat membantu perusahaan mengatasi dampak finansial dari serangan siber.	• Pertumbuhan pasar asuransi siber di Indonesia mencerminkan peningkatan kesadaran dan literasi masyarakat serta perusahaan terhadap risiko siber, yang mendorong adopsi langkah-langkah proaktif dalam manajemen risiko digital. Hal ini menjadi indikator positif bagi kematangan ekosistem digital nasional. • Asuransi siber berperan penting sebagai instrumen transfer risiko yang efektif untuk mengurangi dampak ekonomi dari serangan siber bagi perusahaan dan individu. Dengan mekanisme perlindungan finansial ini, bisnis dapat pulih lebih cepat dari insiden siber, meminimalisasi gangguan operasional, dan mencegah kebangkrutan	BSSN perlu beradaptasi dan memperkuat kerja sama strategis dengan industri asuransi siber untuk memastikan standarisasi produk asuransi siber di pasar Indonesia. Sebagai otoritas keamanan siber nasional, BSSN berpeluang mengembangkan kerangka regulasi dan standar minimum keamanan siber yang dapat diadopsi sebagai persyaratan polis asuransi siber. Kolaborasi ini juga memungkinkan BSSN mengakses data dan wawasan berharga mengenai tren serangan siber dari klaim asuransi, yang dapat dimanfaatkan untuk memperkuat sistem peringatan dini nasional. Dengan pendekatan integratif antara regulasi keamanan siber dan insentif finansial melalui asuransi, BSSN dapat mendorong kepatuhan yang lebih luas terhadap standar keamanan siber nasional.	P

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
		akibat serangan siber yang merugikan. • Peningkatan adopsi asuransi siber mendorong implementasi standar keamanan siber yang lebih tinggi di berbagai sektor, karena perusahaan asuransi umumnya mensyaratkan pemenuhan kontrol keamanan tertentu. Kondisi ini secara tidak langsung meningkatkan postur keamanan siber nasional dan mendukung terciptanya stabilitas ekonomi digital Indonesia.		
5	Ekonomi Pasar Gelap Siber. Terdapat ekonomi bawah tanah yang berkembang di sekitar kejahatan siber, termasuk penjualan alat dan layanan yang digunakan dalam serangan siber, serta penjualan data yang dicuri.	• Penjualan data pribadi dan bisnis Indonesia di pasar gelap bisa membahayakan privasi dan keamanan warga dan perusahaan Indonesia. • Penggunaan alat dan layanan kejahatan siber yang dijual di pasar gelap bisa meningkatkan frekuensi dan keparahan serangan siber di Indonesia. • Dampak ekonomi dan teknis dari ekonomi pasar gelap siber ini dapat merusak kepercayaan	BSSN perlu meningkatkan kerja sama Internasional karena penanggulangan kejahatan siber memerlukan kerja sama lintas negara. à tantangan dalam hal koordinasi dan hukum internasional.	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/T
		masyarakat dan bisnis dalam teknologi dan ekonomi digital.		
6	Tren terkait *Cryptocurrency*. *Cryptocurrency* sering digunakan sebagai metode pembayaran dalam berbagai jenis kejahatan siber à "cryptojacking", pencurian langsung dari dompet atau bursa *cryptocurrency*, dll.	• Menghambat adopsi dan perkembangan teknologi *blockchain* dan *cryptocurrency* di Indonesia, yang pada gilirannya dapat mempengaruhi inovasi dan pertumbuhan ekonomi di masa depan. • Dampak ekonomi dan teknis, kejahatan ekonomi *Cryptocurrency* ini dapat merusak kepercayaan masyarakat dan bisnis dalam teknologi dan ekonomi digital.	• BSSN perlu meningkatkan kapabilitas dalam hal pengetahuan dan alat untuk menghadapi ancaman yang terkait dengan *cryptocurrency*. • BSSN perlu memperkuat kerja sama dengan lembaga lain baik pemerintah atau swasta baik di dalam dan di luar negeri dalam menanggulangi kejahatan siber terkait dengan *cryptocurrency*.	T
			• BSSN perlu menciptakan regulasi untuk mengatur *cryptocurrency*.	P
7	Peningkatan Ekonomi Digital. Ekonomi digital merujuk kepada aspek ekonomi yang berbasis pada teknologi digital, termasuk *e-commerce, digital marketing, fintech*, dan lainnya. Ekonomi digital telah berkembang pesat dan membawa perubahan besar pada berbagai sektor, termasuk sektor Usaha Mikro, Kecil, dan Menengah (UMKM) dan iklim usaha secara umum.	Kementerian/Lembaga yang bertanggung jawab terhadap sektor ekonomi digital dan kewirausahaan telah memasukkan program-program ekonomi digital, namun belum memasukkan aspek keamanan siber.	BSSN bisa menyelenggarakan program peningkatan kompetensi terkait keamanan digital dan sertifikasi keamanan digital.	P

Dalam era digital saat ini, nilai ekonomi data telah mengalami peningkatan yang signifikan. Digitalisasi yang terus berkembang telah menjadikan data sebagai aset yang sangat berharga. Data ini dapat digunakan untuk berbagai tujuan, mulai dari analisis bisnis yang mendalam hingga penargetan iklan yang lebih efektif. Karena pentingnya data ini, terjadi peningkatan motivasi ekonomi untuk melakukan serangan siber. Para pelaku serangan siber melihat peluang untuk mencuri data dan menjualnya di pasar gelap atau menggunakan informasi tersebut untuk keuntungan finansial, seperti melalui penipuan atau pemerasan dengan *ransomware*.

Dampak dari fenomena ini terhadap keamanan nasional sangat signifikan. Serangan siber tidak hanya mengancam privasi individu, tetapi juga keamanan dan stabilitas ekonomi sebuah negara. Oleh karena itu, BSSN sebagai lembaga yang bertanggung jawab atas keamanan siber di Indonesia, perlu mengambil langkah-langkah strategis untuk menghadapi tantangan ini.

Pertama, BSSN perlu meningkatkan upaya deteksi dan pencegahan serangan siber, baik terhadap masyarakat umum maupun instansi pemerintah. Ini melibatkan investasi yang lebih besar dalam teknologi keamanan siber dan sumber daya manusia yang terlatih. Selain itu, peningkatan kerja sama dengan lembaga lain, baik di dalam maupun luar negeri, sangat penting untuk memperkuat sistem keamanan siber nasional.

Kedua, BSSN perlu meningkatkan *information sharing* atau berbagi informasi, baik di dalam organisasi maupun dengan *stakeholder* lainnya. Pertukaran informasi tentang ancaman siber terbaru dan cara-cara penanganannya sangat penting untuk membangun pertahanan yang lebih kuat terhadap serangan siber.

Ketiga, mengembangkan dan menerapkan kebijakan baru untuk menangani peningkatan ancaman yang berkaitan dengan data menjadi

penting. Kebijakan ini harus mencakup aspek hukum, teknis, dan operasional dalam rangka mengamankan data nasional.

Terakhir, BSSN perlu melakukan edukasi kepada masyarakat dan instansi pemerintah tentang pentingnya keamanan siber. Kesadaran tentang bagaimana melindungi data pribadi dan instansi sangat penting untuk mencegah serangan siber.

Kejahatan siber merupakan salah satu tantangan terbesar di era digital ini, tidak hanya karena dampaknya yang langsung terhadap korban, tetapi juga karena kerugian ekonomi yang signifikan yang dapat ditimbulkannya. Kerugian ini tidak hanya berupa pencurian uang atau data secara langsung, tetapi juga mencakup kerugian tidak langsung seperti kerusakan reputasi, penurunan kepercayaan dari publik dan pelaku bisnis, serta biaya yang harus dikeluarkan untuk pemulihan dari serangan tersebut.

Dalam konteks ini, BSSN memiliki tanggung jawab besar dalam melindungi ruang siber Indonesia dari ancaman kejahatan siber yang terus meningkat. Untuk menghadapi tantangan ini, BSSN perlu melakukan beberapa langkah strategis:

a. Peningkatan Dana dan Kompetensi SDM: BSSN perlu meningkatkan anggaran dan sumber daya manusia yang kompeten dalam bidang keamanan siber. Hal ini penting untuk memastikan BSSN memiliki kapasitas yang cukup untuk menghadapi ancaman siber yang semakin kompleks.
b. Peningkatan Kerja sama dengan Entitas Lain: Kerja sama dengan berbagai pihak seperti penyedia layanan keamanan siber (*managed service*), perusahaan asuransi siber, dan lembaga internasional sangat penting. Kerja sama ini dapat membantu dalam pertukaran informasi, pengembangan strategi keamanan yang lebih efektif, dan pemulihan cepat pasca-serangan.

c. Perubahan Strategi atau Kebijakan: BSSN perlu meninjau dan memperbarui strategi atau kebijakan keamanan siber untuk menyesuaikan dengan perkembangan terbaru dalam taktik dan teknik yang digunakan oleh pelaku kejahatan siber.
d. Edukasi Masyarakat dan Organisasi: Memastikan bahwa masyarakat dan organisasi di Indonesia memahami risiko kejahatan siber dan bagaimana menanggapinya adalah kunci.
e. Meningkatkan Mitigasi dan *Recovery*: BSSN perlu mengembangkan dan menerapkan strategi mitigasi yang efektif untuk mengurangi dampak serangan siber. Selain itu, rencana pemulihan yang cepat dan efisien sangat penting untuk meminimalisasi kerugian ekonomi dan reputasi pasca-serangan.

Secara keseluruhan, kejahatan siber bukan hanya masalah keamanan siber semata, tetapi juga masalah ekonomi nasional. Oleh karena itu, respons yang komprehensif dan terkoordinasi dari BSSN sangat penting untuk melindungi kepentingan nasional Indonesia di ruang siber.

Dunia saat ini sedang menghadapi tantangan berupa perlambatan ekonomi. Perlambatan ekonomi global ini juga mulai berdampak pada Indonesia, yang terlihat dari beberapa indikator ekonomi seperti neraca perdagangan. Dampak dari perlambatan ekonomi ini tidak hanya terbatas pada aspek ekonomi makro, tetapi juga pada alokasi anggaran untuk berbagai sektor, termasuk keamanan siber. Dalam konteks ini, BSSN sebagai lembaga yang bertanggung jawab atas keamanan siber di Indonesia, berpotensi menghadapi tantangan dalam bentuk anggaran yang lebih terbatas. Hal ini memerlukan BSSN untuk mencari cara yang lebih efisien dan efektif dalam melindungi ruang siber Indonesia, mengingat keamanan siber adalah aspek kritikal yang tidak bisa diabaikan.

Salah satu dampak langsung dari perlambatan ekonomi adalah peningkatan potensi kejahatan siber. Situasi ekonomi yang sulit sering kali

mendorong peningkatan aktivitas ilegal, termasuk kejahatan siber. Kejahatan siber tidak hanya merugikan individu, tetapi juga perusahaan dan lembaga pemerintah, dengan kerugian yang bisa mencakup pencurian data, penipuan finansial, dan gangguan operasional. Dalam kondisi ekonomi yang turun, perusahaan dan individu mungkin mengurangi pengeluaran untuk keamanan siber, yang ironisnya meningkatkan kerentanan mereka terhadap serangan.

Dengan meningkatnya potensi kejahatan siber, muncul pula berbagai celah keamanan yang perlu ditangani. BSSN perlu mengantisipasi hal ini dengan strategi yang lebih adaptif dan responsif.

Pasar asuransi siber telah mengalami pertumbuhan. Hal ini mencerminkan peningkatan kesadaran terhadap risiko siber dan kebutuhan akan perlindungan finansial terhadap serangan siber. Asuransi siber ini memainkan peran penting dalam strategi manajemen risiko perusahaan, dengan menyediakan perlindungan finansial untuk membantu mengatasi dampak dari serangan siber.

Di Indonesia, pertumbuhan pasar asuransi siber ini merupakan indikator positif dari peningkatan kesadaran masyarakat dan perusahaan terhadap risiko siber. Hal ini menunjukkan bahwa semakin banyak entitas yang menyadari pentingnya perlindungan terhadap ancaman siber dan bersedia untuk menginvestasikan sumber daya dalam mengelola risiko tersebut. Dari perspektif nasional, ini adalah perkembangan yang menggembirakan karena dapat membantu mengurangi dampak ekonomi dari serangan siber. Dengan adanya asuransi siber, perusahaan dan individu dapat lebih terlindungi dari kerugian finansial yang mungkin terjadi akibat serangan siber, yang pada gilirannya dapat membantu menjaga stabilitas ekonomi Indonesia.

Dalam konteks ini, BSSN perlu beradaptasi dengan perkembangan pasar asuransi siber dan bekerja sama dengan sektor asuransi untuk

memastikan bahwa produk asuransi siber yang ditawarkan di pasar sesuai dengan standar dan kebijakan keamanan siber yang berlaku. Kerja sama ini bisa mencakup beberapa aspek:

a. Pengaturan dan Standarisasi: BSSN dapat berperan dalam membantu menetapkan standar atau pedoman untuk produk asuransi siber, memastikan bahwa mereka menawarkan perlindungan yang memadai dan sesuai dengan risiko siber yang dihadapi oleh perusahaan dan individu di Indonesia.
b. Edukasi dan Kesadaran: BSSN dapat bekerja sama dengan perusahaan asuransi untuk meningkatkan edukasi dan kesadaran tentang pentingnya asuransi siber. Ini termasuk menyebarkan informasi tentang manfaat asuransi siber dan bagaimana itu dapat menjadi bagian dari strategi manajemen risiko yang komprehensif.
c. Data dan Analisis Risiko: BSSN dapat berbagi wawasan dan data tentang ancaman siber yang terjadi, yang dapat digunakan oleh perusahaan asuransi untuk mengembangkan produk yang lebih sesuai dengan kebutuhan pasar.

Ekonomi pasar gelap siber merupakan fenomena global yang berkembang dan memiliki dampak signifikan, termasuk di Indonesia. Di pasar gelap siber ini, terjadi penjualan alat dan layanan yang digunakan dalam serangan siber, serta penjualan data yang dicuri, termasuk data pribadi dan bisnis. Kehadiran pasar gelap ini menunjukkan betapa kompleks dan canggihnya ekosistem kejahatan siber saat ini.

Dampak dari ekonomi pasar gelap siber ini terhadap Indonesia cukup serius. Pertama, penjualan data pribadi dan bisnis Indonesia di pasar gelap dapat membahayakan privasi dan keamanan warga serta perusahaan di Indonesia. Kebocoran data ini tidak hanya melanggar privasi tetapi juga dapat digunakan untuk kejahatan lebih lanjut seperti penipuan, pemerasan, dan serangan siber lainnya. Kedua, penggunaan alat dan

layanan kejahatan siber yang dijual di pasar gelap dapat meningkatkan frekuensi dan keparahan serangan siber di Indonesia. Alat-alat ini memudahkan pelaku kejahatan untuk melancarkan serangan yang lebih canggih dan merusak.

Selain itu, dampak ekonomi dan teknis dari ekonomi pasar gelap siber ini dapat merusak kepercayaan masyarakat dan bisnis dalam teknologi dan ekonomi digital. Ketika kepercayaan terhadap keamanan data dan transaksi *online* menurun, ini dapat menghambat pertumbuhan ekonomi digital dan inovasi teknologi.

Menghadapi tantangan ini, BSSN perlu mengambil langkah-langkah strategis. Salah satu langkah penting adalah meningkatkan kerja sama internasional. Kejahatan siber adalah masalah lintas batas yang memerlukan kerja sama lintas negara untuk penanggulangannya. BSSN perlu bekerja sama dengan lembaga keamanan siber di negara lain, organisasi internasional, serta sektor swasta untuk bertukar informasi, strategi, dan praktik terbaik dalam memerangi kejahatan siber.

Kerja sama internasional ini tidak tanpa tantangan. Terdapat hambatan dalam hal koordinasi dan hukum internasional, mengingat setiap negara memiliki peraturan dan pendekatan yang berbeda terhadap kejahatan siber.

Kejahatan siber yang terkait dengan *cryptocurrency*, seperti "*cryptojacking*", pencurian langsung dari dompet atau bursa *cryptocurrency*, telah menjadi semakin umum. Fenomena ini memiliki beberapa dampak signifikan, baik secara nasional maupun terhadap BSSN di Indonesia.

Dari perspektif nasional, penggunaan *cryptocurrency* dalam kejahatan siber dapat menghambat adopsi dan perkembangan teknologi *blockchain* dan *cryptocurrency* di Indonesia. Ini karena kejahatan tersebut menimbulkan keraguan dan ketidakpercayaan terhadap keamanan dan kestabilan teknologi ini. Hal ini pada gilirannya dapat mempengaruhi

inovasi dan pertumbuhan ekonomi digital di masa depan, mengingat potensi besar yang dimiliki *blockchain* dan *cryptocurrency* dalam berbagai sektor.

Selain itu, dampak ekonomi dan teknis dari kejahatan ekonomi yang berkaitan dengan *cryptocurrency* dapat merusak kepercayaan masyarakat dan bisnis dalam teknologi dan ekonomi digital secara lebih luas. Ketika kepercayaan terhadap sistem keuangan digital menurun, ini dapat menghambat adopsi teknologi baru dan mengurangi investasi dalam inovasi digital.

Menghadapi tantangan ini, BSSN perlu mengambil beberapa langkah strategis. Pertama, BSSN perlu meningkatkan kapabilitasnya dalam hal pengetahuan dan alat untuk menghadapi ancaman yang terkait dengan *cryptocurrency*. Ini termasuk pengembangan keahlian dalam teknologi *blockchain*, analisis transaksi *cryptocurrency*, dan teknik forensik digital untuk melacak dan menginvestigasi kejahatan siber.

Kedua, BSSN perlu memperkuat kerja sama dengan lembaga lain, baik pemerintah atau swasta, baik di dalam maupun di luar negeri, dalam menanggulangi kejahatan siber terkait dengan *cryptocurrency*. Kerja sama ini penting untuk pertukaran informasi, pengembangan strategi bersama, dan koordinasi dalam penanganan insiden.

Terakhir, BSSN perlu berperan aktif dalam proses penciptaan regulasi untuk mengatur *cryptocurrency*. Regulasi ini penting untuk memberikan kerangka kerja hukum yang jelas, yang tidak hanya melindungi konsumen dan investor, tetapi juga membantu dalam pencegahan dan penindakan terhadap kejahatan siber yang berkaitan dengan *cryptocurrency*.

Peningkatan ekonomi digital merujuk pada aspek ekonomi yang berbasis pada teknologi digital seperti *e-commerce, digital marketing, fintech*, dan lainnya. Pertumbuhan ekonomi digital ini membawa perubahan besar

pada berbagai sektor, termasuk sektor Usaha Mikro, Kecil, dan Menengah (UMKM) dan iklim usaha secara umum di Indonesia. Transformasi digital ini membuka peluang besar bagi pertumbuhan ekonomi, inovasi, dan penciptaan lapangan kerja.

Namun, dengan pertumbuhan ekonomi digital, muncul pula tantangan baru, khususnya terkait dengan keamanan siber. Meskipun Kementerian/Lembaga yang bertanggung jawab terhadap sektor ekonomi digital dan kewirausahaan telah memasukkan program-program ekonomi digital, aspek keamanan siber sering kali belum menjadi prioritas utama. Ini menciptakan celah keamanan yang bisa dimanfaatkan oleh pelaku kejahatan siber.

Dalam konteks ini, BSSN dapat mengambil inisiatif untuk menyelenggarakan program peningkatan kompetensi terkait keamanan digital dan sertifikasi keamanan digital.

1.2.3 Teknologi

Analisis eksternal pada faktor teknologi merupakan hal penting untuk diperhatikan. Tujuan dari analisis pada aspek teknologi adalah untuk mengidentifikasi fakta-fakta terkait perkembangan teknologi baik pada skala nasional maupun internasional. Dari fakta-fakta yang telah dikumpulkan pada analisis teknologi, fakta-fakta tersebut akan dikelompokkan apakah fakta tersebut merupakan sebuah potensi (P) atau tantangan (T) bagi BSSN. Berikut adalah analisis beberapa fakta pada aspek teknologi yang telah dilakukan serta dampaknya bagi BSSN.

Tabel 1.11. Analisis Dampak Teknologi

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/ T
1	Maraknya kasus penyebaran tautan dan aplikasi yang dapat mengambi	Meningkatkan risiko bocornya data pribadi yang disebabkan oleh kelalaian	BSSN perlu untuk mengedukasi masyarakat terkait pentingnya mengamankan data	T

	l data pribadi masyarakat serta menginstal aplikasi yang berbahaya di ponsel masyarakat.	masyarakat pada saat menggunakan layanan berbasis elektronik	pribadi saat menggunakan layanan berbasis elektronik.	
			BSSN dapat membuat *platform* untuk mendata tautan resmi dari berbagai penyedia layanan berbasis elektronik agar mencegah terjadinya penyebaran *phising* di masyarakat	P
2	Berkembangnya teknologi kecerdasan buatan yang semakin mudah diakses oleh masyarakat.	Masyarakat Indonesia dapat terbantu dengan pemanfaatan teknologi kecerdasan artifisial untuk berbagai sektor	BSSN perlu untuk mengedukasi masyarakat terkait aspek keamanan data pribadi dalam menggunakan teknologi kecerdasan artifisial.	T
			BSSN perlu untuk membuat tindakan preventif untuk memastikan tidak ada kebocoran data. Karena data yang didapatkan dari hal tersebut dapat digunakan untuk melatih model kecerdasan artifisial.	T
		Pemerintah dapat memanfaatkan teknologi kecerdasan artifisial dalam mendukung pembangunan nasional	BSSN dapat mengoptimalkan pemanfaatan kecerdasan artifisial, khususnya dalam bidang keamanan informasi	P
3	Berkembangnya teknologi quantum yang dapat dimanfaatkan untuk mengamankan informasi melalui metode *Quantum Key Distribution* (QKD)	Perkembangan QKD dapat dimanfaatkan dalam mengamankan informasi yang dikomunikasikan melalui distribusi kunci yang aman di berbagai sektor	BSSN dapat menyusun kajian terkait QKD dalam rangka penyusunan kebijakan teknis dan implementasinya pada layanan distribusi kunci	P

4	Berkembangnya Algoritma *Post Quantum Cryptography* (PQC) diprediksi dapat mengamankan komunikasi dari serangan berbasis teknologi kuantum	Perkembangan Algoritma PQC dapat dimanfaatkan untuk mengamankan komunikasi dari serangan berbasis teknologi kuantum	BSSN dapat menyusun kajian teknis terkait PQC dan perkembangannya, migrasi PQC, dan implementasinya pada Layanan Kriptografi (*cryptography as a service*)	P
5	Berkembangnya layanan komputasi awan *(Cloud Computing)* yang semakin mudah diakses baik oleh masyarakat maupun korporasi	Perkembangan teknologi komputasi awan *(Cloud Computing)* dapat diterapkan di berbagai sektor (pendidikan, keuangan, pertanian, dll) serta keuntungan yang ditawarkan dari perkembangan teknologi ini dapat dirasakan oleh masyarakat maupun korporasi.	BSSN dapat membuat kebijakan untuk mengatur standar keamanan dari layanan komputasi awan yang beroperasi di Indonesia. Serta memastikan bahwa penyedia layanan komputasi awan yang beroperasi di Indonesia tidak menyalahgunakan data masyarakat yang disimpan.	T
6	Berkembangnya teknologi *blockchain* dan web3 yang bersamaan dengan meningkatnya animo masyarakat terhadap aset kripto di Indonesia.	Perkembangan teknologi *blockchain* dan web3 dapat memperjelas lagi utilitas dari inovasi yang sudah ada di aset kripto, salah satunya adalah tokenisasi. Dengan mengadopsi teknologi ini, maka perpindahan kepemilikan suatu aset nyata dapat dilacak.	BSSN dapat terlibat dalam aspek keamanan siber dalam pemanfaatan teknologi *blockchain* dan web3 untuk mendukung pembangunan nasional.	P
			BSSN perlu membuat standar keamanan untuk layanan berbasis *blockchain* dan web3 agar masyarakat dapat menggunakan teknologi ini dengan aman.	T
		Masih minimnya pemahaman masyarakat tentang teknologi *blockchain* dan	BSSN dan regulator aset kripto dapat membuat *framework* regulasi terkait aspek keamanan pada aset	T

		web3. Hal terkait *blockchain* yang dipahami oleh masyarakat masih terbatas pada aset kripto.	kripto serta mengedukasi masyarakat terkait pemahaman untuk mengamankan aset kripto.	
7	Berkembangnya teknologi IOT (*Internet Of Things*) yang memungkinkan masyarakat, institusi, maupun korporasi mengakuisisi data secara *real time.*	Data terkait suatu fenomena dapat langsung dianalisis secara *real time.* Dan data yang telah dianalisis dapat dijadikan acuan untuk membuat kebijakan baik di tingkat masyarakat, pemerintah, maupun korporasi.	BSSN dapat membuat regulasi terkait standar keamanan pada protokol yang digunakan dan data yang telah diakuisisi.	T
		Pemerintah dapat memanfaatkan teknologi *internet of things* untuk mendukung strategi pembangunan nasional	BSSN perlu untuk mengelola dan mengamankan data yang telah didapatkan untuk strategi pembangunan nasional secara berkelanjutan.	T
8	Berkembangnya teknologi komunikasi 5G and next generation yang memberikan peningkatan kecepatan, latensi rendah dan kapasitas jaringan yang lebih besar	Perkembangan Teknologi Komunikasi 5G and next generation dapat dimanfaatkan berbagai sektor namun ancaman dan kerentanan dari teknologi ini juga perlu dianalisis dan diantisipasi	BSSN menyusun kebijakan keamanan teknologi 5G and next generation serta implementasi dan reka gunanya	P
9	Terintegrasinya Teknologi Operasional (TO) yang digunakan di sektor industri dengan TIK	Perkembangan TO menghadirkan manfaat dan juga ancaman juga kerentanan	BSSN menyusun kajian keamanan TO, implementasi serta kajian dan pengembangan penggunaan TO	P

Kaspersky telah mendeteksi dan menggagalkan sebanyak 534.759 serangan phishing keuangan yang menargetkan bisnis di seluruh wilayah Asia Tenggara selama periode Januari hingga Desember 2024. Negara dengan jumlah serangan *phising* tertinggi di kawasan Asia Tenggara adalah Thailand dengan 247.560 serangan, diikuti oleh Indonesia di posisi kedua dengan 85.908 serangan. Metode pencurian data dengan menyebarkan tautan ini dapat disebut sebagai *phising*. Data pribadi dari korban *phising* didapatkan saat korban menekan suatu tautan dan kemudian korban memasukkan data pribadi seperti alamat *email, username, password*, dan data pribadi lainnya. Selain itu dalam beberapa kasus, *link* yang ditekan oleh korban dapat menginstal suatu aplikasi *backdoor* yang dapat mengambil data dari korban tanpa disadari oleh korban.

Pada kasus ini, BSSN perlu untuk mengedukasi masyarakat terkait bentuk kejahatan dalam dunia siber agar masyarakat dapat menjaga data pribadinya dengan lebih hati-hati. Selain itu, BSSN perlu untuk melacak dan menandai lokasi dari pelaku *phising* yang telah merugikan masyarakat. Selain perlu diberikan wewenang untuk menindak, BSSN juga perlu untuk mendata atau memverifikasi *link* dari penyedia layanan berbasis elektronik baik dari pemerintahan atau korporasi.

Selain kasus penyebaran tautan berbahaya. Saat ini sedang berkembang teknologi kecerdasan buatan yang semakin mudah diakses oleh banyak kalangan dengan biaya yang murah. Berdasarkan riset dari PWC, penggunaan kecerdasan buatan dapat meningkatkan GDP global sebesar 14% hingga tahun 2030. Hal tersebut terjadi karena penggunaan kecerdasan buatan dapat meningkatkan produktivitas bisnis dengan mengotomasi banyak proses dan meningkatkan tenaga kerja yang ada. Kedua, penggunaan kecerdasan buatan dapat memberikan rekomendasi produk yang dapat dibuat sesuai dengan kebutuhan pengguna dan pelanggan.

Semakin masifnya penggunaan teknologi kecerdasan buatan ini. BSSN perlu untuk mengedukasi masyarakat terkait aspek keamanan data pribadi pada saat menggunakan teknologi kecerdasan buatan ini. Karena model kecerdasan buatan yang digunakan oleh masyarakat akan dilatih dan disesuaikan dengan perilaku dari masyarakat dan pengguna. Sehingga BSSN dirasa perlu untuk mengedukasi masyarakat dalam aspek pengamanan data pribadi. Selain itu, BSSN perlu untuk memastikan tidak ada kebocoran data dan penyalahgunaan data pribadi dari masyarakat pada layanan berbasis elektronik baik yang dimiliki oleh pemerintah maupun korporasi. Namun, BSSN juga dapat memanfaatkan teknologi ini untuk mendukung program pembangunan nasional khususnya dalam membuat kebijakan, regulasi dan mekanisme yang mengatur tata kelola, implementasi keamanan kecerdasan artifisial.

Keamanan siber tidak dapat lepas dari kriptografi. Hal tersebut sesuai dengan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional (SKSN). Pada dokumen SKSN, pasal 11 dinyatakan tentang kemandirian kriptografi nasional yang meliputi: penetapan kebijakan kriptografi nasional; peningkatan riset pengembangan dan inovasi di bidang kriptografi untuk mendukung pembangunan nasional; penerapan kebijakan kriptografi nasional pada pemangku kepentingan; serta pembangunan dan pengembangan industri kriptografi nasional. Dalam rangka penjabaran amanat untuk menyusun kebijakan kriptografi nasional, pada tahun 2024 BSSN telah menetapkan Peraturan BSSN Nomor 11 Tahun 2024 tentang Penyelenggaraan Algoritma Kriptografi dan Penilaian Kesesuaian Keamanan Modul Kriptografi. Pada peraturan tersebut mengatur dua hal, yaitu mengenai kriteria algoritma kriptografi yang dibedakan berdasarkan kategorisasi sistem elektronik dan penilaian kesesuaian untuk modul kriptografi untuk jaminan keamanan sebuah produk. Kriptografi dan teknologi lain yang terus berkembang perlu disikapi BSSN dengan melakukan kajian teknis keamanan dan implementasinya.

Perkembangan teknologi kuantum yang menggunakan prinsip mekanika kuantum telah diimplementasikan para peneliti maupun industri dengan melakukan pengembangan komputer kuantum. Komputer kuantum merupakan jenis komputer yang menggunakan teknologi kuantum untuk memproses informasi dengan prinsip yang berbeda dari komputer klasik. Hal ini memungkinkan komputer kuantum melakukan banyak operasi secara paralel dalam satu waktu bersamaan, memecahkan permasalahan yang sangat kompleks seperti faktorisasi bilangan besar dengan waktu yang jauh lebih cepat dengan komputer klasik. Teknologi kuantum memungkinkan efisiensi dan kecepatan dalam proses pembelajaran mesin dan kecerdasan artifisial, terutama dalam analisis data besar dan pengenalan pola yang rumit, pengenalan suara dan bahasa, deteksi anomali dan analisis data medis. Selain memberikan banyak peluang, teknologi ini juga diprediksi dapat memecahkan algoritma persandian/ kriptografi klasik.

Perkembangan teknologi kuantum dalam mengamankan komunikasi diimplementasikan dalam *Quantum Key Distribution* (QKD). QKD merupakan metode keamanan yang menggunakan prinsip fisika kuantum untuk mengamankan komunikasi. Dengan QKD kedua pihak yang berkomunikasi dapat berbagi kunci enkripsi secara aman sehingga aspek konfidensialitas tercapai. Keunggulan penerapan QKD adalah jika ada pihak ketiga yang mencoba menyadap atau mencuri kunci selama proses, percobaan tersebut akan langsung terdeteksi karena hukum fisika kuantum dapat memastikan bahwa pengamatan atau interaksi terhadap data akan mengubah kondisi kunci itu sendiri, sehingga komunikasi akan tetap aman.

Dengan menggunakan nano satelit, teknologi QKD dapat diimplementasikan secara lebih ekonomis dan fleksibel, memungkinkan distribusi kunci enkripsi kuantum secara aman di seluruh dunia. Contoh pemanfaatannya adalah Distribusi Kunci Kuantum Global, Keamanan

Komunikasi yang Tinggi, Efisiensi dan Biaya Rendah, Konstelasi Nano Satelit dan eksperimen serta pengembangan teknologi. Komputer kuantum berpotensi untuk memecahkan algoritma kriptografi klasik, seperti Algoritma Kunci Publik RSA, dan *Elliptic Curve Cryptography* (ECC) dengan cepat menggunakan algoritma Shor's yang dapat menghancurkan keamanan algoritma kriptografi klasik yang sampai saat ini digunakan secara luas di berbagai sektor. *Post quantum cryptography* (PQC) hadir sebagai solusi menghadapi serangan komputer kuantum. PQC merupakan cabang kriptografi yang berfokus pada pengembangan algoritma kriptografi yang aman dari serangan komputer kuantum. PQC menggunakan teknik kriptografi, di antaranya *lattice-based cryptography*, *hash-based cryptography* dan *code-based cryptography*.

Perkembangan teknologi informasi dan komunikasi di Indonesia juga mendorong perkembangan teknologi *blockchain* dan web3. *Blockchain* merupakan teknologi pembukuan atau pencatatan dari perpindahan suatu aset digital dari seorang pemilik ke pemilik lainnya yang direpresentasikan melalui suatu alamat publik ke alamat publik lainnya. Data dari *blockchain* tidak disimpan di satu entitas terpusat melainkan data tersebut disimpan di komputer yang tidak terpusat sehingga data bersifat lebih transparan dan terdesentralisasi.

Future Market Insights memproyeksikan pertumbuhan pasar Web 3.0 Blockchain diperkirakan akan mencapai USD 229,15 miliar pada tahun 2034, didorong oleh CAGR sebesar 44,90% dari 2024 hingga 2034. Pertumbuhan ini didorong oleh peningkatan adopsi teknologi blockchain oleh institusi, perkembangan platform *peer-to-peer*, dan kerangka regulasi yang semakin matang.

Hal tersebut juga diperkuat dengan pasar kripto Indonesia yang menunjukkan pertumbuhan yang luar biasa sepanjang tahun 2024. Data terbaru per Oktober 2024 mengungkapkan bahwa jumlah trader kripto di

Indonesia telah mencapai angka 21 juta orang, menjadikan Indonesia sebagai salah satu negara dengan basis investor kripto terbesar di kawasan Asia Pasifik. Pertumbuhan ini tidak hanya terlihat dari jumlah investor, tetapi juga dari nilai transaksinya. Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti) mencatat lonjakan signifikan pada nilai transaksi kripto di Indonesia pada Maret 2024, yang mencapai Rp103,58 triliun, meningkat tajam sebesar 207,5% dibandingkan bulan Februari 2024 yang hanya sebesar Rp33,69 triliun.

Mayoritas pengguna kripto di Indonesia adalah generasi muda, dengan lebih dari 60% investor berusia antara 18-30 tahun. Hal ini mencerminkan tingginya minat dan literasi digital di kalangan generasi muda Indonesia terhadap aset digital sebagai instrumen investasi alternatif dan teknologi *blockchain*.

Dalam menghadapi teknologi ini, BSSN perlu untuk membuat standarisasi dalam aspek keamanan data untuk layanan elektronik yang menggunakan teknologi *blockchain* maupun web 3 agar masyarakat dapat memanfaatkan teknologi ini dengan baik sehingga dapat mempercepat pertumbuhan ekonomi. Selain itu, BSSN perlu untuk berkolaborasi dengan regulator aset kripto untuk membuat regulasi terkait keamanan baik keamanan pada saat penyimpanan aset kripto maupun keamanan data dan kode program yang dibuat pada sebuah aset kripto. Namun, BSSN dapat berkolaborasi dengan pemangku kepentingan lainnya untuk memanfaatkan teknologi ini untuk mendukung pembangunan nasional dan mempercepat pertumbuhan ekonomi.

Selain perkembangan teknologi *blockchain* dan web 3. Perkembangan teknologi dan informasi juga mendorong adopsi *Internet Of Things* (IoT) di Indonesia. IoT banyak digunakan dalam kehidupan sehari-hari baik dalam skala rumah tangga seperti *smart home* sampai di fasilitas publik seperti di jembatan yang dilengkapi dengan sensor untuk mengetahui kondisi

materialnya secara *real time* sehingga biaya perawatan jembatan dapat diestimasi. Saat ini, teknologi IoT sudah berkembang sampai ke transportasi dengan masifnya pengembangan sarana transportasi tanpa awak seperti *drone* dan sarana transportasi seperti mobil yang dapat dikendalikan secara otomatis.

Menurut Fortune Business Insights, ukuran pasar IoT global dinilai sebesar USD 595,73 miliar pada 2023 dan diproyeksikan tumbuh dari USD 714,48 miliar pada 2024 menjadi USD 4.062,34 miliar pada 2032, dengan CAGR sebesar 24,3% selama periode perkiraan.

Dalam menghadapi perkembangan teknologi IoT, BSSN perlu untuk membangun regulasi dan standarisasi dari aspek keamanan data pada sebuah perusahaan atau layanan yang menggunakan teknologi IoT. BSSN juga perlu untuk memastikan bahwa data yang dikumpulkan melalui protokol yang digunakan tidak disalahgunakan oleh perusahaan atau penyedia layanan. Namun, BSSN dapat berkolaborasi dengan para pemegang kepentingan lainnya untuk mengadopsi teknologi ini dari sisi keamanan data untuk mendukung program pembangunan nasional dan pertumbuhan ekonomi.

Teknologi 5G telah hadir sejak 2019 secara global dan Indonesia sudah mulai mengadopsi sejak pertengahan 2021. 5G mengenalkan berbagai kemampuan baru serta membawa perubahan dalam penyelenggaraan dan pengelolaan jaringan. Termasuk di antaranya virtualisasi dan kontainerisasi, virtualisasi fungsi jaringan (*Network Function Virtualization* - NFV), perangkat lunak *open source*, jaminan keamanan, keamanan O-RAN, *network slicing*, jaringan *programmable*, dan lain-lain. Berdasarkan riset dari Institut Teknologi Bandung (ITB), pengembangan jaringan 5G di Indonesia berpotensi menyumbang lebih dari 2.800 triliun rupiah atau setara dengan 9,5 persen dari total PDB di tahun

2030. Angka ini bahkan bisa meningkat menjadi 3.500 triliun rupiah atau setara dengan 9,8 persen dari total PDB Indonesia di tahun 2035 .

Menurut studi IHS Markit, pada tahun 2035, 5G dapat berkontribusi pada *output* ekonomi global sebesar USD 13,2 triliun. Sementara, Arthur D. Little memperkirakan di era Revolusi Industri 4.0, nilai IoT yang didukung 5G akan mencapai USD 1,5 triliun pada tahun 2030 . Oleh karena itu, penerapan 5G merupakan langkah penting dalam revolusi industri dan harus dilakukan dengan tepat.

Meskipun transisi ke 5G menghadirkan banyak peluang dan kemampuan, transisi ini juga memperkenalkan berbagai kerentanan (*vulnerability*) dan ancaman (*threat*) keamanan siber yang baru. 5G adalah bentuk konvergensi antara dunia telekomunikasi dan Teknologi Informasi (TI), sehingga banyak isu keamanan baru yang tadinya hanya dikenal di dunia TI kini juga menjadi tantangan dalam pengamanan 5G. Pengembangan kebijakan dan standar 5G berfungsi sebagai fondasi untuk mengamankan infrastruktur komunikasi 5G di masa depan dan program serta kontrol keamanan 5G yang baru telah dikembangkan untuk mengamankan sistem 5G. Keamanan siber adalah topik yang sangat penting, dan menjadi landasan dalam proses pengembangan ekosistem 5G. Walaupun pada saat ini implementasi 5G masih dalam tahap pengembangan, pengkajian dan implementasi lanjutan pada teknologi 5.5 G bahkan sampai pada 6G sudah mulai dilakukan.

Keamanan siber tidak hanya terkait infrastruktur berbasis teknologi informasi (IT) saja, untuk sektor industri harus memperhatikan pula perangkat pendukung bisnis proses yang berbasis teknologi operasional (TO). TO adalah perangkat keras dan perangkat lunak yang digunakan untuk mendeteksi atau mengontrol perubahan fisik melalui perangkat,sistem, dan proses industri. TO sering digunakan dalam infrastruktur penting seperti pabrik, sistem transportasi, dan utilitas energi

untuk mengelola perangkat fisik seperti katup, mesin, dan sensor. Berbeda dengan teknologi informasi (IT) yang berfokus pada data, TO berfokus pada pengoperasian dan pengendalian perangkat fisik di lingkungan industri. Dibutuhkan kebijakan Keamanan, implementasi, riset, kajian dan pengembangan.

Insiden siber yang melibatkan TO di sektor industri terus meningkat dan menjadi perhatian besar. Berikut adalah beberapa insiden penting yang perlu diperhatikan dalam menjaga keamanan siber untuk TO, antara lain: Serangan *Ransomware* di Industri Maritim di mana produsen teknologi maritim Brunswick Corporation menghadapi serangan *ransomware* yang menunjukkan kerentanan dalam segmentasi jaringan TO yang mengakibatkan gangguan operasi dan kerugian hingga USD 85 juta. Kemudian Eksploitasi Perangkat Wireless yaitu Grup ancaman VOLTZITE mengeksploitasi perangkat Sierra Wireless Airlink milik entitas pengelola lalu lintas di AS. Serangan ini menunjukkan bagaimana perangkat yang terhubung internet menjadi pintu masuk bagi penyerang. Serangan LockBit 3.0 pada Boeing : Eksploitasi celah keamanan Citrix Bleed digunakan untuk menyerang sistem distribusi suku cadang Boeing, menyebabkan gangguan operasi yang signifikan. Dan untuk serangan yang terjadi secara rutin, studi menunjukkan bahwa 26% organisasi industri mengalami serangan setiap minggu, dengan ancaman yang meningkat dari AI dan 5G sebagai vektor risiko baru. Insiden-insiden ini menegaskan perlunya investasi besar dalam keamanan OT, terutama di sektor industri yang strategis, untuk menerapkan langkah-langkah pencegahan seperti: melakukan segmentasi jaringan dengan memastikan pemisahan antara jaringan OT dan IT untuk mencegah penyebaran *malware* di seluruh sistem operasi, melakukan pemantauan dan pembatasan komunikasi keluar dengan mengontrol komunikasi keluar dari perangkat TO untuk mencegah akses jarak jauh yang tidak sah dan eksfiltrasi data, Integrasi Keamanan IT dan TO untuk mengatasi konflik antara tim IT dan TO untuk menciptakan solusi

keamanan terpadu, serta melakukan pelatihan kesadaran keamanan dan evaluasi dan adaptasi berkelanjutan.

Selain beberapa teknologi di atas, perkembangan penggunaan teknologi informasi dan komunikasi di Indonesia juga mendorong penggunaan layanan komputasi awan (*cloud computing*). Berdasarkan data dari *markets and markets*, permintaan terhadap layanan komputasi awan meningkat seiring dengan berkembangnya ide dari perusahaan untuk menyediakan produk atau layanannya yang sesuai dengan masyarakat. Selain itu, keandalan dari layanan komputasi awan juga cenderung untuk bertumbuh. Teknologi ini juga dapat meningkatkan efisiensi untuk membangun infrastruktur teknologi informasi dan komunikasi dengan biaya yang lebih efisien dengan adanya sistem *pay as you go*.

Menurut laporan terbaru dari The Insight Partners, pasar cloud computing global diprediksi akan mencapai nilai USD 1465,82 miliar pada tahun 2028, dengan tingkat pertumbuhan tahunan majemuk (CAGR) yang mengesankan sebesar 23,9% selama periode perkiraan 2022-2028. Pertumbuhan signifikan ini didorong oleh adopsi teknologi cloud yang semakin meluas di berbagai industri seperti BFSI (perbankan, keuangan, dan asuransi), teknologi informasi, kesehatan, pemerintahan, dan media.

Dalam menghadapi perkembangan teknologi *cloud computing*, BSSN perlu untuk membuat regulasi dan standar keamanan dari layanan komputasi awan khususnya yang beroperasi di Indonesia. Serta BSSN harus memastikan bahwa layanan komputasi awan yang beroperasi di Indonesia tidak menyalahgunakan data pengguna yang disimpan di servernya. Namun, BSSN dapat memanfaatkan teknologi ini dari aspek keamanan data untuk mendukung program pembangunan nasional dan mencerdaskan masyarakat Indonesia terkait teknologi ini untuk mendorong pertumbuhan ekonomi.

1.2.4 Perubahan Lingkungan Hidup

Perubahan lingkungan hidup merupakan faktor eksternal yang juga tidak kalah penting untuk dianalisis. Analisis perubahan lingkungan hidup bertujuan untuk mengidentifikasi fakta-fakta terkait perubahan lingkungan hidup dan dampaknya di skala nasional (sektor teknologi informasi) dan dampaknya terhadap BSSN. Dari analisis dampak perubahan lingkungan hidup tersebut akan ditentukan apakah fakta-fakta yang terjadi tersebut menjadi potensi (P) atau tantangan (T) bagi BSSN. Perubahan lingkungan hidup mengacu pada perubahan kondisi dan kualitas lingkungan. Perubahan lingkungan yang dianalisis seperti: degradasi tanah, polusi udara dan air, serta perubahan iklim yang disebabkan oleh aktivitas manusia dan faktor alami. Berikut adalah hasil analisis dampak dari fakta-fakta perubahan lingkungan hidup terhadap BSSN.

Tabel 1.12. Analisis Dampak Perubahan Lingkungan Hidup

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/ T
1	Terjadinya bencana alam seperti banjir, badai, gelombang panas, kekeringan, gempa bumi, dll.	Potensi kerusakan pada peralatan/ infrastruktur TIK akibat bencana alam	• Bencana alam dapat merusak peralatan dan infrastruktur TIK yang dimiliki oleh BSSN. • Ketersediaan *(availability)* dan keandalan *(reliability)* layanan data dan TIK akan menurun à baik layanan yang diberikan kepada internal BSSN maupun kepada Masyarakat.	T
		Bencana alam dapat menyebabkan gangguan jaringan komunikasi seperti kabel serat optik, satelit, menara nirkabel (BTS/ *tower* jaringan), dan lainnya.	Gangguan jaringan komunikasi dapat: • memengaruhi aksesibilitas dan kinerja layanan data dan TIK, • menyebabkan latensi, kehilangan (sinyal/jaringan), atau gangguan layanan.	T

No	Fakta	Dampak Nasional	Dampak Terhadap BSSN	P/ T
2	Terjadinya fenomena perubahan iklim, krisis energi, dan polusi lingkungan di seluruh dunia	Mulai munculnya tren *green* IT sebagai respons terhadap tantangan global yang dihadapi oleh dunia, seperti perubahan iklim, krisis energi, dan polusi lingkungan	• BSSN perlu mengikuti perkembangan teknologi yang lebih hemat energi dan ramah lingkungan, seperti *chip* yang lebih efisien, sistem heterogen, komputasi awan, virtualisasi, dan kontainerisasi	P
			• BSSN perlu memperhatikan desain dan optimasi pendinginan pusat data, mengurangi penggunaan bahan berbahaya atau langka dalam pembuatan dan pembuangan sistem IT, dan meningkatkan daur ulang sistem IT yang sudah usang	P
			• BSSN perlu mengembangkan dan menerapkan kebijakan dan standar keamanan siber dan sandi yang sesuai dengan prinsip-prinsip *green* IT	P
			• BSSN perlu memberikan edukasi dan sosialisasi kepada masyarakat tentang pentingnya *green* IT dan dampaknya terhadap lingkungan, serta cara-cara untuk menerapkan *green* IT dalam kehidupan sehari-hari	P

Fakta perubahan lingkungan hidup yang pertama yaitu: terjadinya bencana alam seperti banjir, badai, gelombang panas, kekeringan, gempa bumi, dll. Bencana alam tersebut dapat merusak peralatan dan infrastruktur TIK, seperti *server, router*, sakelar, kabel, dan lainnya, sehingga menyebabkan kegagalan fungsi atau kerusakan pada peralatan dan infrastruktur TIK tersebut. Hal ini tentunya dapat mempengaruhi ketersediaan *(availability)* dan keandalan *(reliability)* layanan data dan TIK BSSN, serta mengakibatkan penurunan layanan, kerusakan/kehilangan data, pemadaman listrik, atau gangguan lainnya. Contoh konkret dampak terjadinya bencana alam terhadap peralatan dan infrastruktur TIK terjadi pada tahun 2012, di mana Badai Sandy menyebabkan pemadaman listrik

dan banjir yang meluas di Pantai Timur AS, serta merusak banyak pusat data dan jaringan komunikasi di sana.

Bencana alam juga dapat menyebabkan gangguan jaringan komunikasi, seperti kerusakan pada kabel serat optik dan menara nirkabel (BTS/*tower* jaringan), gangguan satelit, dll. Gangguan jaringan komunikasi tersebut dapat menyebabkan hilangnya konektivitas jaringan atau sinyal. Hal ini dapat memengaruhi aksesibilitas dan kinerja layanan data dan TIK BSSN, serta mengakibatkan latensi, kehilangan (sinyal/jaringan), atau gangguan terhadap layanan (internal dan eksternal) yang diberikan oleh BSSN. Contoh konkret dampak terjadinya bencana alam yang menyebabkan gangguan terhadap jaringan komunikasi terjadi pada tahun 2006, di mana gempa bumi di Taiwan berdampak pada rusaknya beberapa kabel bawah laut dan mengganggu layanan internet dan telepon di Asia.

Fakta lain yang disebabkan oleh perubahan lingkungan hidup adalah fenomena perubahan iklim, krisis energi, dan polusi lingkungan yang sedang terjadi di seluruh dunia. Faktor lingkungan hidup seperti perubahan iklim, polusi, bencana alam, dll., dapat meningkatkan risiko serangan siber, karena dapat menciptakan peluang bagi penyerang *(hacker/attacer)* untuk mengeksploitasi kerentanan atau kelemahan sistem atau jaringan TI. Penyerangan tersebut dapat memanfaatkan pemadaman listrik atau gangguan jaringan yang disebabkan oleh faktor lingkungan untuk melancarkan serangan *malware, ransomware, DDoS,* atau *phishing*. Serangan siber yang dilakukan oleh *hacker/attacker* tersebut membahayakan keamanan data yang dimiliki oleh BSSN dan juga berdampak pada fungsionalitas sistem informasi dan layanan yang diberikan oleh BSSN. Dengan demikian, serangan siber terhadap BSSN dapat menyebabkan kerugian, baik *tangible* maupun *intangible.*

Potensi terjadinya bencana alam dan fenomena perubahan iklim yang sedang terjadi dapat menyebabkan rusaknya peralatan/infrastruktur TIK,

gangguan terhadap jaringan komunikasi yang dimiliki BSSN, dan memberikan peluang kepada *hacker/ attacker* untuk melakukan serangan siber terhadap BSSN merupakan ancaman *(threat)* yang harus dapat dimitigasi oleh BSSN. Hal ini perlu dilakukan agar BSSN dapat menghindari atau setidaknya dapat mengurangi dampak negatif yang akan dialami oleh BSSN dari terjadinya bencana alam.

Fenomena perubahan iklim, krisis energi, dan polusi lingkungan di seluruh dunia memaksa dunia untuk merespons dengan menemukan solusi untuk menanggulangi dampak yang ditimbulkannya. Salah satunya adalah mulai populernya tren *green* IT sebagai respons terhadap tantangan global yang dihadapi oleh dunia, seperti perubahan iklim, krisis energi, dan polusi lingkungan. *Green* IT merupakan istilah yang mengacu pada penggunaan teknologi informasi dan komunikasi (ICT) yang ramah lingkungan. Tujuan dari *Green* IT adalah untuk mengurangi dampak negatif dari sistem ICT terhadap lingkungan, seperti emisi karbon, konsumsi energi, dan limbah elektronik. *Green* IT juga berusaha untuk meningkatkan keberlanjutan dengan menggunakan ICT untuk mendukung praktik bisnis yang hemat sumber daya dan efisien. *Green* IT juga mencakup pemilihan bahan baku yang bersumber secara berkelanjutan, mengurangi limbah elektronik, dan meningkatkan keberlanjutan melalui penggunaan sumber daya terbarukan. Popularitas penerapan *green* IT memberikan peluang *(opportunity; O)* bagi BSSN untuk turut serta berkontribusi dalam menanggulangi permasalahan perubahan iklim global. Berikut adalah peluang yang dapat diterapkan oleh BSSN:

1. Aspek teknis: BSSN perlu mengikuti perkembangan teknologi yang lebih hemat energi dan ramah lingkungan, seperti menggunakan *chip* yang lebih efisien, sistem heterogen, komputasi awan, virtualisasi, dan kontainerisasi. Hal ini dapat membantu BSSN mengurangi konsumsi energi dan emisi karbon dari sistem IT yang digunakan, baik di pusat data maupun di perangkat pengguna. BSSN juga perlu memperhatikan

desain dan optimisasi pendinginan pusat data, mengurangi penggunaan bahan berbahaya atau langka dalam pembuatan dan pembuangan sistem IT, dan meningkatkan daur ulang sistem IT yang sudah usang.

2. Aspek strategis: BSSN perlu mengembangkan dan menerapkan kebijakan dan standar keamanan siber dan sandi yang sesuai dengan prinsip-prinsip *green* IT, seperti mengurangi jejak karbon, meningkatkan efisiensi energi, dan mempromosikan ICT yang keberlanjutan. Hal ini dapat membantu BSSN meningkatkan reputasi dan kredibilitas sebagai lembaga pemerintah yang peduli terhadap lingkungan, sekaligus melindungi kepentingan nasional di bidang siber dan sandi. BSSN juga perlu berkolaborasi dengan pihak-pihak terkait, seperti pemerintah, industri, akademisi, dan masyarakat, untuk meningkatkan kesadaran dan partisipasi dalam upaya *green* IT.
3. Aspek sosial: BSSN perlu memberikan edukasi dan sosialisasi kepada masyarakat tentang pentingnya *green* IT dan dampaknya terhadap lingkungan, serta cara-cara untuk menerapkan *green* IT dalam kehidupan sehari-hari. Hal ini dapat membantu BSSN membangun hubungan yang baik dengan masyarakat, serta meningkatkan literasi dan keterampilan masyarakat di bidang IT, siber, dan sandi. BSSN juga perlu memberikan contoh dan inspirasi kepada masyarakat tentang bagaimana *green* IT dapat memberikan manfaat bagi kehidupan, kesejahteraan, dan kemajuan bangsa.

BAB II
VISI, MISI, TUJUAN, DAN SASARAN STRATEGIS BSSN

2.1 Visi BSSN 2025-2029

Berdasarkan lampiran Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional (Permen PPN/Bappenas) nomor 10 tahun 2023 tentang Tata Cara Penyusunan Rencana Strategis Kementerian/Lembaga tahun 2025-2029, Visi merupakan gambaran umum mengenai keadaan yang ingin dicapai oleh Kementerian/Lembaga pada akhir periode perencanaan. Selain itu, Visi juga harus memberikan gambaran konsistensi kinerja Kementerian/Lembaga selama 5 (lima) tahun mendatang serta gambaran menyeluruh mengenai peranan dan fungsi suatu organisasi.

Presiden dan Wakil Presiden menetapkan Visi Presiden tahun 2025-2029 yang kemudian dituangkan dan diimplementasikan dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) tahun 2025-2029 berdasarkan Peraturan Presiden (Perpres) Nomor 12 tahun 2025 tentang Rencana Pembangunan Jangka Menengah Nasional. Visi Indonesia tahun 2025-2029 tersebut adalah:

"Bersama Indonesia Maju Menuju Indonesia Emas 2045"

Berdasarkan RPJMN 2025-2029, Visi Presiden ini mengandung arti pembangunan memerlukan kerja sama seluruh putra-putri terbaik bangsa dengan kesamaan tekad berdasarkan

fondasi yang telah dibangun oleh pemerintah sebelumnya untuk mewujudkan Indonesia setara negara maju di tahun 2045.

Dalam menghadapi berbagai tantangan dan memanfaatkan berbagai peluang yang dimiliki BSSN ke depan, serta dalam mendukung terwujudnya Visi Presiden yang diamanatkan melalui RPJMN tahun 2025-2029, maka Visi BSSN dalam Rencana Strategis (Renstra) BSSN tahun 2025-2029 adalah:

"BSSN menjadi PERISAI
Bagi Keamanan Siber dan Sandi Negara Dalam Rangka
Mewujudkan Indonesia Maju Menuju Indonesia Emas 2045"

Visi BSSN tahun 2029 ini menjadi arah BSSN dalam melaksanakan kebijakan, strategi, program maupun kegiatan selama tahun 2025-2029. Visi BSSN ini mengandung beberapa kata kunci penting yang dapat dijabarkan sebagai berikut:

- Kata kunci 1: BSSN menjadi PERISAI Bagi Keamanan Siber dan Sandi Negara Dalam Rangka Mendukung Penyelenggaraan Pemerintahan

  BSSN menjadi PERISAI Keamanan Siber dan Sandi Negara dalam rangka mendukung penyelenggaraan pemerintahan mengandung makna bahwa BSSN merupakan penggerak utama dalam melindungi keamanan siber dan sandi nasional. Dalam konteks ini, BSSN berperan sebagai *leading sector* di bidang keamanan dan ketahanan siber dan sandi guna mendukung terwujudnya transformasi digital nasional yang aman. Sebagai penanggung jawab utama, BSSN memimpin

upaya perlindungan terhadap keamanan dan ketahanan siber dan sandi nasional melalui sinergi dan kolaborasi lintas sektor. Kolaborasi ini melibatkan Kementerian/ Lembaga, Lembaga Pemerintah Non Kementerian (LPNK), lembaga non-struktural, lembaga independen, Badan Usaha Milik Negara (BUMN), Badan Usaha Milik Daerah (BUMD), pelaku usaha di sektor swasta, serta masyarakat luas.

Dalam pelaksanaan tugasnya, BSSN bertanggung jawab merumuskan kebijakan dan tata kelola keamanan serta ketahanan siber dan sandi nasional yang diimplementasikan di seluruh sektor, baik pemerintahan maupun swasta. Praktik-praktik yang dikembangkan BSSN akan menjadi *best practices* bagi instansi pemerintah dan sektor privat, sekaligus menjadi acuan dalam menjaga keamanan siber dan sandi secara nasional. Dengan demikian, BSSN juga berperan sebagai pembina dalam pelaksanaan keamanan dan ketahanan siber dan sandi nasional, guna memastikan kontribusinya terhadap pencapaian tujuan pembangunan nasional. Peran ini menandai revitalisasi posisi BSSN, dari sebelumnya sebagai pendukung menjadi aktor utama dalam bidang keamanan siber dan sandi.

Dalam mendukung visi di atas, BSSN menerapkan sistem nilai PERISAI yang mencakup Profesional, Elaboratif, Responsif, Integratif, Solid, Akuntabel dan Inovatif. Sistem nilai BSSN PERISAI mencerminkan budaya organisasi yang bertujuan untuk memperkuat pembentukan ciri khas karakter dan identitas pegawai BSSN sebagai penjaga ruang siber Indonesia. Implementasi sistem nilai BSSN PERISAI dilaksanakan selaras dengan Core Value ASN Berakhlak sebagai fondasi utama. Dengan menerapkan nilai-nilai

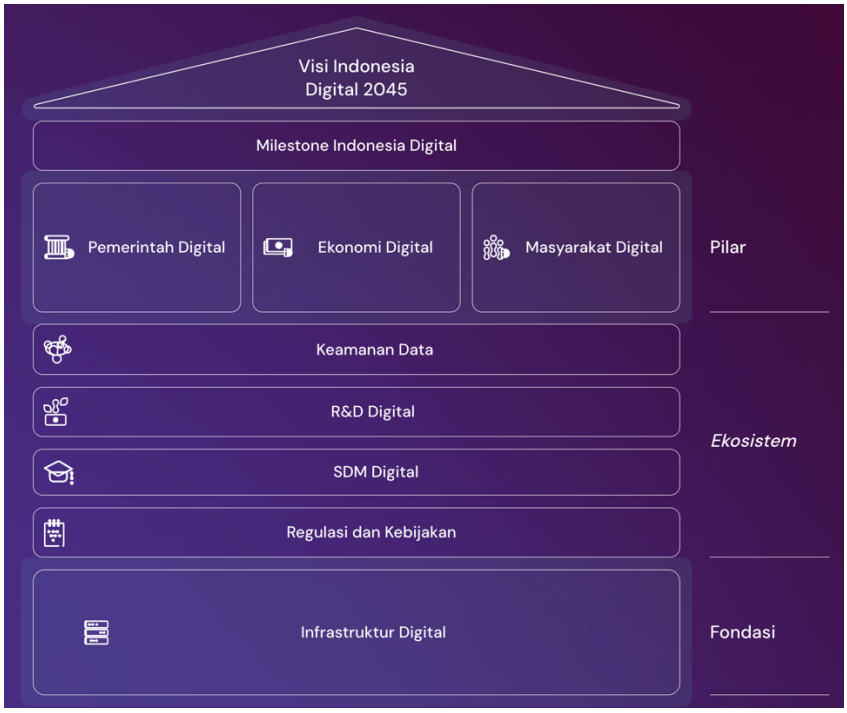
PERISAI, diharapkan BSSN dapat terus meningkatkan kinerja dan kontribusinya dalam menjaga keamanan siber dan informasi nasional.

Sesuai RPJPN tahun 2025-2045, untuk mewujudkan Visi Indonesia Emas 2045, keberhasilan transformasi menyeluruh baik di tataran nasional maupun daerah perlu didukung oleh penciptaan supremasi hukum, demokrasi substansial, keamanan nasional, stabilitas ekonomi, serta diplomasi tangguh sebagai faktor pemampu. Keamanan nasional diarahkan menuju keselamatan bangsa, kedaulatan dan keutuhan wilayah Negara Kesatuan Republik Indonesia yang aman, damai, serta aktif menjaga perdamaian dunia. Untuk mencapai sasaran tersebut di bidang keamanan siber dan sandi, diperlukan arah kebijakan terkait penguatan keamanan siber antara lain meliputi, perlindungan warga negara di ranah siber melalui pengaturan tata kelola pertanggungjawaban pemilik sistem elektronik serta transformasi tata kelola keamanan siber yang proaktif dan terintegrasi di tingkat individu, masyarakat, bangsa dan negara, dan kolaborasi identifikasi, proteksi, deteksi, respons, dan pemulihan insiden siber nasional.

Dalam dokumen RPJMN 2025-2029 transformasi digital menjadi salah satu fokus pemerintah. Transformasi digital merupakan elemen kunci pendorong birokrasi yang transparan, inklusif, efisien, dan akuntabel. Transformasi digital layanan publik dalam pemerintah digital diarahkan untuk meningkatkan aksesibilitas dan kualitas layanan kepada masyarakat. Upaya tersebut tentunya harus didukung dengan teknologi yang andal, data yang terintegrasi dan aman,

kompetensi sumber daya manusia yang tinggi, serta layanan publik yang modern sehingga pemerintah digital dapat memberikan kontribusi nyata pada pencapaian tujuan utama pembangunan nasional.

Visi Indonesia Digital tahun 2045 (VID 2045) telah ditetapkan oleh Kementerian Komunikasi dan Digital dalam mendukung terwujudnya Indonesia Emas tahun 2045. Kerangka strategis dalam mewujudkan VID 2045 dapat digambarkan pada gambar berikut ini.



Gambar 2.1. Visi Indonesia Digital tahun 2045 (sumber: https://digital2045.id/)

Pada gambar di atas dapat dilihat bahwa dalam mencapai Visi Indonesia Digital tahun 2045, maka perlu diwujudkan *milestone* Indonesia digital yang akan dibagi menjadi beberapa tahap. *Milestone* tersebut akan diwujudkan melalui 3 (tiga) pilar digital, yaitu (i) pemerintah digital, (ii) ekonomi digital serta (iii)

masyarakat digital. Ketiga pilar ini berdiri di atas ekosistem digital yang meliputi (i) keamanan data, (ii) *Research and Development* (R&D), (iii) Sumber Daya Manusia (SDM) digital serta (iv) regulasi dan kebijakan. Fondasi digital yaitu infrastruktur digital sangat dibutuhkan untuk menopang ekosistem digital di atasnya. Selain itu, dalam Rancangan Akhir RPJPN tahun 2025-2045 disebutkan bahwa *cybersecurity* serta *Research and Development* (R&D) menjadi *enabler* dalam mewujudkan transformasi digital.

BSSN memiliki peran strategis sebagai penjaga utama keamanan digital nasional. Keberadaan BSSN sangat vital dalam memastikan bahwa setiap lapisan pilar digital, baik pemerintah digital, ekonomi digital, maupun masyarakat digital beroperasi dalam lingkungan siber yang aman, terpercaya, dan tangguh. BSSN bertanggung jawab mengembangkan dan menerapkan standar keamanan data nasional, membina kesiapsiagaan siber lintas sektor, serta mengoordinasikan respons terhadap insiden siber berskala nasional. Selain itu, BSSN juga diharapkan berperan aktif dalam mendukung pengembangan talenta keamanan siber *(cybersecurity talent)*, memperkuat kemampuan deteksi dan respons dini terhadap ancaman digital, serta mendorong kolaborasi global guna mengantisipasi risiko keamanan siber lintas batas negara. Dengan demikian, BSSN bukan hanya menjadi pelindung, tetapi juga *enabler* yang mendorong pertumbuhan transformasi digital nasional secara berkelanjutan dan aman menuju Indonesia Emas 2045.

- Kata kunci 2 : Bersama Indonesia Maju Menuju Indonesia Emas tahun 2045

  Makna kata kunci ini sebenarnya adalah memasukkan Visi Presiden terpilih pada saat Presiden terpilih sudah dilantik dan sudah menetapkan Visi sebagai kebijakan yang dituangkan dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) tahun 2025-2029. Berdasarkan Perpres nomor 12 tahun 2025 tentang RPJMN, maka Visi Presiden adalah "Bersama Indonesia Maju Menuju Indonesia Emas 2045" beserta makna yang telah dijelaskan sebelumnya.

  Sehingga secara keseluruhan, Visi BSSN ini mengandung makna bahwa BSSN akan menjadi *leading sector* di bidang keamanan dan ketahanan siber dan sandi dalam mencapai transformasi digital yang aman, baik pada pilar digital, ekosistem digital maupun fondasi digital dalam mendukung terwujudnya Visi Presiden terpilih yang tertuang dalam RPJMN tahun 2025-2029. Hal ini merupakan penguatan peran BSSN sekaligus penguatan keamanan dan ketahanan siber dan sandi dalam menghadapi tantangan digitalisasi ke depan.

2.2 Misi BSSN 2025-2029

RPJMN 2025-2029 telah menetapkan Misi Pembangunan Nasional yang dituangkan ke dalam delapan Asta Cita Presiden dalam mewujudkan Visi Presiden tahun 2025-2029, yaitu:

1. Memperkokoh Ideologi Pancasila, demokrasi dan Hak Asasi Manusia (HAM)
2. Memantapkan sistem pertahanan keamanan negara dan mendorong kemandirian bangsa melalui swasembada pangan,

energi, air, ekonomi syariah, ekonomi digital, ekonomi hijau dan ekonomi biru

3. Melanjutkan pengembangan infrastruktur dan meningkatkan lapangan kerja yang berkualitas, mendorong kewirausahaan, mengembangkan industri kreatif, serta mengembangkan agromaritim industri di sentra produksi melalui peran aktif koperasi
4. Memperkuat pembangunan Sumber Daya Manusia (SDM), sains, teknologi, pendidikan, kesehatan, prestasi olahraga, kesetaraan gender, serta penguatan peran perempuan, pemuda (generasi milenial dan generasi Z), dan penyandang disabilitas
5. Melanjutkan hilirisasi dan mengembangkan industri berbasis sumber daya alam untuk meningkatkan nilai tambah di dalam negeri
6. Membangun dari desa dan dari bawah untuk pertumbuhan ekonomi, pemerataan ekonomi dan pemberantasan kemiskinan
7. Memperkuat reformasi politik, hukum dan birokrasi, serta memperkuat pencegahan dan pemberantasan korupsi, narkoba, judi, dan penyelundupan
8. Memperkuat penyelarasan kehidupan yang harmonis dengan lingkungan, alam dan budaya, serta peningkatan toleransi antar umat beragama untuk mencapai masyarakat yang adil dan makmur

Misi BSSN tahun 2025-2029 merupakan upaya strategis yang harus dilakukan BSSN dalam mewujudkan Visi BSSN tahun 2029. Misi BSSN juga merupakan penjabaran dari Asta Cita

Presiden yang sesuai dengan tugas dan fungsi BSSN. Misi BSSN tersebut adalah:

1. Misi 1: Mengoptimalkan ketahanan dan keamanan siber dan sandi nasional

   Misi pertama adalah mengoptimalkan ketahanan dan keamanan siber dan sandi nasional. Misi ini merupakan upaya strategis yang dilakukan untuk memastikan berjalannya proses identifikasi, deteksi, proteksi, penanggulangan, pemulihan dan pemantauan keamanan siber dan keamanan informasi. Pada misi ini juga dipastikan pemanfaatan dan kemandirian kriptografi dalam meningkatkan keamanan siber nasional.

2. Misi 2: Meningkatkan dampak langsung reformasi birokrasi BSSN bagi masyarakat

   Misi kedua adalah meningkatkan dampak langsung reformasi birokrasi BSSN bagi masyarakat. Misi ini terkait tata kelola pemerintahan BSSN menuju *good government governance*. Misi ini juga merupakan bagian dari pelaksanaan penajaman Reformasi Birokrasi Nasional (RBN) yang menekankan pada dampak penyelenggaraan reformasi birokrasi bagi masyarakat melalui reformasi birokrasi tematik dan mengurangi aspek administratif (hulu) yang selama ini menjadi acuan utama pelaksanaan reformasi birokrasi.

2.3 Tujuan BSSN 2025 – 2029

Tujuan merupakan visi yang dipersempit yang menggambarkan kondisi yang ingin dicapai dalam mewujudkan visi serta melaksanakan misi BSSN. Tujuan dipetakan

berdasarkan Misi BSSN tahun 2025-2029 dalam mewujudkan Visi BSSN tahun 2029. Tujuan BSSN tahun 2025-2029 dapat dijabarkan sebagai berikut:

1. Tujuan 1: Meningkatnya tata kelola keamanan siber dan sandi Indonesia

   Tujuan pertama adalah meningkatnya tata kelola keamanan siber dan sandi Indonesia dengan 2 (dua) Indikator Tujuan (IT), yaitu:

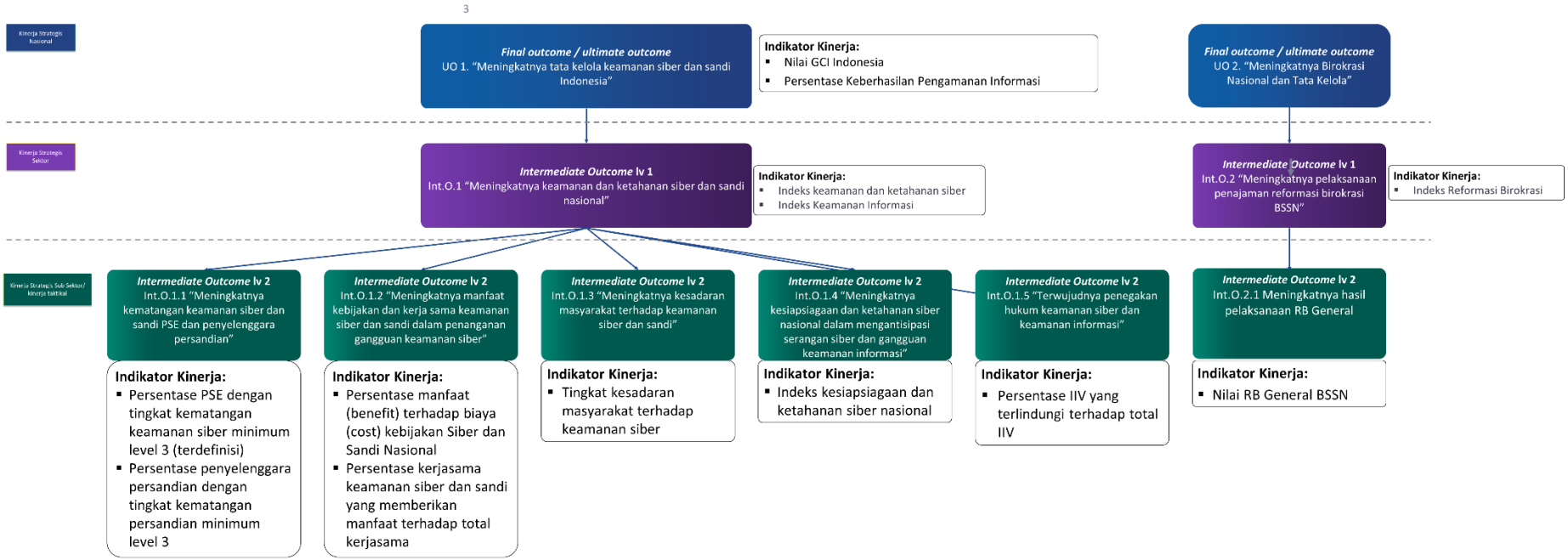
   - IT.1.1 “Nilai Global Cybersecurity Index (GCI) Indonesia”. GCI merupakan indeks keamanan siber global yang diukur oleh International Telecomunication Union (ITU). Indikator ini menggambarkan adanya komitmen Indonesia dalam rangka penguatan keamanan siber tahun 2025-2029. Tujuan ini merupakan bentuk dipersempit dari Visi BSSN dan mendukung upaya strategis pada Misi 1 BSSN yaitu “Mengoptimalkan ketahanan dan keamanan siber dan sandi nasional”. Target indikator tujuan ini adalah 98,6 pada tahun 2029.
   - IT 1.2 “Persentase Keberhasilan Pengamanan Informasi”. Indikator Tujuan ini menggambarkan tingkat keberhasilan pengamanan informasi yang dilakukan BSSN atas permintaan Presiden dan/atau kebutuhan nasional melalui berbagai media komunikasi. Target indikator tujuan ini adalah 97,50% pada tahun 2029.

2. Tujuan 2: Meningkatnya hasil pelaksanaan reformasi birokrasi BSSN

Tujuan kedua adalah meningkatnya hasil pelaksanaan reformasi birokrasi BSSN. Tujuan ini mendukung Misi 2 yaitu "Meningkatkan dampak langsung reformasi birokrasi BSSN bagi masyarakat". Tujuan ini diukur dengan Indikator Tujuan 2.1 (IT 2.1) yaitu "Tren peningkatan nilai reformasi birokrasi BSSN". IT 2.1 ini mengukur peningkatan nilai reformasi birokrasi selama periode 2025 - 2029. Pertumbuhan ini menggambarkan komitmen BSSN untuk terus melakukan perbaikan penerapan reformasi birokrasi di seluruh aspek, sehingga dapat mendukung terwujudnya reformasi birokrasi nasional. Target indikator tujuan ini adalah 5,35% pada tahun 2029.

2.4 Sasaran Strategis BSSN 2025-2029

Perumusan Sasaran Strategis BSSN didasarkan pada pohon kinerja BSSN. Pohon kinerja menggambarkan kerangka logis penjenjangan kinerja BSSN menggunakan prinsip model logis sesuai ketentuan pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Permen PANRB) nomor 89 tahun 2021 tentang Penjenjangan Kinerja Instansi Pemerintah. Pohon kinerja menggambarkan kinerja yang terdiri dari 5 (lima) jenjang, meliputi (i) Kinerja Strategis Nasional, (ii) Kinerja Strategis Sektor, (iii) Kinerja Strategis Sub Sektor, (iv) Kinerja Taktikal, serta (v) Kinerja Operasional. Pada dokumen Renstra BSSN 2025-2029 ini, disampaikan pohon kinerja BSSN sampai dengan level Kinerja Strategis Sub Sektor.



Gambar 2.2. Pohon Kinerja BSSN sampai Intermediate Outcome Level 2

Berdasarkan gambar di atas, dapat dilihat bahwa pada tahun 2025-2029, BSSN berupaya dalam mewujudkan 2 (dua) *final outcome/ultimate outcome* atau *outcome* akhir. *Final outcome/ ultimate outcome* (UO) pertama adalah UO 1. "Meningkatnya kontribusi dan kualitas keamanan siber dan sandi dalam transformasi perekonomian nasional" dengan 2 (dua) indikator kinerja yaitu Nilai GCI Indonesia dan Persentase Keberhasilan Pengamanan Informasi.

Untuk dapat mewujudkan UO 1, maka *Critical Success Factor* (CSF) yang harus dicapai atau *Intermediate Outcome* level 1 (Int.O) sebagai kinerja strategis sektor adalah Int.O.1 "Meningkatnya keamanan dan ketahanan siber dan sandi nasional". Int.O.1 ini diukur melalui 2 (dua) indikator kinerja, yaitu:

- IK 1. Indeks Keamanan dan Ketahanan Siber
- IK 2. Indeks Keamanan Informasi

Dalam mewujudkan Int.O.1 ini, maka dibutuhkan 5 (lima) CSF sebagai kinerja strategis sub sektor atau *Intermediate Outcome* level 2, meliputi:

- Int.O.1.1 "Meningkatnya kematangan keamanan siber dan sandi PSE dan penyelenggara persandian"
- Int.O.1.2 "Meningkatnya manfaat kebijakan dan kerja sama keamanan siber dan sandi dalam penanganan gangguan keamanan siber"
- Int.O.1.3 "Meningkatnya kesadaran masyarakat terhadap keamanan siber dan sandi"
- Int.O.1.4 "Meningkatnya kesiapsiagaan dan ketahanan siber nasional dalam mengantisipasi serangan siber dan gangguan keamanan informasi"

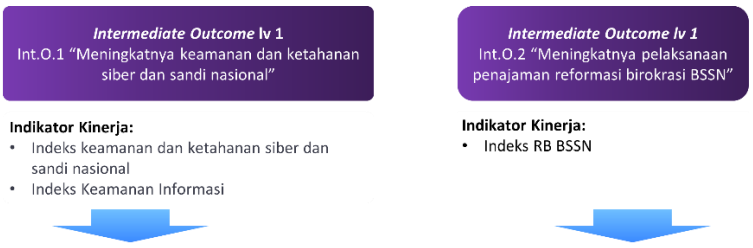
- Int.O.1.5 “Terwujudnya penegakan hukum keamanan siber dan keamanan informasi”.

Penjabaran masing-masing *Intermediate Outcome* level 2 sampai dengan level kinerja taktikal hingga operasional sehingga terbentuk *logic model* dan *crosscutting* dalam mewujudkan UO 1 sebagai tujuan akhir BSSN terdapat dalam dokumen terpisah. Khusus pada Int.O.1.5 “Terwujudnya penegakan hukum keamanan siber dan keamanan informasi” belum diterjemahkan ke dalam sasaran kinerja BSSN maupun dokumen perencanaan BSSN, dikarenakan belum adanya peraturan yang mendukung tugas dan fungsi tersebut.

Selanjutnya *Final outcome/ultimate outcome* kedua adalah UO 2. “Reformasi Birokrasi Nasional dan Tata Kelola” dengan indikator kinerja “Rata-rata nilai RB K/L/D”. Indikator kinerja ini akan diwujudkan melalui CSF sebagai *Intermediate Outcome* level 1, yaitu Int.O.2 “Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN”, dengan indikator kinerja Indeks RB BSSN. Int.O 2 ini akan terwujud melalui capaian pada *Intermediate Outcome* level 2, yaitu Int.O.2.1 “Meningkatnya hasil pelaksanaan RB General”, dengan indikator kinerja Nilai RB General BSSN. Int.O 2.1 ini akan diwujudkan melalui 3 (tiga) kinerja taktikal beserta indikator kinerja dan turunan hingga kinerja operasional. Sehingga terbentuk *logic model* dan *crosscutting* dalam mewujudkan UO 2 sebagai tujuan akhir BSSN.

Kinerja strategis sektor atau *Intermediate Outcome* level 1 akan menjadi dasar acuan dalam menerjemahkan pohon kinerja menjadi standar kinerja Kepala BSSN dalam bentuk Sasaran Strategis (SS) dan Indikator Kinerja Sasaran Strategis (IKSS).

Penerjemahan kinerja strategis sektor pada Pohon Kinerja ke dalam Sasaran Strategis dan Indikator Kinerja Sasaran Strategis BSSN dapat ditunjukkan pada gambar berikut ini.



KODE	SASARAN STRATEGIS	KODE	INDIKATOR KINERJA SASARAN STRATEGIS	SAT	TARGET				
					2025	2026	2027	2028	2029
SS.1	Meningkatnya keamanan dan ketahanan siber dan sandi nasional	IKSS 1.1	Indeks Keamanan dan Ketahanan Siber	Indeks	0,69	0,73	0,76	0,80	0,84
		IKSS 1.2	Indeks Keamanan Informasi	Indeks	0,75	0,78	0,83	0,87	0,90
SS.2	Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN	IKSS 2.1	Indeks Reformasi Birokrasi BSSN	Indeks	90,55	91,22	93,31	94,11	95,29

Gambar 2.3. Penerjemahan Int.O1 dan Int.O2 menjadi SS 1 dan SS 2

Penerjemahan level kinerja strategis sektor dilakukan dengan mengambil seluruh kinerja dan indikator pada level kinerja strategis sektor menjadi SS dan IKSS. Tidak ada perubahan antara kinerja pada pohon kinerja dengan kinerja pada dokumen perencanaan.

Berdasarkan pohon kinerja dan penerjemahan pohon kinerja ke dalam dokumen perencanaan yang telah diuraikan sebelumnya, maka Sasaran Strategis (SS) dan Indikator Kinerja Sasaran Strategis (IKSS) BSSN tahun 2025-2029 adalah:

(1) SS.1 Meningkatnya keamanan dan ketahanan siber dan sandi nasional, dengan IKSS 1.1 Indeks keamanan dan ketahanan siber dan IKSS 1.2 Indeks Keamanan Informasi;
(2) SS.2 Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN, dengan indikator kinerja IKSS 2.1 Indeks Reformasi Birokrasi BSSN.

Peraturan Presiden (Perpres) Nomor 80 Tahun 2025 tentang Penyusunan Rencana Strategis dan Rencana Kerja Kementerian/ Lembaga mengamanatkan bahwa setiap sasaran strategis wajib disertai dengan identifikasi indikasi risiko. Ketentuan ini bertujuan untuk mengenali dan menentukan risiko yang berpotensi memengaruhi pencapaian sasaran strategis BSSN.

Sebagai tindak lanjut, BSSN menerapkan Manajemen Risiko Pembangunan Nasional di bidang keamanan siber dan sandi sebagai upaya mitigasi, penanganan, dan pencegahan risiko yang dapat menghambat pencapaian kinerja pada periode tersebut.

Berdasarkan analisis yang telah dilakukan, maka identifikasi risiko atas sasaran strategis BSSN tahun 2025-2029 dapat diuraikan pada tabel berikut ini.

Tabel 2.1. Identifikasi Risiko pencapaian SS dan IKSS

No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
1	Meningkatnya keamanan dan ketahanan siber dan sandi nasional	1	Tumpang tindih regulasi dan kewenangan K/L terkait keamanan dan ketahanan siber dan sandi	1	Menyusun undang-undang Keamanan dan Ketahanan Siber sebagai payung hukum tertinggi	Direktorat Strategi Keamanan Siber dan Sandi
				2	Membentuk komite penyusunan peraturan perundang-undangan terkait keamanan dan ketahanan siber dan sandi	Direktorat Strategi Keamanan Siber dan Sandi
				3	Menyelenggarakan workshop penyelarasan penyusunan kebijakan/perundang-undangan terkait keamanan dan ketahanan siber dan sandi	Direktorat Strategi Keamanan Siber dan Sandi

No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
				4	Melakukan kajian evaluasi yang menghasilkan rekomendasi kebijakan terkait keamanan dan ketahanan siber dan sandi	- Direktorat Strategi Keamanan Siber dan Sandi - Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi - Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi - Direktorat Kebijakan SDM Keamanan Siber dan Sandi
				5	Menyelenggarakan pelatihan perancangan peraturan perundang-undangan terkait keamanan dan ketahanan siber dan sandi	Pusat Pengembangan Sumber Daya Manusia
		2	Terjadinya kebocoran data elektronik strategis	1	Menyelenggarakan Literasi Kesadaran Keamanan Informasi	Direktorat Operasi Keamanan dan Pengendalian Informasi
				2	Melaksanakan audit kepatuhan keamanan Sistem elektronik	Direktorat Operasi Keamanan dan Pengendalian Informasi
				3	Melaksanakan Monitoring dan Deteksi serangan siber	- Direktorat Operasi Keamanan Siber - Direktorat Operasi Keamanan dan Pengendalian Informasi - Direktorat Operasi Sandi
				4	Menerapkan fungsi kriptografi untuk pengamanan informasi pada sistem elektronik	Direktorat Operasi Sandi
				5	Menerapkan standar keamanan sesuai sistem manajemen keamanan informasi pada sistem elektronik	- Direktorat Operasi Keamanan Siber - Direktorat Operasi Keamanan dan Pengendalian Informasi - Direktorat Operasi Sandi - Pusertif
				6	Melakukan pembinaan kematangan keamanan siber dan sandi PSE	- Direktorat Kebijakan SDM Keamanan Siber dan Sandi - Direktorat Keamanan Siber dan Sandi Pemerintah Pusat

No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
						- Direktorat Keamanan Siber dan Sandi Pemerintah Daerah - Direktorat Keamanan Siber dan Sandi Pembangunan Manusia - Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata - Direktorat Keamanan Siber dan Sandi Energi dan SDA - Direktorat Keamanan Siber dan Sandi Teknologi Informasi Komunikasi, Media dan Transportasi - Direktorat Keamanan Siber dan Sandi Industri - Pusbang SDM
				7	Menyusun rencana mitigasi tanggap darurat kebocoran data	- Direktorat Operasi Keamanan Siber - Direktorat Keamanan Siber dan Sandi Pemerintah Pusat - Direktorat Keamanan Siber dan Sandi Pemerintah Daerah - Direktorat Keamanan Siber dan Sandi Pembangunan Manusia - Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata - Direktorat Keamanan Siber dan Sandi Energi dan SDA - Direktorat Keamanan Siber dan Sandi Teknologi Informasi Komunikasi, Media dan Transportasi - Direktorat Keamanan Siber dan Sandi Industri

No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
		3	Terjadinya insiden siber pada K/L/ D dan PSE	1	Menyelenggarakan Literasi Kesadaran Keamanan Informasi	Direktorat Operasi Keamanan dan Pengendalian Informasi
				2	Melaksanakan Audit kepatuhan keamanan Sistem elektronik	Direktorat Operasi Keamanan dan Pengendalian Informasi
				3	Melaksanakan Monitoring dan Deteksi serangan siber	- Direktorat Operasi Keamanan Siber - Direktorat Operasi Sandi
				4	Menerapkan fungsi kriptografi untuk pengamanan informasi pada sistem elektronik	- Direktorat Operasi Sandi - Pusertif
				5	Menerapkan standar keamanan sesuai sistem manajemen keamanan informasi pada sistem elektronik	- Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi - Direktorat Operasi Keamanan Siber - Pusertif
				6	Melakukan pembinaan kematangan keamanan siber dan sandi PSE	- Direktorat Kebijakan SDM Keamanan Siber dan Sandi - Direktorat Operasi Keamanan Siber - Direktorat Keamanan Siber dan Sandi Pemerintah Pusat - Direktorat Keamanan Siber dan Sandi Pemerintah Daerah - Direktorat Keamanan Siber dan Sandi Pembangunan Manusia - Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata - Direktorat Keamanan Siber dan Sandi Energi dan SDA - Direktorat Keamanan Siber dan Sandi Teknologi Informasi Komunikasi, Media dan Transportasi - Direktorat Keamanan Siber dan Sandi Industri - Pusbang SDM

No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
				7	Menyusun rencana mitigasi penanganan insiden siber pada PSE	Direktorat Operasi Keamanan Siber
		4	Kegagalan dalam menangani insiden siber yang berpotensi menjadi krisis	1	Melaksanakan Monitoring dan Deteksi serangan siber	- Direktorat Operasi Keamanan Siber - Direktorat Operasi Keamanan dan Pengendalian Informasi
				2	Melakukan pembinaan kematangan keamanan siber dan sandi PSE	- Direktorat Operasi Keamanan Siber - Direktorat Keamanan Siber dan Sandi Pemerintah Pusat - Direktorat Keamanan Siber dan Sandi Pemerintah Daerah - Direktorat Keamanan Siber dan Sandi Pembangunan Manusia - Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata - Direktorat Keamanan Siber dan Sandi Energi dan SDA - Direktorat Keamanan Siber dan Sandi Teknologi Informasi Komunikasi, Media dan Transportasi - Direktorat Keamanan Siber dan Sandi Industri
				3	Peningkatan kompetensi SDM Keamanan Siber dan Sandi	- Direktorat Kebijakan SDM Keamanan Siber dan Sandi - Pusbang SDM
				4	Menerapkan standar keamanan sesuai sistem manajemen keamanan informasi pada sistem elektronik	- Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi - Direktorat Operasi Keamanan Siber - Pusertif
				5	Menyusun rencana respon insiden siber dan sandi	Direktorat Operasi Keamanan Siber
				6	Melakukan penguatan infrastruktur keamanan siber	- Direktorat Operasi Keamanan Siber

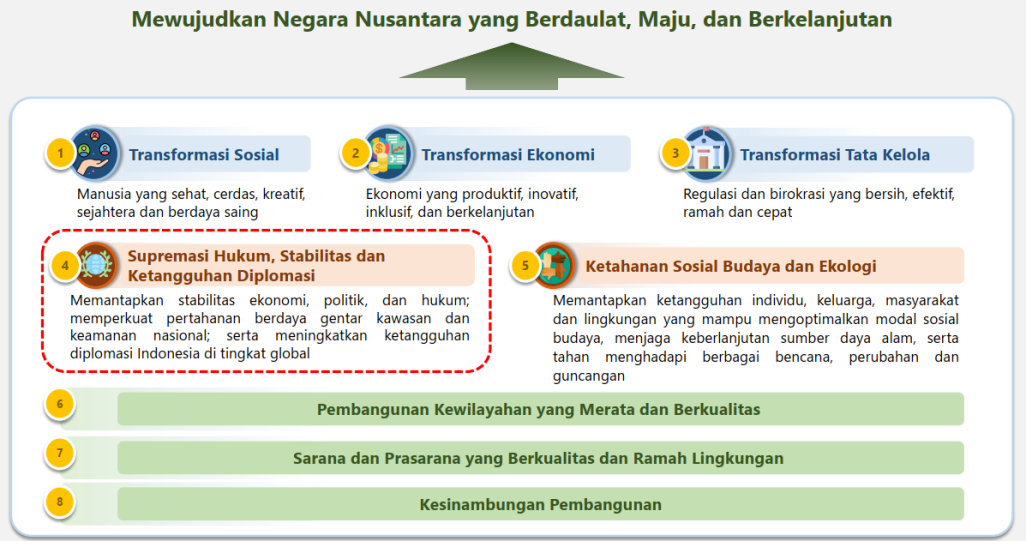
No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
						- Direktorat Operasi Keamanan dan Pengendalian Informasi - Direktorat Operasi Sandi - Balai Sertifikasi Elektronik - Balai Layanan Penghubung Identitas Digital
				7	Melakukan pelindungan IIV	- Direktorat Operasi Keamanan Siber - Direktorat Keamanan Siber dan Sandi Pemerintah Pusat - Direktorat Keamanan Siber dan Sandi Pemerintah Daerah - Direktorat Keamanan Siber dan Sandi Pembangunan Manusia - Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata - Direktorat Keamanan Siber dan Sandi Energi dan SDA - Direktorat Keamanan Siber dan Sandi Teknologi Informasi Komunikasi, Media dan Transportasi - Direktorat Keamanan Siber dan Sandi Industri
2	Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN	1	Menurunnya nilai RB BSSN	1	Melakukan penguatan tata kelola dan kepatuhan internal	- Biro Perencanaan dan Keuangan - Biro Organisasi dan SDM - Biro Hukum dan Komlik - Biro Umum - Pusdatik - Inspektorat
				2	Menerapkan manajemen kinerja melalui program Quick Wins	- Biro Organisasi dan SDM - Biro Perencanaan dan Keuangan

No	Sasaran Strategis	Indikasi Risiko		Perlakuan Risiko		Penanggungjawab Perlakuan Risiko
				3	Mengoptimalkan pemanfaatan teknologi informasi sehingga lebih efisien dan akuntabel	Biro Organisasi dan SDM
				4	Melakukan peningkatan kapasitas SDM dan internalisasi budaya kerja BerAKHLAK	Pusdatik
				5	Melakukan manajemen perubahan dan penguatan komitmen di setiap level organisasi	Biro Organisasi dan SDM
		2	Pelaporan keuangan yang tidak sesuai dengan standar akuntansi pemerintah	1	Melakukan penguatan tata kelola dan kepatuhan internal	- Biro Perencanaan dan Keuangan, - Biro Umum
				2	Meningkatkan kompetensi SDM dalam penyusunan Laporan Keuangan sesuai standar	Biro Perencanaan dan Keuangan,
				3	Mengoptimalkan pemanfaatan teknologi informasi sehingga lebih efisien dan akuntabel	- Biro Perencanaan dan Keuangan - Pusdatik
		3	Terjadinya kasus korupsi dan kecurangan (*fraud*) di lingkungan BSSN	1	Melakukan penguatan tata kelola dan membangun budaya integritas anti korupsi	Inspektorat
				2	Mengoptimalkan pengendalian internal yang efektif melalui sistem pelaporan dan whistleblowing system	Inspektorat
				3	Mengoptimalkan pemanfaatan teknologi informasi sehingga lebih transparan dan akuntabel	- Inspektorat - Pusdatik
				4	Melaksanakan audit dan penegakan hukum	Inspektorat

BAB III
ARAH KEBIJAKAN, STRATEGI, KERANGKA REGULASI, DAN KERANGKA KELEMBAGAAN BSSN

3.1 Arah Kebijakan dan Strategi Nasional

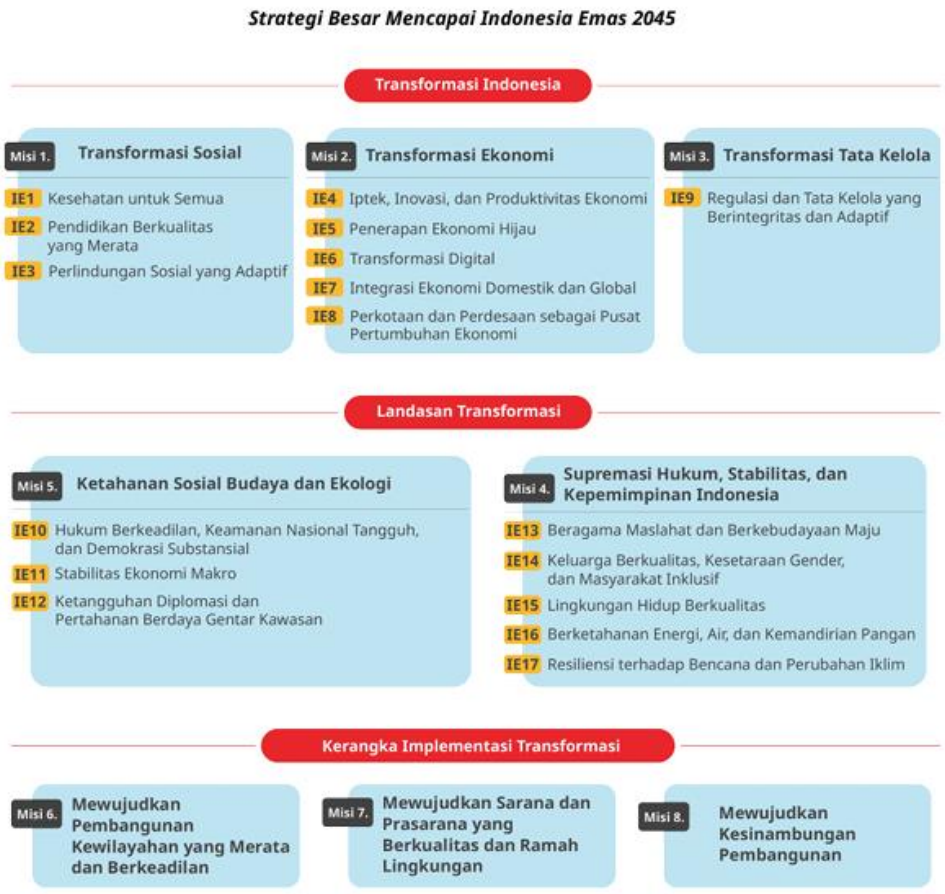
Pelaksanaan perumusan Renstra BSSN 2025 – 2029 dilakukan dengan mengacu pada arah kebijakan dan strategi nasional. Pendekatan *top-down* dari tingkat nasional ke tingkat Kementerian/Lembaga bertujuan untuk menjaga keselarasan dan bentuk akuntabilitas pembangunan nasional. Penyusunan Renstra BSSN 2025-2029 mengacu pada Rencana Pembangunan Jangka Panjang Nasional Tahun 2025-2045 dan Rencana Pembangunan Jangka Menengah Nasional Tahun 2025-2029 (lampiran III).



Gambar 3.4. Agenda Pembangunan RPJPN 2025-2045

Berdasarkan naskah RPJPN 2025 – 2045, tujuan jangka panjang nasional adalah "Indonesia Emas 2045: Negara Berdaulat, Maju, dan Berkelanjutan." Visi tersebut kemudian diterjemahkan ke dalam misi, tujuan, sasaran hingga

transformasi yang perlu dilakukan secara kolektif. Setidaknya terdapat 3 (tiga) transformasi yaitu (1) Transformasi Sosial; (2) Transformasi Ekonomi; (3) Transformasi Tata Kelola; dan 2 (dua) landasan transformasi yaitu, (1) Ketahanan Sosial Budaya dan Ekologi; dan (2) Supremasi Hukum, Stabilitas, dan Kepemimpinan Indonesia yang harus dilakukan untuk mewujudkan Visi Nasional 2045.



Gambar 3.5. Arah Pembangunan Nasional

Berdasarkan transformasi dan landasannya sebagaimana di atas, bidang keamanan siber dan sandi berkontribusi pada (IE).6 Transformasi Digital dan (IE).10 Hukum Berkeadilan, Keamanan Nasional Tangguh, dan Demokrasi Substansial. Pada IE.6, BSSN

berperan dalam membangun kedaulatan digital dengan meningkatkan keamanan dan perlindungan data pribadi serta mewujudkan ruang digital yang kondusif. Sedangkan pada IE. 10, BSSN berperan dalam keamanan siber, sandi dan sinyal dalam rangka penguatan tata kelola, identifikasi, proteksi, deteksi, respons, dan *recovery* yang dilaksanakan melalui:

a. memperkuat keamanan teknologi informasi telekomunikasi;
b. pengembangan sumber daya manusia, peningkatan profesionalisme, dan kesejahteraan sumber daya manusia keamanan siber, sandi, dan sinyal;
c. penguatan kelembagaan keamanan siber, sandi, dan sinyal; serta
d. operasi keamanan siber, sandi, dan sinyal strategis.

Selanjutnya, strategis besar di atas dituangkan ke dalam 8 (delapan) Prioritas Nasional (PN) pembangunan jangka menengah. Sesuai amanat RPJMN tahun 2025-2029, BSSN berkontribusi pada PN 2 dan PN 7 sebagai berikut:

a. Prioritas Nasional 2 pada Program Prioritas: Keamanan Siber, Sandi, dan Sinyal

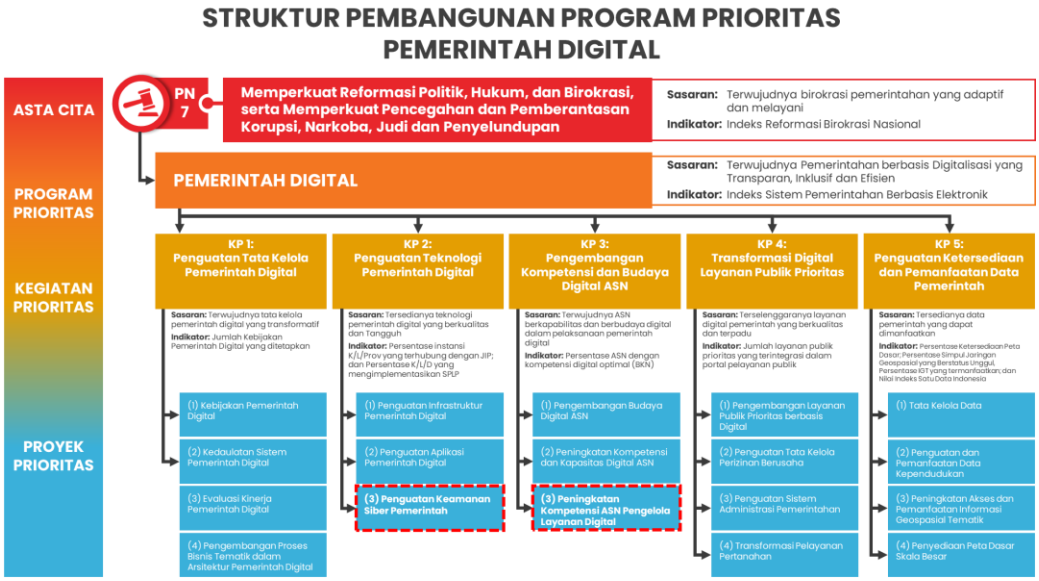
   Tahapan arah kebijakan pembangunan keamanan siber pada periode lima tahun mendatang berfokus pada penguatan fondasi melalui pembangunan ekosistem siber nasional yang tangguh untuk mewujudkan keamanan/ketahanan dan kemandirian ranah siber. Fokus pembangunan tersebut dijabarkan dalam Program Penguatan Siber, Sandi, dan Sinyal dengan sasaran Terwujudnya Interaksi dan Transaksi Siber, Persandian, dan Sinyal yang Aman dengan Indikator *Global Cybersecurity Index* (GCI). Untuk mendukung arah kebijakan

tersebut, BSSN perlu menyusun masukan berupa serangkaian inisiatif strategi yang perlu dilakukan secara terintegrasi, kolaboratif, dan berkelanjutan sehingga tujuan pembangunan nasional dapat tercapai.

Gambar 3.6. Kegiatan BSSN pada Prioritas Nasional 2

b. Prioritas Nasional 7 pada Program Prioritas: Pemerintahan Digital

Tahapan arah kebijakan transformasi digital pelayanan publik diarahkan pada terwujudnya pelayanan publik yang berkualitas dan inklusif dengan didukung penjaminan keamanan siber, informasi, dan sandi.



Gambar 3.7. Kegiatan BSSN pada Prioritas Nasional 7

Bidang keamanan siber dan sandi merupakan *enabler* dalam mendukung penguatan *supply*, penguatan teknologi dan penguatan *demand*. Oleh karena itu, penguatan keamanan siber merupakan salah satu aspek fundamental dalam transformasi digital yang bermuara pada keberhasilan transformasi ekonomi nasional. Agar hal tersebut dapat terwujud, penguatan keamanan siber dilakukan melalui beberapa strategi sebagai berikut.

1. Penguatan Badan Siber dan Sandi Negara (BSSN).
2. Pengembangan regulasi yang ketat seperti Undang-Undang ITE dan peraturan terkait perlindungan data pribadi.
3. Penguatan pendidikan dan pelatihan SDM di bidang keamanan siber.
4. Mendorong investasi dalam teknologi keamanan siber yang lebih canggih untuk melindungi infrastruktur kritis dan menjaga integritas sistem informasi nasional.

Berdasarkan arah kebijakan dan strategi nasional terkait penguatan keamanan siber, BSSN memiliki peran dan kontribusi strategis dalam pembangunan nasional, khususnya terkait transformasi ekonomi serta Supremasi Hukum, Stabilitas, dan Kepemimpinan Indonesia. Ke depan, BSSN harus dengan cermat menentukan *positioning* terkait peran dalam menjaga keamanan siber. Tentunya, hal tersebut dimulai dengan pijakan dan dasar yang kuat, yaitu penerjemahan ke dalam arah kebijakan dan strategi BSSN 2025 – 2029.

Berdasarkan Prioritas Nasional tersebut, maka BSSN berkontribusi secara langsung dalam melaksanakan "Prioritas Nasional 2 : Memantapkan sistem pertahanan keamanan negara dan mendorong kemandirian bangsa melalui swasembada pangan, energi, air, ekonomi kreatif, ekonomi hijau dan ekonomi biru". Namun keamanan siber juga akan berkontribusi secara tidak langsung terhadap seluruh Prioritas Nasional yang telah diuraikan sebelumnya.

Rencana Strategis BSSN tahun 2025-2029 juga selaras dengan RPJMN tahun 2025-2029. Visi dan Misi RPJMN tahun 2025-2029 dijelaskan pada Bab II dapat digambarkan sebagai berikut:

Gambar 3.8. Visi dan Misi (Asta Cita) Presiden RI tahun 2025-2029

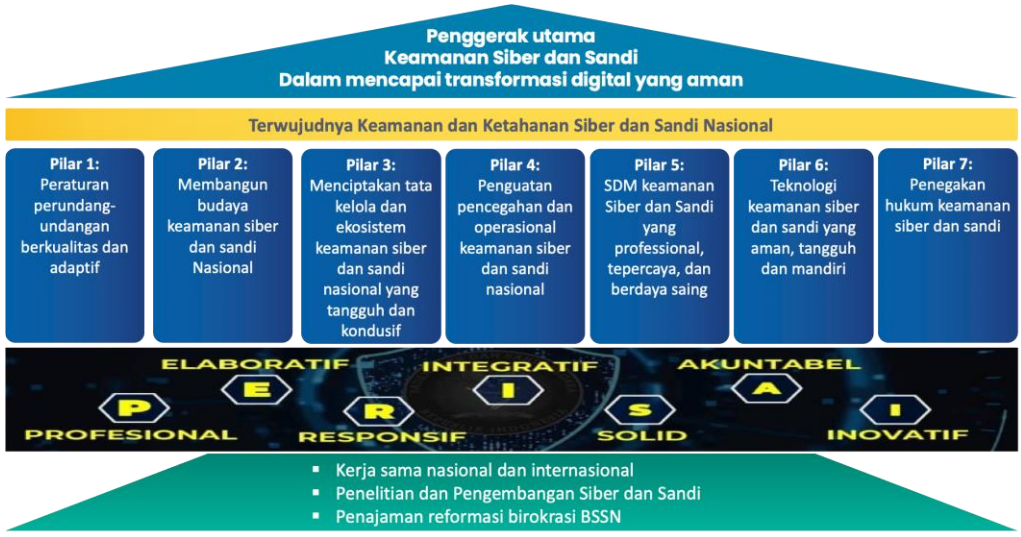
Dalam mewujudkan Visi Presiden, maka RPJMN mengamanatkan 17 program prioritas presiden serta 8 program hasil terbaik cepat yang ditunjukkan pada gambar berikut ini.

Gambar 3.9. 17 program prioritas dan 8 program hasil terbaik cepat

Keamanan siber dan sandi sebagai dasar dalam transformasi digital tentunya berdampak terhadap seluruh program prioritas ini. Namun secara spesifik, keamanan siber dan sandi berkontribusi langsung terhadap program prioritas 3 dan program prioritas 9. Program prioritas ini kemudian dijabarkan menjadi prioritas nasional, program prioritas nasional, kegiatan prioritas hingga proyek prioritas nasional.

3.2 Arah Kebijakan dan Strategi BSSN

Kerangka strategi merupakan gambaran tentang arah kebijakan maupun strategi BSSN tahun 2025-2029 yang dirumuskan berdasarkan analisis dan permasalahan maupun analisis penjenjangan kinerja dalam mewujudkan visi dan misi BSSN tahun 2025-2029. Selain itu, kerangka strategi BSSN tahun 2025-2029 juga disusun selaras dengan RPJPN tahun 2025-2045 maupun RPJMN tahun 2025-2029. Kerangka strategi BSSN digambarkan dalam bentuk rumah strategi yang menggambarkan tujuan akhir, pilar strategis hingga pondasi strategis BSSN. Rumah strategi BSSN tahun 2025-2029 dapat dijabarkan sebagai berikut:



Gambar 3.10. Rumah Strategi BSSN Sebagai Kerangka Strategi BSSN Tahun 2025-2029

Pada gambar di atas dapat dijelaskan bahwa tujuan akhir BSSN yang berkontribusi dalam mewujudkan tujuan pembangunan nasional adalah BSSN menjadi penggerak utama keamanan siber dan sandi dalam mencapai transformasi digital yang aman guna terwujudnya Visi Pembangunan Nasional. Hal ini

sesuai dengan visi yang ingin diwujudkan BSSN tahun 2029 seperti telah diuraikan pada Bab II, yaitu “Mewujudkan BSSN sebagai PERISAI bagi Keamanan Siber dan Sandi Negara dalam mewujudkan Bersama Indonesia Maju Menuju Indonesia Emas 2045”. Cita-cita besar tersebut merupakan bentuk kontribusi langsung BSSN dalam mewujudkan Misi Transformasi Ekonomi pada Rancangan Akhir RPJPN tahun 2025-2045 dalam mewujudkan Indonesia Emas tahun 2045. Selain itu, Visi BSSN ini juga merepresentasikan penguatan peran BSSN dalam mewujudkan RPJMN tahun 2025-2029.

Untuk mewujudkan tujuan akhir tersebut, maka dibutuhkan tercapainya tujuan antara yaitu Terwujudnya Keamanan dan Ketahanan Siber dan Sandi Nasional. Hal ini menjadi *milestone* sekaligus kondisi yang harus diwujudkan agar tujuan akhir dapat tercapai dengan memastikan keamanan siber nasional dan keamanan informasi dari berbagai ancaman gangguan keamanan siber, baik dari dalam maupun luar negeri. Harapannya adalah dengan terwujudnya Keamanan dan Ketahanan Siber dan Sandi Nasional maka akan berdampak terhadap terwujudnya Visi BSSN dalam mewujudkan Visi Presiden tahun 2045.

Tujuan akhir dan tujuan antara tersebut dapat diwujudkan melalui pelaksanaan 7 (tujuh) pilar strategis, yaitu:

1. Pilar 1: Peraturan perundang-undangan berkualitas dan adaptif

   Pilar pertama adalah tersedianya Peraturan Perundang-undangan berkualitas dan adaptif. Berkualitas bermakna bahwa peraturan perundang-undangan yang disusun harus

mengikuti kaidah penyusunan peraturan perundang-undangan sesuai ketentuan dan *best practices* yang berlaku. Sedangkan adaptif bermakna bahwa peraturan perundang-undangan yang disusun harus mampu mengikuti perkembangan tren digital ke depan agar dapat menjawab kebutuhan maupun permasalahan terkait siber dan persandian.

2. Pilar 2: Membangun budaya keamanan siber dan sandi nasional

   Pilar kedua adalah membangun budaya keamanan siber dan sandi nasional, di mana hal ini penting dalam mendukung terwujudnya ketahanan siber nasional. Membangun budaya keamanan siber dan sandi di seluruh *stakeholder* akan meningkatkan kesadaran *(awareness)* masyarakat, sektor privat maupun pemerintah untuk menjalankan aktivitas digital secara aman dan bertanggung jawab. Pembangunan kesadaran siber dan sandi akan dimulai dengan peningkatan pengetahuan dan pemahaman tentang keamanan siber dan sandi, kemudian akan diikuti sikap dan perilaku yang patuh terhadap ketentuan peraturan perundang-undangan yang berlaku terkait dengan keamanan siber dan sandi.

3. Pilar 3: Menciptakan tata kelola dan ekosistem keamanan siber dan sandi nasional yang tangguh dan kondusif

   Pilar ketiga adalah menciptakan tata kelola dan ekosistem keamanan siber dan sandi nasional yang tangguh dan kondusif. Tata kelola yang baik akan mampu membangun ekosistem keamanan siber dan sandi yang tangguh sehingga pada akhirnya akan dapat menciptakan keamanan siber dan sandi secara menyeluruh. Pelibatan *stakeholder* dalam

penyelenggaraan keamanan siber dan sandi perlu diatur dan diselaraskan agar dapat mencapai tujuan yang sama.

4. Pilar 4: Penguatan pencegahan dan operasional keamanan siber dan sandi nasional

   Pilar keempat adalah penguatan pencegahan dan operasional keamanan siber dan sandi nasional. Penanganan gangguan keamanan siber dan sandi berbasis risiko perlu dilakukan secara komprehensif mulai dari pencegahan sebelum insiden terjadi, penanganan saat insiden terjadi serta pemulihan pasca insiden terjadi.

   Selain itu, penguatan operasi keamanan siber maupun operasi kriptografi yang aman dan tangguh sangat dibutuhkan dalam menjaga keamanan siber dan sandi nasional, termasuk di dalamnya adalah perlindungan menyeluruh terhadap Infrastruktur Informasi Vital (IIV). Standardisasi operasional keamanan siber dan sandi akan dapat meningkatkan kualitas penyelenggaraan keamanan siber dan sandi yang merata.

5. Pilar 5: SDM keamanan siber dan sandi yang profesional, terpercaya, dan berdaya saing

   Pilar kelima adalah SDM keamanan siber dan sandi yang profesional, terpercaya, dan berdaya saing. Sumber Daya Manusia (SDM) selalu menjadi kunci keberhasilan atas setiap aspek pembangunan, tidak terkecuali keamanan siber dan sandi. Untuk itu, maka perlu adanya pengembangan SDM keamanan siber dan sandi yang profesional, terpercaya dan mampu bersaing dengan SDM dari luar negeri. Pembangunan modal manusia siber dan sandi menjadi faktor kritis dalam

mewujudkan kemandirian serta menjaga keamanan siber di masa yang akan datang.

SDM Siber dan Sandi merupakan modal manusia yang sangat menentukan keamanan siber, mulai dari preemtif, preventif hingga penanganan dan pemulihan dampak atas gangguan keamanan siber yang terjadi. Penguatan terhadap pertahanan siber nasional perlu dilakukan melalui sinergi dengan seluruh K/L/Pemda maupun sektor swasta dan masyarakat.

6. Pilar 6: Teknologi keamanan siber dan keamanan informasi yang aman, tangguh dan mandiri

   Pilar keenam adalah teknologi keamanan siber dan sandi yang aman, tangguh dan mandiri. Penguasaan teknologi merupakan salah satu faktor yang penting dalam penyelenggaraan keamanan siber dan sandi nasional. Kebutuhan akan teknologi tidak hanya pada kuantitas, namun juga dari sisi kualitas di mana teknologi yang tersedia harus aman, tangguh dan andal. Selain itu, kemandirian teknologi juga penting untuk melepaskan ketergantungan Indonesia dari pihak asing sehingga harga akan menjadi lebih terjangkau.

   Teknologi keamanan siber dan sandi ini tidak hanya dimiliki oleh BSSN saja, namun juga perlu ditempatkan pada seluruh K/L/Pemda, khususnya yang telah memiliki/menetapkan CSIRT. Ketersediaan dan pemanfaatan teknologi keamanan siber dan sandi ini diharapkan dapat meningkatkan upaya pencegahan, meningkatkan waktu respons terhadap gangguan atau potensi gangguan hingga meminimalisasi risiko yang terjadi saat terjadi gangguan keamanan siber.

7. Pilar 7: Penegakan hukum, penindakan dan pengawasan kepatuhan keamanan siber dan keamanan informasi

   Pilar ketujuh adalah penegakan hukum, penindakan dan pengawasan kepatuhan keamanan siber dan sandi. Penegakan hukum sangat dibutuhkan dalam menjaga stabilitas keamanan dari berbagai gangguan keamanan siber, baik *pro justicia* maupun penindakan dan pengawasan kepatuhan terhadap peraturan perundang-undangan yang berlaku. Penegakan hukum keamanan siber dan sandi merupakan bagian dari upaya menciptakan kepastian hukum sehingga akan dapat melindungi seluruh masyarakat maupun pemerintah dari insiden keamanan siber. BSSN dapat menjadi *cyber police* sesuai kewenangan yang diatur dalam peraturan perundang-undangan, sehingga dapat membantu aparat penegak hukum lain dalam menegakkan hukum terkait keamanan siber dan sandi. Penegakan hukum yang optimal tentunya akan menciptakan kepastian hukum sehingga transformasi digital dapat segera terwujud dalam mendukung tercapainya Indonesia Emas 2045.

Ketujuh pilar strategis tersebut ditopang oleh sistem nilai "PERISAI" yang harus diinternalisasi ke seluruh SDM ASN BSSN. Sistem nilai PERISAI ini sekaligus menjadi budaya organisasi BSSN yang diharapkan dapat berkembang dan mempererat hubungan kerja seluruh SDM ASN di lingkungan BSSN. Adapun makna dari sistem nilai PERISAI ini adalah:

- Profesional, bermakna bahwa SDM ASN BSSN harus memegang teguh protokol dan kerangka peraturan, serta kapasitas kemampuan yang kredibel.

- Elaboratif, bermakna bahwa SDM ASN BSSN mampu mengembangkan wawasan, ide dan kreativitas dalam pelaksanaan tugas.
- Responsif, bermakna bahwa SDM ASN BSSN memiliki kepedulian dan ketanggapsegeraan terhadap apa yang menjadi bagian dari fungsi, peran dan tugas BSSN.
- Integratif, bermakna bahwa SDM ASN BSSN terbuka terhadap integrasi berbagai unsur atau aspek secara harmonis (internal dan eksternal).
- Solid, bermakna bahwa SDM ASN BSSN memiliki kesadaran kolektif sebagai satu kesatuan yang kokoh dan saling mendukung dalam pelaksanaan tugas.
- Akuntabel, bermakna bahwa SDM ASN BSSN memiliki transparansi kinerja dan tanggung jawab dalam melaksanakan tugas.
- Inovatif, bermakna bahwa SDM ASN BSSN unggul dalam inovasi dan modernisasi teknologi dan sistem keamanan siber

Rumah strategi BSSN ini membutuhkan fondasi yang kokoh sebagai *strategic asset* dalam menopang seluruh struktur diatasnya. Fondasi strategis BSSN tersebut mencakup 3 (tiga) aspek, yaitu:

1. Kerja sama nasional dan internasional

   Kerja sama dalam penyelenggaraan siber dan sandi dilakukan terhadap ketujuh pilar strategis yang telah dijelaskan sebelumnya. Kerja sama dilakukan didalam maupun luar negeri, baik dengan instansi pemerintah, sektor privat, maupun masyarakat luas. Selain itu, peran aktif BSSN dalam

forum keamanan siber dan sandi internasional juga penting untuk dilakukan dalam menjaga hubungan baik dan/atau membangun kerja sama baru sesuai dengan kebutuhan.

2. Penelitian dan pengembangan siber dan kriptografi

   Penelitian dan pengembangan (Litbang) sangat penting dan menentukan kemajuan penyelenggaraan siber dan sandi nasional. Litbang dilakukan dalam rangka menghasilkan inovasi yang dapat dimanfaatkan dalam penyelenggaraan siber dan sandi nasional. Saat ini, pelaksanaan seluruh Litbang dipusatkan di BRIN, sehingga BSSN perlu membangun kolaborasi dalam menghasilkan inovasi di bidang keamanan dan ketahanan siber dan informasi sesuai dengan harapan.

3. Penajaman reformasi birokrasi BSSN

   Pelaksanaan reformasi birokrasi mengalami penajaman secara nasional, di mana fokus pelaksanaan reformasi birokrasi tidak lagi pada pemenuhan administrasi (hulu), namun lebih mengedepankan dampak langsung reformasi birokrasi bagi masyarakat. BSSN melaksanakan reformasi birokrasi, baik general maupun tematik, dalam memberikan dampak langsung kepada masyarakat. Selain itu, pelaksanaan reformasi birokrasi sekaligus merupakan upaya dalam menciptakan birokrasi yang transparan dan akuntabel sehingga dapat mewujudkan *good government governance* atau tata kelola pemerintahan yang baik.

Berdasarkan rumah strategi yang telah dijelaskan sebelumnya, maka arah kebijakan dan strategi BSSN tahun 2025-2029 dalam mewujudkan visi BSSN tahun 2029 adalah:

- Arah kebijakan 1: Membangun ketahanan dan keamanan siber dan keamanan informasi nasional bagi pemerintah, sektor privat, maupun masyarakat luas. Strategi yang dilakukan adalah:
  - Strategi 1: Menyelenggarakan keamanan siber dan sandi yang aman, andal, akuntabel dan profesional

    Strategi ini menekankan pada penyelenggaraan keamanan siber dan keamanan informasi nasional yang aman, andal, akuntabel dan profesional. Strategi ini terdiri dari beberapa uraian strategi, meliputi:

    - Uraian strategi 1.1 Meningkatkan kualitas peraturan perundang-undangan keamanan siber dan sandi yang adaptif terhadap perubahan, melalui:
      - Penyusunan RUU tentang Keamanan dan Ketahanan Siber;
      - Penyusunan RUU tentang Persandian;
      - Analisis dan evaluasi kebijakan keamanan siber (*policy analysis*);
      - Rekomendasi kebijakan keamanan siber;
      - Penyusunan kebijakan keamanan siber berbasis bukti (*evidence –based policy*);
      - Penyusunan Peraturan Badan tentang Rencana aksi nasional keamanan siber;
      - Penyusunan Peraturan Badan tentang Penyelenggaraan Manajemen Krisis Siber;
      - Penyusunan Peraturan Badan tentang Penerapan dan pelaporan hasil penerapan manajemen risiko keamanan siber;

- Penyusunan Peraturan Badan tentang Tim tanggap insiden siber, pelaporan, penanganan insiden siber, dan pelaksanaan kesiapan terhadap insiden siber;
- Perumusan dan penetapan rencana kontingensi untuk pengelolaan krisis siber;
- Perumusan kebijakan kriptografi nasional;
- Penetapan kebijakan dan prioritas kerja sama internasional di bidang keamanan siber;
- Penyusunan Peraturan Badan tentang Peta jalan perlindungan IIV sektor Administrasi Pemerintah.

▪ Uraian Strategi 1.2: Membangun dan meningkatkan kesadaran dan budaya keamanan siber dan sandi nasional, melalui:

- Pembudayaan hukum dan peningkatan kesadaran hukum masyarakat terkait keamanan siber dan sandi;
- Penguatan pertukaran informasi yang aman dan memiliki akses yang tinggi dalam kesiapsiagaan dan ketahanan siber nasional;
- Pengembangan dan penerapan program peningkatan kesadaran keamanan siber yang terkoordinasi dan berkesinambungan.

▪ Uraian Strategi 1.3: Menciptakan tata kelola dan ekosistem keamanan siber dan sandi nasional yang tangguh dan kondusif, melalui :

- Penguatan ekosistem keamanan siber, meliputi penguatan modal manusia (*human capital*) siber dan

sandi, penguatan proses serta teknologi di bidang siber dan kriptografi;

- Peningkatan sinergi dan kolaborasi dalam pelaksanaan keamanan siber dan sandi;
- Literasi keamanan digital untuk pemerintah, sektor privat serta masyarakat;
- Mengukur dan meningkatkan maturitas Penyelenggara Sistem Elektronik (PSE) keamanan siber dan sandi;
- Mengukur dan meningkatkan maturitas obyek keamanan siber dan sandi.

▪ Uraian Strategi 1.4: Penguatan pencegahan dan operasional keamanan siber dan keamanan informasi nasional, melalui :

- Kesiapsiagaan dan ketahanan keamanan siber dan sandi;
- Operasi keamanan siber dan sandi;
- Pembangunan kapasitas tanggap insiden siber yang efektif dan efisien;
- Perumusan dan penetapan rencana kontingensi untuk pengelolaan krisis siber;
- Penyelenggaraan penanganan tanggap darurat;
- Penguatan pertukaran informasi yang aman dan memiliki akses yang tinggi;
- Penyelenggaraan perlindungan IIV;
- Peningkatan pembinaan dan pengawasan penyelenggaraan perlindungan IIV;
- Identifikasi sektor IIV dan IIV;

- Koordinasi penyelenggaraan perlindungan IIV.

- Uraian Strategi 1.5: Meningkatkan kualitas SDM keamanan siber dan sandi yang profesional, terpercaya, dan berdaya saing, melalui :
  - Pembangunan kapasitas tanggap insiden siber yang efektif dan efisien;
  - Pengembangan kurikulum keamanan siber pada PAUD, pendidikan dasar, menengah dan tinggi;
  - Pengembangan dan penerapan program keterampilan dan pelatihan SDM;
  - Penguatan kapasitas teknologi keamanan siber dan sandi;
  - Peningkatan riset, pengembangan dan inovasi IPTEK keamanan siber;
  - Pengembangan program khusus sektor dan kelompok rentan sesuai kebutuhan;
  - Pengembangan perguruan tinggi kedinasan keamanan dan ketahanan siber dan sandi nasional.

- Uraian Strategi 1.6: Pengembangan teknologi keamanan siber dan keamanan informasi yang aman, tangguh dan mandiri, melalui :
  - Pembangunan dan pengembangan industri kriptografi nasional;
  - Penguatan kapasitas teknologi keamanan siber;
  - Pembangunan dan pengembangan industri keamanan siber.

- Uraian Strategi 1.7: Penegakan hukum, penindakan dan pengawasan kepatuhan keamanan siber dan keamanan informasi, melalui :
  - Penegakan hukum di bidang keamanan siber secara terpadu;
  - Pemberian pendapat/opini hukum terkait keamanan siber dan sandi;
  - Penindakan terhadap pelanggaran hukum terkait keamanan siber dan keamanan informasi sesuai ketentuan peraturan perundang-undangan yang berlaku;
  - Pengawasan kepatuhan terhadap peraturan perundang-undangan yang berlaku terkait keamanan siber dan sandi.
- Uraian Strategi 1.8: Melaksanakan kerja sama nasional dan internasional, melalui :
  - Penetapan kebijakan dan prioritas kerja sama internasional di bidang keamanan siber dan sandi;
  - Peningkatan inisiatif kerja sama internasional dalam mendukung terciptanya ruang siber yang aman, damai dan terbuka serta meningkatkan kapasitas nasional di bidang keamanan siber dan sandi;
  - Peningkatan kerja sama praktis, berbagi informasi dan praktik terbaik dalam menghadapi krisis siber;
  - Peningkatan peran Indonesia dalam forum bilateral, regional dan multilateral di bidang keamanan siber dan sandi;

- Uraian Strategi 1.9 : Melakukan penelitian dan pengembangan (Litbang) siber dan sandi, melalui :
  - Peningkatan riset, pengembangan dan inovasi IPTEK keamanan siber;
  - Peningkatan riset, pengembangan dan inovasi kriptografi untuk mendukung pembangunan nasional;
  - Pembangunan dan pengembangan industri kriptografi nasional.

- Arah kebijakan 2: Hilirisasi pelaksanaan reformasi birokrasi BSSN yang selaras dengan Reformasi Birokrasi Nasional (RBN). Strategi yang dilakukan adalah:
  - Strategi 2: Penajaman pelaksanaan reformasi birokrasi BSSN yang berdampak langsung kepada masyarakat.
    Strategi ini merupakan strategi pelaksanaan reformasi birokrasi BSSN sebagai bagian dari pelaksanaan Reformasi Birokrasi Nasional (RBN). Strategi ini terdiri dari beberapa uraian strategi, meliputi:
    - Uraian Strategi 2.1: Optimasi pelaksanaan RB General, melalui :
      - Implementasi kebijakan penyederhanaan birokrasi;
      - Implementasi kebijakan sistem kerja baru dengan model fleksibel bagi pegawai ASN dengan baik;
      - Implementasi kebijakan arsitektur SPBE Nasional;
      - Implementasi Sistem Perencanaan, Penganggaran dan Informasi Kinerja yang Terintegrasi, Berbasis

Teknologi Informasi yang Mendorong Peningkatan Akuntabilitas Kinerja Instansi Pemerintah;

- Membangun pelayanan publik digital (*Digital Services*);
- Meningkatkan kualitas pengawasan;
- Meningkatkan kualitas kebijakan dan regulasi;
- Meningkatkan kualitas pengelolaan arsip digital dan data statistik sektoral;
- Meningkatkan kualitas pengadaan barang dan jasa pemerintah, pengelolaan keuangan dan aset;
- Percepatan transformasi jabatan fungsional;
- Manajemen talenta ASN yang efektif dan efisien;
- Percepatan peningkatan kapasitas pegawai ASN;
- Rekrutmen pegawai ASN yang efektif dan efisien;
- Percepatan transformasi digital manajemen ASN;
- Sistem kesejahteraan ASN yang adil, layak, dan berbasis kinerja;
- Peningkatan kepatuhan terhadap sistem merit dan sistem manajemen ASN.

▪ Uraian Strategi 2.2: Pelaksanaan Reformasi Birokrasi Tematik, melalui :

- RB tema penurunan kemiskinan;
- RB tema peningkatan investasi;
- RB tema digitalisasi layanan administrasi pemerintah;
- RB tema pemanfaatan Produk Dalam Negeri (PDN) dan pengendalian inflasi.

- Uraian Strategi 2.3: Peningkatan kualitas layanan internal, melalui:
  - Layanan Perencanaan;
  - Layanan Keuangan;
  - Layanan Organisasi dan Tata Laksana;
  - Layanan SDM ASN;
  - Layanan Hukum;
  - Layanan Komunikasi Publik;
  - Layanan Umum.

3.3 Kerangka Regulasi

Kerangka regulasi adalah perencanaan pembentukan regulasi dalam rangka memfasilitasi, mendorong dan mengatur perilaku masyarakat dan penyelenggara negara dalam rangka mencapai tujuan bernegara. Kerangka regulasi merupakan salah satu elemen dalam penyusunan rencana strategis (Renstra) Kementerian dan Lembaga (K/L) yang berisi tentang peraturan perundang-undangan yang menjadi dasar hukum bagi K/L dalam melaksanakan tugas dan fungsinya. Kerangka regulasi juga mencakup rencana perubahan atau penyusunan peraturan baru yang diperlukan untuk mendukung pencapaian sasaran strategis K/L. Kerangka regulasi yang disusun harus selaras dengan RPJPN dan RPJMN.

BSSN adalah lembaga pemerintah yang bertugas melaksanakan keamanan siber nasional. BSSN telah menyusun beberapa regulasi terkait dengan tugas dan fungsinya, namun BSSN masih membutuhkan regulasi-regulasi strategis terkait keamanan siber dan sandi nasional dalam mendukung pencapaian visi, misi, dan sasaran strategis BSSN periode 2025-

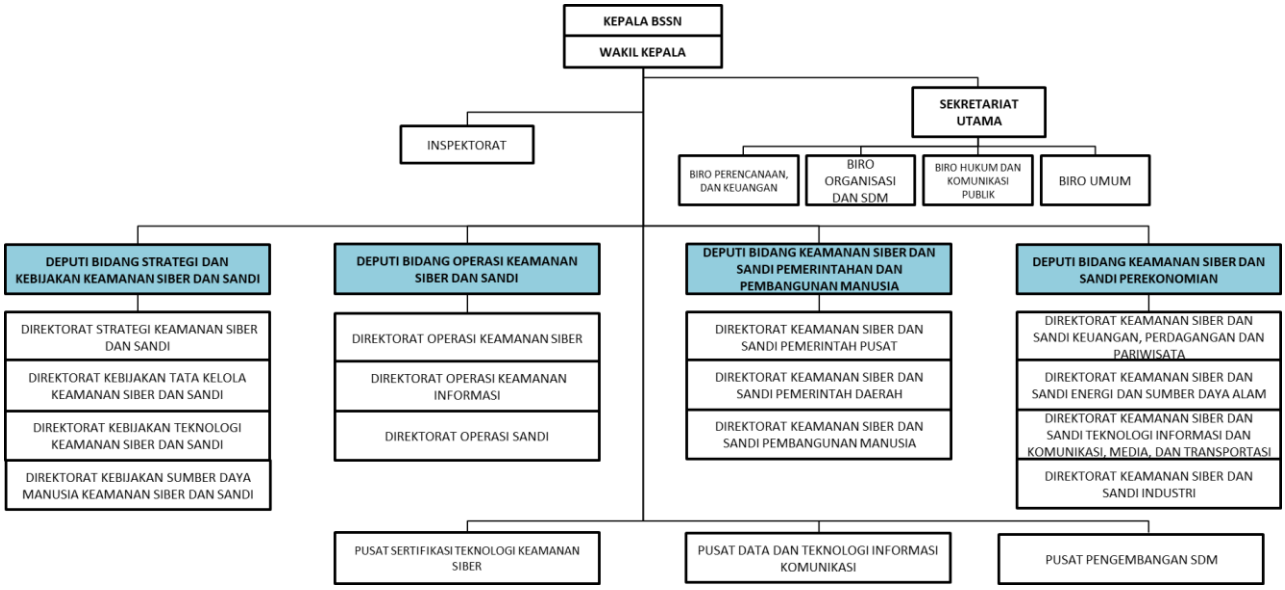
2029. Kerangka regulasi yang disusun oleh BSSN telah sejalan dengan kerangka regulasi pada RPJMN 2025-2029 khususnya terkait Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber. Regulasi-regulasi yang dibutuhkan oleh BSSN dalam mendukung pencapaian visi, misi, dan sasaran strategis BSSN periode 2025-2029 dapat dilihat pada Lampiran 2.

3.4 Kerangka Kelembagaan

Berdasarkan Perpres 28 Tahun 2021 tentang Badan Siber dan Sandi Negara BSSN melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan. Dalam melaksanakan tugas tersebut, BSSN melaksanakan fungsi sebagai berikut:

a. perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi;
b. pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi;
c. penyusunan norma, standar, prosedur, dan kriteria di bidang persandian;
d. pelaksanaan bimbingan teknis dan supervisi di bidang persandian;
e. koordinasi pelaksanaan tugas, pembinaan, dan dukungan administrasi kepada seluruh unsur organisasi di lingkungan BSSN;
f. pengelolaan barang milik negara yang menjadi tanggung jawab BSSN;
g. pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN; dan
h. pengawasan atas pelaksanaan tugas di lingkungan BSSN.

Organisasi dan Tata Kerja BSSN, Struktur Organisasi BSSN ditunjukkan pada Gambar 3.8.



Gambar 3.8. Struktur Organisasi dan Tata Kerja BSSN

BSSN terdiri atas :

a. Kepala;
b. Wakil Kepala;
c. Sekretariat Utama;
d. Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi;
e. Deputi Bidang Operasi Keamanan Siber dan Sandi;
f. Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia; dan
g. Deputi Bidang Keamanan Siber dan Sandi Perekonomian.

BSSN juga didukung dengan unsur-unsur pendukung yaitu:

a. Pusat Sertifikasi Teknologi Keamanan Siber dan Sandi;
b. Pusat Data dan Teknologi Informasi Komunikasi;
c. Pusat Pengembangan Sumber Daya Manusia.

Dalam rangka menjawab potensi, permasalahan, dan aspirasi masyarakat terkait tugas dan fungsi BSSN di bidang keamanan siber dan sandi untuk mendukung arah kebijakan pembangunan nasional, maka perlu dilakukan evaluasi pada struktur organisasi BSSN saat ini, dimana:

1. Dibutuhkan unit kerja khusus yang mendukung aspek keamanan siber perlindungan data pribadi, sebagai langkah antisipatif sesuai amanat Undang-undang 27 Tahun 2022 tentang PDP;
2. Dibutuhkan unit kerja khusus yang menangani pengawasan, penindakan dan penegakan hukum bidang keamanan siber dan informasi di BSSN. Sementara ini dilakukan oleh Polri dan Kementerian Komunikasi dan Digital;
3. Dibutuhkan unit khusus yang menangani perlindungan Infrastruktur Informasi Vital (IIV);
4. Dibutuhkan unit kerja khusus yang menangani kerja sama keamanan siber dalam dan luar negeri, termasuk memastikan peran aktif Indonesia pada berbagai forum dan komunitas internasional siber dan sandi;
5. Dibutuhkan unit kerja khusus yang menangani kesiapsiagaan dan ketahanan keamanan siber dan informasi, termasuk intelijen siber dan intelijen informasi;
6. Dibutuhkan unit kerja khusus yang menangani adopsi dan penerapan teknologi keamanan siber, sandi dan sinyal.

Kerangka kelembagaan BSSN menggambarkan kebutuhan desain organisasi dan fungsi agar dapat menjalankan seluruh arah kebijakan dan strategi dalam mewujudkan visi dan misi BSSN tahun 2025-2029. Desain organisasi disusun dengan mempertimbangkan RPJMN 2025-2029, rumah strategi BSSN

maupun permasalahan yang ada pada struktur organisasi BSSN saat ini.

Desain organisasi BSSN atau kriteria desain organisasi BSSN yang dibutuhkan dalam mendukung terlaksananya RPJMN tahun 2025-2029 dapat diuraikan sebagai berikut:

- Prioritas Nasional 2: Memantapkan Sistem Pertahanan dan Keamanan Negara, dengan kebutuhan desain organisasi:
  - Dibutuhkan organisasi setingkat Kementerian (Kementerian atau LPNK) dalam mengoordinasikan pengelolaan keamanan siber dan sandi dari hulu ke hilir secara sentralistis;
  - Organisasi tersebut fokus dalam mencegah, menangani hingga melakukan pengawasan, penegakan hukum dan penindakan atas keamanan siber dan keamanan informasi;
  - Organisasi yang saat ini ada (BSSN) perlu diperkuat dan diperluas kewenangannya sehingga pelaksanaan keamanan dan ketahanan siber dapat dilakukan secara optimal.
  - Dalam rangka meningkatkan keamanan dan ketahanan siber dan sandi secara merata di seluruh wilayah Indonesia, maka Organisasi yang saat ini ada (BSSN) juga perlu dikembangkan di seluruh wilayah NKRI, terutama di ibukota provinsi dan kota-kota besar yang aktif berinteraksi di ruang digital.
  - Memperkuat pendidikan, sains dan teknologi dengan kebutuhan desain organisasi: unit kerja yang menangani literasi digital dan keamanan siber secara terintegrasi; unit kerja yang mengoordinasikan perancangan dan penerapan kurikulum keamanan siber dan keamanan informasi di berbagai tingkat pendidikan; unit kerja yang

mengoordinasikan pelaksanaan pendidikan tinggi siber dan persandian.

- Prioritas Nasional 7 : Reformasi Tata Kelola Pemerintahan, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja yang menangani keamanan siber pada perencanaan dan penerapan Sistem Pemerintah Berbasis Elektronik (SPBE);
  - Dibutuhkan unit kerja yang menangani perlindungan Infrastruktur Informasi Vital (IIV) secara komprehensif sesuai amanat Perpres 82/2022.

Desain organisasi BSSN atau kriteria desain organisasi BSSN yang dibutuhkan dalam mendukung terlaksananya rumah strategis BSSN dapat diuraikan sebagai berikut:

- Pilar 1: Peraturan perundang-undangan berkualitas dan adaptif, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon II yang menangani pembentukan peraturan perundang-undangan bidang siber dan sandi;
  - Dibutuhkan unit kerja setingkat eselon II yang menangani substansi teknis peraturan perundang-undangan bidang siber dan sandi secara terpusat.
- Pilar 2: Membangun budaya keamanan siber dan sandi nasional, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon II yang menangani pembangunan budaya keamanan siber dan sandi masyarakat maupun pemerintah;

- Dibutuhkan unit kerja kewilayahan setingkat eselon II yang memiliki fungsi pembangunan budaya keamanan siber dan sandi masyarakat maupun pemerintah (BSSN Provinsi).

- Pilar 3: Menciptakan tata kelola dan ekosistem keamanan siber dan sandi nasional yang tangguh dan kondusif, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon I yang menangani tata kelola keamanan siber dan sandi nasional, meliputi:
    - Perencanaan dan penerapan strategi keamanan siber dan sandi terintegrasi;
    - Pengembangan ekosistem keamanan siber dan sandi;
    - Kolaborasi (koordinasi, sinergi dan kerja sama) dalam pelaksanaan strategi keamanan siber dan sandi.

- Pilar 4: Penguatan pencegahan dan operasional keamanan siber dan sandi nasional, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon I yang menangani kesiapsiagaan dan ketahanan keamanan siber dan informasi nasional:
    - Intelijen siber;
    - Intelijen informasi;
    - Pengendalian informasi;
    - Deteksi gangguan siber dan keamanan informasi;
    - Kesiapsiagaan keamanan siber dan keamanan informasi;
    - Ketahanan keamanan siber dan keamanan informasi.
  - Dibutuhkan unit kerja setingkat eselon I yang menangani operasi perlindungan IIV:
    - Identifikasi sektor IIV dan IIV

- Penyelenggaraan pelindungan IIV
- Pembinaan dan pengawasan pelindungan IIV
- Koordinasi penyelenggaraan pelindungan IIV

o Dibutuhkan unit kerja kewilayahan setingkat eselon II yang memiliki fungsi pencegahan dan operasional keamanan siber dan sandi di wilayah (BSSN Provinsi)

- Pilar 5: SDM keamanan siber dan sandi yang profesional, tepercaya, dan berdaya saing, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon I yang menangani pengembangan SDM Siber dan Sandi sebagai modal manusia (*Human Capital*):
    - Pendidikan siber dan sandi;
    - Pelatihan siber dan sandi;
    - Asesmen kompetensi siber dan sandi;
    - Pembinaan JF siber dan sandi.
    - Pembangunan budaya keamanan siber dan sandi Masyarakat
    - Literasi digital, keamanan siber dan persandian
    - Sinkronisasi penerapan kurikulum keamanan siber dan keamanan informasi di berbagai tingkat pendidikan
- Pilar 6: Teknologi keamanan siber dan sandi yang aman, tangguh dan mandiri, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon II yang menangani penerapan teknologi keamanan siber dan informasi:
    - Adopsi teknologi keamanan siber;
    - Adopsi teknologi kriptografi;

- Adopsi teknologi sinyal;
- Diseminasi dan penerapan teknologi keamanan siber dan sandi;
- Standardisasi dan sertifikasi teknologi keamanan siber dan sandi.

- Pilar 7: Penegakan hukum, penindakan dan pengawasan kepatuhan keamanan siber dan sandi, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit kerja setingkat eselon I yang menangani pengawasan, penindakan dan penegakan hukum siber dan sandi, meliputi:
    - Pengawasan kepatuhan keamanan siber dan sandi;
    - Pembinaan keamanan siber dan sandi nasional;
    - Penegakan hukum (penyelidikan) tindak pidana keamanan siber;
    - Penindakan gangguan keamanan siber;
    - Penindakan gangguan keamanan informasi.
  - Dibutuhkan unit kerja kewilayahan setingkat eselon II yang memiliki fungsi penegakan hukum, penindakan dan pengawasan kepatuhan keamanan siber dan sandi di wilayah (BSSN Provinsi)
- Pondasi 1: Kerja sama nasional dan internasional, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit setingkat eselon I yang menangani kerja sama keamanan siber dan sandi di tingkat nasional dan internasional (global), sekaligus memastikan peran aktif Indonesia pada berbagai forum dan dan komunitas internasional siber dan sandi.

- Pondasi 2: Penelitian dan pengembangan siber dan kriptografi, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit setingkat eselon I yang menangani penelitian dan pengembangan siber dan sandi, dalam hal ini penerapan teknologi keamanan siber dan sandi yang meliputi:
    - Adopsi teknologi keamanan siber;
    - Adopsi teknologi kriptografi;
    - Adopsi teknologi sinyal
    - Diseminasi dan penerapan teknologi keamanan siber dan kriptografi;
    - Standardisasi dan sertifikasi teknologi keamanan siber dan sandi.
- Pondasi 3: Penajaman reformasi birokrasi BSSN, dengan kebutuhan desain organisasi:
  - Dibutuhkan unit setingkat eselon I yang menangani penajaman reformasi birokrasi sebagai unit dukungan manajemen, yang meliputi:
    - Perencanaan, Keuangan dan Barang Milik Negara (BMN), yang dalam pelaksanaan tugasnya akan dibagi menjadi 4 (empat) unit kerja setingkat eselon III;
    - Organisasi, Tata Laksana, Sumber Daya Manusia (SDM) ASN BSSN dan koordinasi pelaksanaan Reformasi Birokrasi BSSN, yang dalam pelaksanaan tugasnya akan dibagi menjadi 4 (empat) unit kerja setingkat eselon III;
    - Hukum, Humas, Kerja Sama dan Pelayanan Publik, yang dalam pelaksanaan tugasnya akan dibagi menjadi 4 (empat) unit kerja setingkat eselon III;

- Umum dan Pengadaan Barang dan Jasa, yang dalam pelaksanaan tugasnya akan dibagi menjadi 4 (empat) unit kerja setingkat eselon III.

Berdasarkan kebutuhan desain organisasi tersebut, maka kriteria desain organisasi BSSN dalam mendukung pelaksanaan strategi BSSN, membutuhkan transformasi BSSN menjadi Kementerian Siber dan Sandi Negara, dengan 4 (empat) unit eselon I unsur pelaksana, 3 (tiga) unit eselon I unsur pendukung serta Unit eselon I Dukungan Manajemen dan Unit eselon I sebagai Pengawas Intern (Auditor Internal). 4 (empat) unit eselon I unsur pelaksana yang menyelenggarakan fungsi sebagai berikut:

- Kerja Sama Keamanan Siber dan Sandi, meliputi:
  - Kerja sama instansi pemerintah
  - Kerja sama sektor privat
  - Kerja sama luar negeri
  - Atase siber dan sandi
- Kesiapsiagaan dan Ketahanan Keamanan Siber dan Sandi, meliputi:
  - Intelijen Siber
  - Intelijen informasi
  - Pengendalian informasi
  - Deteksi ancaman keamanan siber dan keamanan informasi (*early warning system*)
  - Kesiapsiagaan keamanan siber dan keamanan informasi
  - Ketahanan keamanan siber dan keamanan informasi
- Operasi Pengamanan Informasi dan Pelindungan IIV, meliputi:
  - Operasi pengamanan informasi dan intelijen sinyal
  - Identifikasi sektor IIV dan IIV

- Penyelenggaraan pelindungan IIV
- Pembinaan dan pengawasan pelindungan IIV
- Koordinasi penyelenggaraan pelindungan IIV

- Pengawasan dan Penindakan Keamanan Siber dan Sandi, meliputi:
  - Pengawasan kepatuhan keamanan siber dan sandi
  - Pembinaan keamanan siber dan sandi nasional
  - Penegakan hukum keamanan siber dan sandi
  - Penindakan gangguan keamanan siber dan Sandi

3 (tiga) unit eselon I unsur pendukung yang menyelenggarakan fungsi sebagai berikut:

- Strategi dan Kebijakan Keamanan Siber dan Sandi, meliputi:
  - Perumusan dan pelaksanaan strategi keamanan siber dan sandi
  - Penguatan ekosistem keamanan siber dan sandi nasional
  - Kolaborasi keamanan siber dan sandi instansi pemerintah
  - Kolaborasi keamanan siber dan sandi sektor privat

- Pengembangan Sumber Daya Manusia Siber dan Sandi (*Corporate University*), meliputi:
  - Pendidikan siber dan sandi
  - Pengembangan SDM siber dan sandi
  - Pembangunan budaya keamanan siber dan sandi masyarakat
  - Pembinaan jabatan fungsional siber dan sandi
  - Literasi digital, keamanan siber dan persandian
  - Sinkronisasi penerapan kurikulum keamanan siber dan keamanan informasi di berbagai tingkat pendidikan

- Penerapan Teknologi Keamanan Siber dan Sandi, meliputi:

- Adopsi teknologi keamanan siber
- Adopsi teknologi kriptografi
- Adopsi teknologi sinyal
- Diseminasi dan penerapan teknologi keamanan siber dan kriptografi
- Standardisasi dan sertifikasi teknologi keamanan siber dan sandi

Dalam Renstra BSSN tahun 2025-2029 ini, tentunya kriteria desain yang dihasilkan masih berdasarkan kebutuhan strategi sesuai prinsip *structure follow strategy*. Penyempurnaan kriteria yang dihasilkan sangat dibutuhkan dalam menentukan desain organisasi BSSN yang ideal ke depan dalam mendukung pelaksanaan arah kebijakan dan strategi untuk mewujudkan visi dan misi BSSN tahun 2025-2029.

BAB IV
TARGET KINERJA DAN PENDANAAN

4.1 Target Kinerja

Target kinerja merupakan hasil dan satuan hasil yang akan dicapai dari setiap Indikator Kinerja, baik itu Indikator Kinerja Sasaran Strategis, Indikator Kinerja Program, dan Indikator Kinerja Kegiatan di Badan Siber dan Sandi Negara. Dalam melaksanakan tugas dan fungsinya, Badan Siber dan Sandi Negara menyusun 1 (satu) program teknis, yaitu Program Keamanan dan Ketahanan Siber dan Sandi Negara dan 1 (satu) program generik, yaitu Program Dukungan Manajemen. Kedua program tersebut akan dibagi menjadi beberapa kegiatan yang masing-masing memiliki sasaran, indikator, dan target kinerja. Indikator kinerja sasaran strategis (IKSS) adalah alat untuk mengukur keberhasilan pencapaian hasil *intermediate outcome* level 1 dari suatu rencana strategi K/L dan merupakan representasi dari telah tercapainya suatu sasaran strategis (SS). Sedangkan untuk indikator kinerja sasaran program (IKP) adalah alat untuk mengukur keberhasilan pencapaian *intermediate outcome* level 2 dari suatu program. IKP kemudian diturunkan menjadi indikator kinerja sasaran kegiatan (IKK) yaitu indikator keberhasilan pencapaian *output* dari suatu kegiatan. Tabel di bawah memperlihatkan sasaran strategis, indikator kinerja sasaran strategis serta target periode 2025 – 2029 terkait program teknis Meningkatnya keamanan dan ketahanan siber dan sandi nasional maupun program dukungan manajemen Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN.

Tabel 4.1. Sasaran, Indikator dan Target Badan Siber Dan Sandi Negara Periode 2025 – 2029

No	Sasaran Strategis (SS)	Kode IKSS	Indikator Kinerja Sasaran Strategis (IKSS)	Target				
				2025	2026	2027	2028	2029
SS 1	Meningkatnya keamanan dan ketahanan siber dan sandi nasional	IKSS 1.1	Indeks Keamanan dan Ketahanan Siber	0,69	0,73	0,76	0,80	0,84
		IKSS 1.2	Indeks Keamanan Informasi	0,75	0,78	0,83	0,87	0,90
SS 2	Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN	IKSS 2.1	Indeks Reformasi Birokrasi BSSN	90,55	91,22	93,31	94,11	95,29

4.2 Kerangka Pendanaan

Kerangka pendanaan merupakan penjelasan kebutuhan pendanaan secara keseluruhan untuk mencapai target Sasaran Strategis, Sasaran Program, dan Sasaran Kegiatan dari Badan Siber dan Sandi Negara, dimana pemenuhan kebutuhan pendanaan bersumber dari APBN yang dapat berupa dari Rupiah Murni, Pinjaman dan/atau Hibah Luar Negeri (PHLN), Pinjaman dan/atau Hibah Dalam Negeri (PHDN), dan Penerimaan Negara Bukan Pajak (PNBP). Kebutuhan anggaran tersebut dapat dioptimalkan dengan penyelenggaraan program dan kegiatan BSSN dan disinkronisasikan dengan realitas kemampuan sumber daya yang tersedia dalam BSSN. Secara ringkas, kerangka pendanaan BSSN periode 2025-2029 disampaikan pada Tabel 4.2. Adapun perincian kerangka pendanaan secara detil dapat dilihat pada Lampiran 1.

Tabel 4.2. Kerangka Pendanaan Renstra BSSN 2025 – 2029

KODE	PROGRAM	KERANGKA PENDANAAN (dalam jutaan)				
		2025	2026	2027	2028	2029
KL	BADAN SIBER DAN SANDI NEGARA	1.321.637	5.549.633	5.876.303	6.443.308	7.313.775
051.BO	PROGRAM KEAMANAN DAN KETAHANAN SIBER DAN SANDI NEGARA	848.464	4.857.551	4.798.937	5.341.315	6.163.626
051.WA	PROGRAM DUKUNGAN MANAJEMEN	473.173	692.082	1.077.367	1.101.992	1.150.149

BAB V
PENUTUP

Renstra BSSN tahun 2025-2029 telah disusun secara komprehensif melalui serangkaian *Focus Group Discussion* (FGD) dengan melibatkan berbagai pemangku kepentingan. Proses penyusunan Renstra ini dimulai pada tahun 2023 melalui penyusunan Rancangan Teknokratik Renstra BSSN tahun 2025-2029 dan dilanjutkan pada tahun 2024 melalui penyusunan Rancangan Awal Renstra BSSN tahun 2025-2029 yang selaras dengan Visi, Misi dan Program Kerja Presiden dan Wakil Presiden terpilih. Pasca penetapan RPJMN tahun 2025-2029 melalui Perpres Nomor 12 Tahun 2025 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2025-2029, BSSN melakukan penyesuaian Rancangan Awal Renstra BSSN menjadi Rancangan Renstra BSSN tahun 2025-2029 yang selaras dengan RPJMN Tahun 2025-2029.

Rancangan Renstra BSSN ini telah sesuai dengan arahan pimpinan dan selaras dengan RPJMN tahun 2025-2029. Visi BSSN tahun 2025-2029 telah diselaraskan dan mendukung terwujudnya Visi Presiden pada RPJMN tahun 2025-2029, yaitu "Bersama Indonesia Maju Menuju Indonesia Emas 2045". Misi BSSN juga telah diselaraskan dengan Asta Cita Presiden yang merupakan Misi RPJMN. Sehingga, arah kebijakan, strategi, program, kegiatan hingga SS, IKSS, SP, IKP, SK, IKK, KRO dan RO telah selaras dan mendukung arah pembangunan nasional pada tahun 2025-2029. Renstra BSSN tahun 2025-2029 yang dihasilkan ini akan menjadi pedoman bagi seluruh Unit Kerja dan Satuan Kerja di lingkungan BSSN dalam menyusun Rencana Kerja (Renja), Rencana Kerja dan Anggaran (RKA), Perjanjian

Kinerja (PK) hingga Sasaran Kerja Pegawai (SKP) yang diturunkan dari standar kinerja atasan langsung.

Dalam implementasinya, BSSN menyadari bahwa kebutuhan pendanaan untuk mendukung pembangunan dan penguatan di bidang keamanan siber dan sandi cukup besar. Oleh karena itu, diperlukan pendekatan prioritisasi pelaksanaan program dan kegiatan, guna memastikan bahwa keterbatasan fiskal tidak menghambat pencapaian sasaran strategis utama. Selain itu, pelaksanaan monitoring dan evaluasi yang konsisten dan adaptif menjadi kunci untuk mengantisipasi dinamika kebijakan fiskal yang dapat mempengaruhi pelaksanaan kegiatan, termasuk kegiatan prioritas nasional yang menjadi mandat BSSN.

Renstra BSSN sebagai sebuah perencanaan jangka menengah telah disusun dengan menggunakan metodologi dan pendekatan yang sistematis dengan melibatkan seluruh pejabat maupun ASN di masing-masing unit kerja dan satuan kerja di lingkup BSSN. Dalam implementasinya, dukungan pimpinan maupun seluruh ASN BSSN sangat dibutuhkan untuk memastikan implementasi Renstra BSSN ini sesuai dengan perencanaan yang disusun. Untuk itu, dibutuhkan komitmen yang tinggi kepada seluruh unsur di BSSN dalam melaksanakan Renstra setiap tahunnya, dengan memastikan keselarasan Renja dan RKA dengan Renstra serta melakukan evaluasi secara berkala atas pelaksanaan Renstra BSSN ini.

Lampiran 1 : Matriks Kinerja dan Pendanaan BSSN Tahun 2025 – 2029

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
BADAN SIBER DAN SANDI NEGARA								1.321.637	5.549.633	5.876.303	6.443.308	7.313.775	
SS 1	Meningkatnya keamanan dan ketahanan siber dan sandi nasional												BSSN
IKSS 1.1	Indeks keamanan dan ketahanan siber		0,69	0,73	0,76	0,80	0,84						
IKSS 1.2	Indeks keamanan informasi		0,75	0,78	0,83	0,87	0,90						
SS 2	Meningkatnya pelaksanaan penajaman reformasi birokrasi BSSN												BSSN
IKSS 2.1	Indeks Reformasi Birokrasi BSSN		90,55	91,22	93,31	94,11	95,29						
PROGRAM KEAMANAN DAN KETAHANAN SIBER DAN SANDI NEGARA								848.464	4.857.551	4.798.937	5.341.315	6.163.626	
SP 1	Meningkatnya kematangan PSE dan Penyelenggara Persandian dalam menyelenggarakan keamanan siber dan sandi												Deputi Bidang KSS Pemerintahan dan Pembangunan Manusia dan Deputi Bidang KSS Perekonomian
IKP 1.1	Persentase PSE sektor Pemerintahan dan Pembangunan manusia dengan tingkat kematangan keamanan siber minimum level 3 (terdefinisi)		35%	45%	55%	65%	77%						
IKP 1.2	Persentase PSE sektor Perekonomian dengan tingkat kematangan keamanan siber minimum level 3 (terdefinisi)		24%	34%	44%	54%	64%						
IKP 1.3	Persentase penyelenggara persandian sektor Pemerintahan dengan tingkat kematangan persandian minimal level 3		40%	53%	65%	78%	90%						
IKP 1.4	Nilai Kematangan Keamanan Siber PSE		2,77	2,94	3,19	3,35	3,55						
IKP 1.5	Nilai Kematangan Penyelenggara Persandian		3,00	3,20	3,51	3,58	3,70						
SP 2	Meningkatnya manfaat kerja sama keamanan siber dan sandi dalam pengelolaan strategi dan kebijakan keamanan siber dan sandi												Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi
IKP 2.1	Persentase kerja sama keamanan siber dan sandi yang memberikan manfaat terhadap total kerja sama Siber dan Sandi Nasional terkait pengelolaan strategi dan kebijakan		75%	80%	85%	90%	95%						
SP 3	Meningkatnya manfaat kebijakan keamanan siber dan sandi dalam penanganan gangguan keamanan siber dan sandi												Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi
IKP 3.1	Persentase manfaat (*benefit*) terhadap biaya (*cost*) kebijakan keamanan siber dan sandi nasional		75%	80%	85%	90%	95%						
SP 4	Meningkatnya manfaat kerja sama keamanan siber dan sandi dalam operasi keamanan siber dan sandi												Deputi Bidang Operasi Keamanan Siber dan Sandi
IKP 4.1	Presentase kerja sama operasi keamanan siber dan sandi yang memberikan manfaat terhadap total kerja sama operasi keamanan siber dan sandi nasional		100%	100%	100%	100%	100%						
SP 5	Meningkatnya manfaat kerja sama peningkatan kapasitas keamanan siber dan sandi sektor pemerintahan dan pembangunan manusia												Deputi Bidang KSS Pemerintahan dan Pembangunan Manusia
IKP 5.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi sektor pemerintahan dan pembangunan manusia yang memberikan manfaat terhadap total kerja sama keamanan siber dan sandi nasional		75%	80%	85%	90%	95%						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
SP 6	Meningkatnya manfaat kerja sama peningkatan kapasitas keamanan siber dan sandi sektor perekonomian												Deputi Bidang KSS Perekonomian
IKP 6.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi sektor perekonomian yang memberikan manfaat terhadap total kerja sama siber dan sandi nasional		75%	80%	85%	90%	95%						
SP 7	Meningkatnya kesadaran masyarakat terhadap keamanan siber												Deputi Bidang Operasi Keamanan Siber dan Sandi
IKP 7.1	Tingkat kesadaran masyarakat terhadap keamanan siber		2,8	2,9	3,0	3,1	3,2						
SP 8	Meningkatnya kesadaran K/L/Pemda terhadap keamanan siber												Deputi Bidang KSS Pemerintahan dan Pembangunan Manusia
IKP 8.1	Tingkat kesadaran K/L/Pemda terhadap keamanan siber		2,70	2,80	2,90	3,00	3,10						
SP 9	Meningkatnya kesadaran PSE sektor pembangunan manusia terhadap keamanan siber												Deputi Bidang KSS Pemerintahan dan Pembangunan Manusia
IKP 9.1	Tingkat kesadaran PSE sektor pembangunan manusia terhadap keamanan siber		2,60	2,70	2,80	2,90	3,00						
SP 10	Meningkatnya kesadaran PSE sektor perekonomian terhadap keamanan siber												Deputi Bidang KSS Perekonomian
IKP 10.1	Tingkat kesadaran PSE sektor perekonomian terhadap keamanan siber		2,60	2,70	2,80	2,90	3,01						
SP 11	Meningkatnya kesiapsiagaan dan ketahanan siber nasional												Deputi Bidang Operasi Keamanan Siber dan Sandi
IKP 11.1	Indeks kesiapsiagaan dan ketahanan siber nasional		0,70	0,75	0,77	0,81	0,84						
KEGIATAN : PERUMUSAN KEBIJAKAN KEAMANAN SIBER DAN SANDI								16.713	25.959	24.351	31.572	31.801	
SK 1	Meningkatnya kualitas kerja sama terkait pengelolaan strategi keamanan siber dan sandi												Direktorat Strategi Keamanan Siber dan Sandi
IKK 1.1	Persentase kerja sama terkait pengelolaan strategi keamanan siber dan sandi yang ditindaklanjuti		75%	80%	85%	90%	95%						
IKK 1.2	Persentase peran aktif BSSN dalam kegiatan internasional bidang keamanan siber dan sandi		-	85%	90%	95%	96%						
SK 2	Meningkatnya implementasi kebijakan strategi keamanan siber dan sandi												Direktorat Strategi Keamanan Siber dan Sandi
IKK 2.1	Persentase kebijakan yang diterapkan terhadap total kebijakan teknis strategi keamanan siber dan sandi yang ditetapkan		75%	80%	85%	90%	95%						
SK 3	Meningkatnya kualitas kerja sama terkait pengelolaan kebijakan tata kelola keamanan siber dan sandi												Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi
IKK 3.1	Persentase kerja sama terkait pengelolaan kebijakan tata kelola keamanan siber dan sandi yang ditindaklanjuti		-	80%	85%	90%	95%						
SK 4	Meningkatnya implementasi kebijakan tata kelola keamanan siber dan sandi												Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi
IKK 4.1	Persentase kebijakan yang diterapkan terhadap total kebijakan tata kelola keamanan siber dan sandi yang ditetapkan		75%	80%	85%	90%	95%						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
SK 5	Meningkatnya kualitas kerja sama terkait pengelolaan kebijakan teknologi keamanan siber dan sandi												Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
IKK 5.1	Persentase kerja sama terkait pengelolaan kebijakan teknologi keamanan siber dan sandi yang ditindaklanjuti		75%	80%	85%	90%	95%						
SK 6	Meningkatnya implementasi kebijakan teknologi keamanan siber dan sandi												Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
IKK 6.1	Persentase kebijakan yang diterapkan terhadap total kebijakan teknologi keamanan siber dan sandi yang ditetapkan		75%	80%	85%	90%	95%						
SK 7	Meningkatnya kualitas kerja sama terkait pengelolaan Kebijakan SDM keamanan siber dan sandi												Direktorat Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi
IKK 7.1	Persentase kerja sama terkait pengelolaan kebijakan SDM keamanan siber dan sandi yang ditindaklanjuti		-	80%	85%	90%	95%						
SK 8	Meningkatnya implementasi kebijakan sumber daya manusia keamanan siber dan sandi												Direktorat Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi
IKK 8.1	Persentase kebijakan yang diterapkan terhadap total kebijakan SDM keamanan siber dan sandi yang ditetapkan		75%	80%	85%	90%	95%						
KRO	Kebijakan Bidang Pertahanan dan Keamanan												
	Rekomendasi Kebijakan Prioritas Bidang Strategi Keamanan Siber dan Sandi	Pusat	7	8	8	7	7	4.680	3.032	3.087	2.637	2.637	
	Rekomendasi Kebijakan Prioritas Bidang Tata Kelola Keamanan Siber	Pusat	6	7	8	7	7	2.726	3.048	3.862	3.752	3.822	
	Rekomendasi Kebijakan Prioritas Bidang Teknologi Keamanan Siber dan Sandi	Pusat	5	6	6	7	6	1.563	3.936	4.384	5.558	5.492	
	Rekomendasi Kebijakan Prioritas Bidang SDM Keamanan Siber dan Sandi	Pusat	5	7	6	4	3	2.443	4.761	2.770	1.970	1.370	
	Rekomendasi Kebijakan Bidang Tata Kelola Keamanan Siber dan Sandi dalam rangka tindak lanjut kerja sama	Pusat	-	2	2	2	2	-	900	1.080	1.296	1.555	
	Rekomendasi Kebijakan Bidang Teknologi Keamanan Siber Dan Sandi dalam rangka tindak lanjut kerja sama	Pusat	2	1	1	1	1	661	924	425	450	475	
	Rekomendasi Kebijakan Bidang SDM Keamanan Siber Dan Sandi dalam rangka tindak lanjut kerja sama	Pusat	-	2	2	2	2	-	450	450	450	450	
KRO	Kebijakan Bidang Pertahanan dan Keamanan (RPJMN)												
	Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber (RPJMN)	Pusat	1	1	1	1	1	945	3.507	947	6.841	6.841	
KRO	Standarisasi Produk												
	Rancangan SNI Bidang Keamanan Informasi, Keamanan Siber dan Perlindungan Privasi	Pusat	13	16	15	15	15	620	1.565	1.725	1.984	2.281	
KRO	Standarisasi Profesi dan SDM												

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
	Standarisasi dan Profesi Bidang Sumber Daya Manusia Kebijakan Siber dan Sandi	Pusat	120	140	160	180	200	1.706	648	2.240	2.240	2.240	
KRO	Fasilitasi dan Pembinaan Lembaga												
	Fasilitasi dan Pembinaan Substansi Penambahan Skema Sertifikasi Bidang SDM KSS	Pusat	2	-	-	-	-	467	-	-	-	-	
KRO	Peraturan Lainnya												
	Peraturan Kepala BSSN tentang Pedoman Pengawasan dan Pengendalian Teknologi Keamanan Siber dan Sandi	Pusat	1	-	-	-	-	100	-	-	-	-	
KRO	Peraturan Menteri												
	Peraturan Badan Bidang SDM Keamanan Siber dan Sandi	Pusat	1	-	-	-	-	200	-	-	-	-	
KRO	Kerja sama												
	Kerja Sama Bilateral, Regional dan Multilateral Pengelolaan Strategi Keamanan Siber dan Sandi	Pusat	-	1	1	1	1	-	399	599	898	988	
	Kerja sama Dalam Negeri terkait Pengelolaan Strategi Keamanan Siber dan Sandi	Pusat	-	1	1	1	1	-	266	399	599	898	
KRO	Forum												
	Keterlibatan aktif BSSN dalam kegiatan internasional (keamanan siber, kriptografi, keamanan dan pengendalian informasi, pelindungan IIV)	Pusat	-	14	14	14	14	-	1.720	1.780	1.820	1.910	
KRO	Kerja sama (RPJMN)												
	Kerja sama bilateral dan multilateral di bidang keamanan siber (RPJMN)	Pusat	1	2	1	3	3	603	803	603	1.077	841	
KEGIATAN : PENYELENGGARAAN OPERASI KEAMANAN SIBER DAN SANDI								508.573	3.848.552	3.064.827	3.402.604	3.517.882	
SK 1	Meningkatnya kualitas kerja sama operasi keamanan siber												Direktorat Operasi Keamanan Siber
IKK 1.1	Persentase kerja sama operasi keamanan siber yang ditindaklanjuti		100%	100%	100%	100%	100%						
SK 2	Meningkatnya respon PSE terhadap potensi gangguan keamanan siber risiko tinggi												Direktorat Operasi Keamanan Siber
IKK 2.1	Persentase PSE yang merespons notifikasi potensi gangguan keamanan siber		80%	85%	90%	95%	100%						
SK 3	Meningkatnya akurasi deteksi ancaman gangguan keamanan siber												Direktorat Operasi Keamanan Siber
IKK 3.1	Persentase hasil deteksi ancaman keamanan siber yang tervalidasi benar		80%	82%	84%	86%	88%						
SK 4	Meningkatnya keberhasilan pencegahan potensi ancaman keamanan siber dan keamanan informasi												Direktorat Operasi Keamanan Siber
IKK 4.1	Persentase keberhasilan pencegahan potensi ancaman keamanan siber menjadi insiden pada stakeholder		85%	90%	95%	97%	100%						
SK 5	Meningkatnya efektifitas penanganan insiden keamanan siber												Direktorat Operasi Keamanan Siber
IKK 5.1	Rata-rata waktu yang dibutuhkan dalam memulihkan insiden keamanan siber		36 hari kalender	35 hari kalender	34 hari kalender	33 hari kalender	32 hari kalender						
IKK 5.2	Persentase insiden keamanan siber yang dapat diatasi terhadap total insiden keamanan siber yang terjadi		85%	90%	95%	97%	100%						
SK 6	Terlindunginya Infrastruktur Informasi Vital (IIV) dari serangan siber												Direktorat Operasi Keamanan Siber

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
IKK 6.1	Persentase IIV yang terlindungi terhadap total IIV yang telah ditetapkan oleh sektor		70%	72%	74%	76%	78%						
SK 7	Meningkatnya kualitas kerja sama operasi keamanan dan pengendalian informasi												Direktorat Operasi Keamanan dan Pengendalian Informasi
IKK 7.1	Persentase kerja sama operasi keamanan dan pengendalian informasi yang ditindaklanjuti		-	100%	100%	100%	100%						
SK 8	Meningkatnya pengetahuan dan pemahaman masyarakat terhadap keamanan siber												Direktorat Operasi Keamanan dan Pengendalian InformasI
IKK 8.1	Indeks pengetahuan dan pemahaman masyarakat terhadap keamanan siber		2,8	2,9	3,0	3,1	3,2						
SK 9	Meningkatnya efektifitas penanganan insiden keamanan informasI												
IKK 9.1	Persentase insiden keamanan informasi yang dapat diatasi terhadap total insiden keamanan informasi yang terjadi		100%	100%	100%	100%	100%						
SK 10	Meningkatnya kepatuhan PSE terhadap regulasi dan standar terkait penyelenggaraan sistem elektronik												Direktorat Operasi Keamanan dan Pengendalian InformasI
IKK 10.1	Persentase sistem elektronik yang memenuhi kategori “Patuh” terhadap total sistem elektronik yang didaftarkan		N/A	80%	83%	86%	89%						
SK 11	Meningkatnya kepatuhan K/L/Pemda (IPPD) terhadap peraturan perundang undangan terkait domain keamanan SPBE												Direktorat Operasi Keamanan dan Pengendalian InformasI
IKK 11.1	Rata-rata nilai SPBE K/L/Pemda untuk domain arsitektur keamanan SPBE		100%	100%	100%	100%	100%						
SK 12	Meningkatnya kualitas kerja sama operasi sandi												Direktorat Operasi Sandi
IKK 12.1	Persentase kerja sama operasi sandi yang ditindaklanjuti		100%	100%	100%	100%	100%						
SK 13	Meningkatnya kualitas kerja sama operasi deteksi sinyal												Balai Deteksi Sinyal
IKK 13.1	Persentase kerja sama operasi deteksi sinyal yang ditindaklanjuti		100%	100%	100%	100%	100%						
SK 14	Meningkatnya respon PSE terkait penerapan kriptografi terhadap potensi gangguan keamanan informasi risiko tinggi												Direktorat Operasi Sandi
IKK 14.1	Persentase PSE yang merespon notifikasi terkait penerapan kriptografi dalam mengantisipasi potensi gangguan keamanan informasi risiko tinggi terhadap total PSE yang teridentifikasi memiliki potensi risiko tinggi (*vulnerable*)		85%	88%	90%	95%	100%						
SK 15	Meningkatnya efektifitas penerapan kriptografi dalam mencegah keberhasilan serangan siber												Direktorat Operasi Sandi
IKK 15.1	Persentase penerapan kriptografi yang efektif menjamin perlindungan data dalam sistem elektronik terhadap total insiden siber yang terjadI		100%	100%	100%	100%	100%						
SK 16	Meningkatnya efektifitas penanganan insiden keamanan informasi melalui operasi kriptografi dan keamanan sinyal												Direktorat Operasi Sandi
IKK 16.1	Persentase insiden keamanan informasi yang dapat diatasi melalui operasi kriptografi dan keamanan sinyal terhadap total insiden keamanan informasi yang terjadi		85%	88%	90%	95%	100%						
SK 17	Tersedianya rekomendasi hasil analisis sinyal												Direktorat Operasi Sandi

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
IKK 17.1	Persentase rekomendasi hasil analisis sinyal terhadap deteksi sinyal		80%	83%	90%	93%	95%						
SK 18	Meningkatnya ketersediaan sistem layanan penghubung identitas digital												Balai Layanan Penghubung Identitas Digital
IKK 18.1	Persentase ketersediaan sistem layanan penghubung identitas digital		98,00%	98,25%	98,50%	98,75%	99,00%						
KRO	Operasi Bidang Keamanan												
	Operasi Keamanan Siber	Pusat	95	162	168	195	226	5.011	8.369	8.679	10.088	11.720	
	Operasi Keamanan dan Pengendalian Informasi	Pusat	17	40	40	40	40	2.635	53.905	56.600	59.430	62.402	
	Operasi Pengamanan Sinyal	Pusat	40	50	60	70	80	1.917	4.724	5.669	6.803	8.164	
	Operasi Pengamanan Informasi dengan Penerapan Fungsi Kriptografi	Pusat	65	75	80	100	115	2.611	8.703	10.444	12.533	15.039	
	Operasi Deteksi dan Analisis Sinyal	Pusat	3	4	5	5	5	1.349	3.707	3.807	3.907	4.007	
	Operasi Keamanan Siber pada Event Nasional dan Internasional	Pusat	-	8	8	8	8	-	131.241	160.485	193.481	231.717	
	VVIP Program	Pusat	-	11	11	11	11	-	833	809	838	971	
	Operasi Penanganan Insiden Keamanan Siber	Pusat	-	34	39	44	49	-	1.985	2.787	3.804	5.107	
	Operasi Penyelenggaraan Perlindungan IIV	Pusat	-	8	8	8	8	-	556	667	779	890	
	Operasi Penanganan Insiden Keamanan Siber Bersama Lintas Negara	Pusat	-	2	3	4	5	-	362	553	774	995	
	Operasi Forensik Digital Terkait Penanganan Insiden Keamanan Siber	Pusat	-	30	35	40	45	-	4.335	4.812	5.462	6.080	
	Operasi Keamanan dan Pengendalian Informasi dalam rangka tindak lanjut kerja sama	Pusat	-	11	11	11	11	-	118.942	119.033	70.533	72.128	
	Operasi sandi dalam rangka tindak lanjut kerja sama	Pusat	-	2	2	2	2	-	198	238	286	343	
	Operasi deteksi sinyal dalam rangka tindak lanjut kerja sama	Pusat	-	1	1	1	1	-	374	406	498	544	
KRO	Operasi Bidang Keamanan (RPJMN)												
	Operasi Audit Keamanan SPBE (RPJMN)	Pusat	13	15	18	20	23	2.242	8.032	9.161	10.234	11.094	
	Operasi Penanganan perkara cyber related crime (RPJMN)	Pusat	1	1	1	1	1	488	586	704	845	1.013	
	Peningkatan Budaya Keamanan Siber + Pengukuran Tingkat Kesadaran Kamsiber (RPJMN)	Pusat	4	4	4	4	4	366	439	527	632	758	
	Operasi Pengamanan Siber dan Sandi pada Penyelenggaraan Pemilu Tahun 2029 (RPJMN)	Pusat	-	-	-	58	53	-	-	-	29.000	27.800	
	Operasi Dukungan Penyidikan dalam rangka Pengungkapan Perkara Siber (RPJMN)	Pusat	-	3	3	3	3	-	1.500	1.500	1.500	1.500	
	Operasi Profiling Sinyal di Kawasan Indo-Pasifik (RPJMN)	Pusat	-	3	3	3	3	-	4.020	1.190	1.433	1.326	
KRO	Forum												
	Forum keamanan siber	Pusat	5	8	9	10	11	501	1.709	2.134	2.645	3.036	
	Forum potensi ancaman keamanan siber	Pusat	-	5	7	8	8	-	600	950	1.200	1.200	
KRO	Kebijakan Bidang Pertahanan dan Keamanan (RPJMN)												
	Roadmap Peningkatan Budaya Keamanan Informasi (RPJMN)	Pusat	1	-	-	-	-	197	-	-	-	-	
KRO	Peraturan Menteri												
	Peraturan Badan Siber dan Sandi Negara Tentang Pedoman Pembentukan Security Operation Center	Pusat	1	-	-	-	-	200	-	-	-	-	
	Peraturan BSSN Bidang Operasi Keamanan Siber	Pusat	-	1	-	-	-	-	200	-	-	-	
KRO	Konferensi dan Event												

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
	Konferensi dan Event Keamanan Siber	Pusat	-	5	5	5	5	-	3.176	3.313	3.630	4.028	
KRO	Kebijakan Bidang Pertahanan dan Keamanan												
	Rekomendasi kebijakan rencana penanganan risiko keamanan informasi terkait penerapan kriptografi	Pusat	-	1	-	1	-	-	39	-	47	-	
	Rekomendasi kebijakan rencana penanganan risiko keamanan siber	Pusat	-	-	1	-	1	-	-	240	-	288	
	Rekomendasi kebijakan rencana penanganan risiko keamanan informasi	Pusat	-	1	1	1	1	-	8	9	10	11	
	Kajian rekomendasi kebijakan bidang operasi keamanan siber	Pusat	-	7	7	8	8	-	3.330	3.356	3.843	3.886	
KRO	Koordinasi												
	Koordinasi Program ISAC	Pusat	-	1	1	1	1	-	700	700	700	700	
	Koordinasi dan pendampingan tindak lanjut notifikasi ancaman keamanan siber	Pusat	-	10	15	20	25	-	440	720	1.040	1.400	
	Koordinasi dan pendampingan tindak lanjut notifikasi penerapan kriptografi dalam mengantisipasi potensi ancaman keamanan siber	Pusat	-	10	10	10	10	-	658	790	948	1.137	
KRO	Sosialisasi dan Diseminasi												
	Sosialisasi Diseminasi Layanan Penghubung Identitas Digital	Pusat		120	140	160	180	-	360	420	480	540	
KRO	Pelayanan Publik kepada Lembaga												
	Layanan Integrasi Sistem Elektronik instansi Penyelenggara Negara	Pusat	-	4	8	16	24	-	2.000	3.000	5.000	7.000	
KRO	Fasilitasi dan Pembinaan Lembaga												
	National Cyber Exercise	Pusat	-	50	75	100	125	-	650	975	1.300	1.625	
	Simulasi Rencana Kontingensi	Pusat	-	50	75	100	125	-	500	750	1.000	1.250	
KRO	Sarana Bidang Pertahanan dan Keamanan												
	Optimalisasi Dukungan NSOC	Pusat	-	1	1	1	1	-	2.791	2.930	3.077	3.231	
	Penguatan National Security Operation Center (NSOC) (PHLN)	Pusat	-	1	1	1	1	-	628.929	628.929	628.929	628.929	
	Pembangunan Sistem Pengelolaan Bukti Digital	Pusat	-	1	1	1	1	-	15.000	30.000	25.000	35.000	
	Pengembangan Sistem VVIP	Pusat	-	1	-	-	-	-	25.718	-	-	-	
	Infrastruktur Layanan Penghubung Identitas Digital	Pusat	-	1	-	1	-	-	150.000	-	150.000	-	
KRO	Sarana Bidang Pertahanan dan Keamanan (RPJMN)												
	Sistem Pemantauan dan Deteksi Serangan Siber Sosial (RPJMN)	Pusat	3	3	3	3	3	90.000	15.000	15.000	15.000	15.000	
	Perluasan Cakupan Perangkat Traffic analysis National Security Operation Center (NSOC) (RPJMN)	Pusat	1	3	3	3	3	255.487	975.000	1.121.250	1.289.438	1.482.853	
	Peralatan Operasi Pengamanan Sinyal (RPJMN)	Pusat	-	1	1	1	1	-	250.000	108.149	67.738	67.738 -	
	Infrastruktur Kriptografi Nasional (Cryptography as a Service) (RPJMN)	Pusat	1	-	1	-	1	45.569	-	36.109	-	36.109	
	Sistem Pelindungan Infrastruktur Informasi Vital (RPJMN)	Pusat	-	1	-	-	-	-	110.000	-	-	-	
	Platform National Cyber Threat Database (RPJMN)	Pusat	-	-	-	2	2	-	-	-	50.000	50.000	
	Sistem Penelusuran Indikasi Potensi Ancaman Siber (RPJMN)	Pusat	-	1	-	-	-	-	5.001	-	-	-	
	Sistem Terintegrasi Audit Keamanan SPBE (RPJMN)	Pusat	-	2	1	1	1	-	60.000	5.000	5.000	5.000	
	Penguatan Perangkat Command Center Kriptografi (RPJMN)	Pusat	-	-	-	1	1	-	-	-	50.000	50.000	
	Sarana Operasi Analisis Sinyal (RPJMN)	Pusat	1	1	1	1	1	100.000	200.000	200.000	200.000	200.000	
	Pembangunan SSOC IKN (Perpres 63 2022)	Pusat	-	1	1	1	1	-	690.041	102.946	9.679	9.679	
	Penguatan ekosistem keamanan siber di Indonesia (PHLN)	Pusat	1	-	-	-	-	0,10	-	-	-	-	
	Optimalisasi sistem pemantauan dan deteksi ancaman siber sosial (PHLN)	Pusat	1	-	-	-	-	0,10	-	-	-	-	

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
	Peningkatan kapasitas sistem pengalihan serangan siber (RPJMN)	Pusat	-	-	-	1	1	-	-	-	27.000	5.000	
	Sistem Pangkalan Data Insiden Siber (RPJMN)	Pusat	-	-	-	1	1	-	-	-	35.000	24.500	
KRO	OP Sarana Bidang Pertahanan dan Keamanan												
	Maintenance Data Center NSOC	Pusat	-	1	1	1	1	-	3.892	4.087	4.291	4.506	
	Pemeliharaan SSOC IKN (Perpres 63 2022)	Pusat	-	-	1	1	1	-	-	55.000	57.750	60.638	
KRO	Prasarana Bidang Pertahanan dan Keamanan (RPJMN)												
	Pembangunan National Signal Analysis (RPJMN)	Pusat	-	1	1	1	1	-	350.000	350.000	350.000	350.000	
KEGIATAN : PENGEMBANGAN KAPASITAS KEAMANAN SIBER DAN SANDI SEKTOR PEMERINTAHAN DAN PEMBANGUNAN MANUSIA								17.618	79.369	86.448	99.600	112.284	
SK 1	Meningkatnya kematangan keamanan siber dan sandi PSE Sektor Pemerintah Pusat												Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
IKK 1.1	Nilai kematangan keamanan siber PSE Sektor Pemerintah Pusat		3,00	3,20	3,51	3,60	3,80						
IKK 1.2	Nilai kematangan penyelenggara persandian Sektor Pemerintah Pusat		3,00	3,20	3,51	3,60	3,80						
SK 2	Meningkatnya pengetahuan dan pemahaman K/L terhadap keamanan siber												Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
IKK 2.1	Indeks pengetahuan dan pemahaman K/L terhadap keamanan siber		2,80	2,90	3,00	3,10	3,20						
SK 3	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Pemerintah Pusat												Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
IKK 3.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Pemerintah Pusat yang ditindaklanjuti		75%	80%	85%	90%	95%						
SK 4	Meningkatnya kematangan keamanan siber dan sandi PSE Sektor Pemerintah Daerah												Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
IKK 4.1	Nilai kematangan keamanan siber PSE Sektor Pemerintah Daerah		3,00	3,20	3,51	3,55	3,60						
IKK 4.2	Nilai kematangan penyelenggara persandian Sektor Pemerintah Daerah		3,00	3,20	3,51	3,55	3,60						
SK 5	Meningkatnya pengetahuan dan pemahaman Pemerintah Daerah terhadap keamanan siber												Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
IKK 5.1	Indeks pengetahuan dan pemahaman Pemerintah Daerah terhadap keamanan siber		2,60	2,70	2,80	2,90	3,00						
SK 6	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Pemerintah Daerah												Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
IKK 6.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi Sektor Pemerintah Daerah yang ditindaklanjuti		-	80%	85%	90%	95%						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
SK 7	Meningkatnya kematangan keamanan siber PSE Sektor Pembangunan Manusia												Direktorat Keamanan Siber dan Sandi Pembangunan Manusia
IKK 7.1	Nilai kematangan keamanan siber PSE sektor pembangunan manusia		3,00	3,10	3,20	3,30	3,40						
SK 8	Meningkatnya pengetahuan dan pemahaman PSE sektor Pembangunan manusia terhadap keamanan siber												Direktorat Keamanan Siber dan Sandi Pembangunan Manusia
IKK 8.1	Indeks pengetahuan dan pemahaman PSE sektor Pembangunan manusia terhadap keamanan siber		2,60	2,70	2,80	2,90	3,00						
SK 9	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi sektor pembangunan manusia												Direktorat Keamanan Siber dan Sandi Pembangunan Manusia
IKK 9.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Pembangunan Manusia yang ditindaklanjuti		75%	80%	85%	90%	95%						
KRO	Peraturan Menteri (RPJMN)												
	Peraturan BSSN tentang Peta Jalan Pelindungan IIV Sektor Administrasi Pemerintahan Tahun 2030-2034 (RPJMN)	Pusat	-	-	-	-	1	-	-	-	-	350	
KRO	Kebijakan Bidang Pertahanan dan Keamanan												
	Rekomendasi kebijakan terkait evaluasi Peta Jalan Pelindungan IIV Sektor Pertahanan	Pusat	-	1	1	1	1	-	250	275	300	325	
KRO	Kebijakan Bidang Pertahanan dan Keamanan (RPJMN)												
	Penyusunan Peta Jalan Pelindungan IIV Sektor Pertahanan (RPJMN)	Pusat	1	-	-	-	-	257	-	-	-	-	
KRO	Koordinasi												
	Forum Koordinasi Kematangan Keamanan Siber dan Sandi Pemerintah Pusat	Pusat	-	6	6	6	6	-	2.785	2.239	2.327	2.423	
	Forum Pengawasan Kepatuhan Keamanan Siber PSE sektor Pemerintah Pusat dalam rangka tindak lanjut Kerja sama Regional dan Bilateral	Pusat	-	3	3	3	2	-	1.610	1.788	1.926	1.703	
	Koordinasi pengukuran kematangan keamanan siber sektor pembangunan manusia	Pusat	-	2	2	2	2	-	1.080	432	475	523	
	Forum Koordinasi Perlindungan IIV Sektor Pembangunan Manusia	Pusat	-	1	1	1	1	-	390	216	238	261	
KRO	Sosialisasi dan Diseminasi												
	Diseminasi kebijakan kriptografi nasional di sektor IIV Pemerintah Daerah	Pusat	-	100	200	200	200	-	226	516	516	516	
KRO	Fasilitasi dan Pembinaan Lembaga												
	Fasilitasi dan Pembinaan Kematangan Keamanan Siber Pemerintah Pusat	Pusat	15	18	18	18	18	2.768	3.972	5.089	6.430	7.848	
	Fasilitasi dan Pembinaan Kematangan Keamanan Siber Pembangunan Manusia	Pusat	10	80	80	80	80	1.889	9.761	10.178	11.196	12.316	
	Program peningkatan pengetahuan keamanan siber dan sandi PSE Sektor Pembangunan Manusia	Pusat	-	24	28	32	40	-	1.127	605	666	732	
	Program tindak lanjut kerja sama regional dan bilateral terkait Peningkatan kapasitas keamanan siber PSE sektor Pembangunan Manusia	Pusat	-	-	-	1	1	-	-	-	335	369	

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
	Program tindak lanjut kerja sama dalam negeri terkait peningkatan kapasitas keamanan siber PSE sektor Pembangunan Manusia	Pusat	-	2	2	2	2	-	226	249	274	301	
	Pengawasan kepatuhan keamanan siber PSE sektor Pemerintah Pusat dalam rangka tindak lanjut kerja sama dalam negeri	Pusat	-	125	125	125	125	-	12.484	13.244	13.832	14.421	
KRO	Fasilitasi dan Pembinaan Lembaga (RPJMN)												
	Pembinaan peningkatan kapasitas keamanan SPBE lingkup instansi pengelola aplikasi umum dan inisiatif strategis arsitektur SPBE Nasional (RPJMN)	Pusat	24	32	32	32	32	1.161	3.211	3.471	3.087	2.985	
	Pembinaan kematangan keamanan siber Sektor Administrasi Pemerintahan : Pemerintah Pusat (RPJMN)	Pusat	105	160	160	160	160	5.962	18.784	25.235	30.959	34.989	
KRO	Fasilitasi dan Pembinaan Pemerintah Daerah												
	Fasilitasi dan Pembinaan Penyelenggaraan Keamanan Siber dan Sandi Pemerintah Daerah	Pusat	65	65	65	65	65	1.337	1.986	2.085	2.190	2.299	
	Peningkatan kapasitas keamanan siber PSE sektor Pemerintah Daerah dalam rangka tindak lanjut Kerja sama	Pusat	-	2	2	2	2	-	1.838	1.838	1.838	1.838	
KRO	Fasilitasi dan Pembinaan Pemerintah Daerah (RPJMN)												
	Pembinaan Kematangan Keamanan Siber Sektor Administrasi Pemerintahan: Pemerintah Daerah (RPJMN)	Pusat	7	14	21	28	34	3.212	4.423	4.192	4.483	4.159	
	Penguatan Ekosistem Keamanan Siber dan Sandi pada Provinsi Baru (RPJMN))	Pusat	4	4	4	4	4	1.033	1.166	1.913	2.056	2.799	
KRO	Peningkatan Kapasitas Aparatur Negara												
	Bimtek penyelenggaraan keamanan siber dan sandi pemerintah daerah	Pusat	-	300	300	300	300	-	1.042	1.094	1.149	1.207	
KRO	Sarana Bidang Pertahanan dan Keamanan (RPJMN)												
	Sistem Pengawasan Kepatuhan Penanganan Insiden pada TTIS Organisasi Sektor Administrasi Pemerintahan (RPJMN)	Pusat	-	1	1	1	1	-	13.008	11.789	15.325	19.923	
KEGIATAN : PENGEMBANGAN KAPASITAS KEAMANAN SIBER DAN SANDI SEKTOR PEREKONOMIAN								14.868	76.164	73.827	78.813	91.906	
SK 1	Meningkatnya kematangan keamanan siber PSE sektor Keuangan, Perdagangan, Pariwisata dan Ekonomi Kreatif												Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata
IKK 1.1	Nilai kematangan Keamanan siber PSE sektor Keuangan, Perdagangan, Pariwisata dan Ekonomi Kreatif		2,60	2,80	3,10	3,30	3,51						
SK 2	Meningkatnya pengetahuan dan pemahaman PSE sektor Keuangan, Perdagangan, Pariwisata dan Ekonomi Kreatif terhadap keamanan siber												Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata
IKK 2.1	Indeks pengetahuan dan pemahaman PSE sektor Keuangan, Perdagangan, Pariwisata dan Ekonomi Kreatif terhadap keamanan siber		2,60	2,70	2,80	2,90	3,01						
SK 3	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Keuangan, Perdagangan, Pariwisata dan Ekonomi Kreatif												Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata
IKK 3.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Keuangan, Perdagangan, Pariwisata dan Ekonomi Kreatif yang ditindaklanjuti		75%	80%	85%	90%	95%						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
SK 4	Meningkatnya kematangan keamanan siber PSE Sektor Energi dan Sumber Daya Alam												Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam
IKK 4.1	Nilai kematangan keamanan siber PSE Sektor Energi dan Sumber Daya Alam		2,60	2,80	3,10	3,30	3,51						
SK 5	Meningkatnya pengetahuan dan pemahaman PSE Sektor Energi dan Sumber Daya Alam terhadap keamanan siber												Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam
IKK 5.1	Indeks pengetahuan dan pemahaman PSE Sektor Energi dan Sumber Daya Alam terhadap keamanan siber		2,60	2,70	2,80	2,90	3,01						
SK 6	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi PSE Sektor Energi dan Sumber Daya Alam												Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam
IKK 6.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi PSE Sektor Energi dan Sumber Daya Alam yang ditindaklanjuti		75%	80%	85%	90%	95%						
SK 7	Meningkatnya kematangan keamanan siber PSE sektor TIK, media, transportasi serta logistik												Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi
IKK 7.1	Nilai kematangan Keamanan siber PSE sektor TIK, media, transportasi serta logistik		2,60	2,80	3,10	3,30	3,51						
SK 8	Meningkatnya pengetahuan dan pemahaman PSE sektor TIK, media, transportasi serta logistik terhadap keamanan siber dan sandi												Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi
IKK 8.1	Indeks pengetahuan dan pemahaman PSE sektor TIK, media, transportasi serta logistik terhadap keamanan siber dan sandi		2,60	2,70	2,80	2,90	3,01						
SK 9	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi sektor TIK, Media dan Transportasi serta Logistik												Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi
IKK 9.1	Persentase kerja sama peningkatan kapasitas keamanan siber PSE sektor TIK, Media dan Transportasi serta logistik yang ditindaklanjuti		75%	80%	85%	90%	95%						
SK 10	Meningkatnya kematangan keamanan siber PSE sektor industri dan jasa konstruksi												Direktorat Keamanan Siber dan Sandi Industri
IKK 10.1	Nilai kematangan keamanan siber PSE sektor industri dan jasa konstruksi		2,60	2,70	2,80	3,10	3,51						
SK 11	Meningkatnya pengetahuan dan pemahaman PSE sektor industri dan jasa konstruksi terhadap keamanan siber dan sandi												Direktorat Keamanan Siber dan Sandi Industri
IKK 11.1	Indeks pengetahuan dan pemahaman PSE sektor industri dan jasa konstruksi terhadap keamanan siber		2,60	2,70	2,80	2,90	3,01						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
SK 12	Meningkatnya kualitas kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Industri dan jasa konstruksi												Direktorat Keamanan Siber dan Sandi Industri
IKK 12.1	Persentase kerja sama peningkatan kapasitas keamanan siber dan sandi sektor Industri dan jasa konstruksi yang ditindaklanjuti		75%	80%	85%	90%	95%						
KRO	Koordinasi												
	Forum Koordinasi Analisis dan Berbagi Informasi Kamsiber Sektor Keuangan	Pusat	-	1	1	1	1	-	318	426	468	515	
	Forum Koordinasi Analisis dan Berbagi Informasi Kamsiber Sektor ESDA	Pusat	-	5	1	1	1	-	1.474	391	413	526	
	Forum Koordinasi Pengukuran Kematangan Keamanan Siber Sektor TIK, Media dan Transportasi	Pusat	-	1	1	1	1	-	229	180	206	247	
	Forum Koordinasi Pengukuran Kematangan Keamanan Siber Sektor Industri dan Jasa Konstruksi	Pusat	-	1	1	1	1	-	712	1.067	1.601	2.401	
	Forum Koordinasi perlindungan IIV sektor TIK, Media, dan Transportasi	Pusat	-	1	1	1	1	-	257	211	207	279	
	Forum Koordinasi Perlindungan IIV sektor Industri	Pusat	-	-	1	1	1	-	-	241	289	346	
KRO	Fasilitasi dan Pembinaan Lembaga												
	Fasilitasi dan Pembinaan Kematangan Keamanan Siber Sektor Keuangan, Perdagangan dan Pariwisata	Pusat	10	45	10	10	10	743	1.781	8.300	9.130	10.042	
	Fasilitasi dan Pembinaan Kematangan Keamanan Siber Sektor Energi dan Sumber Daya Alam	Pusat	10	10	10	10	10	389	1.658	2.177	2.660	2.350	
	Fasilitasi dan Pembinaan Kematangan Keamanan Siber Sektor TIK, Media dan Transportasi	Pusat	20	22	24	26	28	777	6.854	7.519	8.271	9.098	
	Fasilitasi dan Pembinaan Kematangan Keamanan Siber Sektor Industri dan Jasa Konstruksi	Pusat	10	10	10	10	10	2.487	10.126	8.478	9.236	10.065	
	Program peningkatan pengetahuan keamanan siber dan sandi Lembaga Sektor ESDA	Pusat	-	40	10	10	10	-	1.545	1.740	1.819	2.049	
	Program peningkatan pengetahuan keamanan siber dan sandi sektor keuangan, perdagangan, pariwisata dan ekonomi kreatif	Pusat	-	20	10	10	10	-	2.043	1.177	1.295	1.425	
	Program peningkatan pengetahuan keamanan siber dan sandi Sektor TIK, Media dan Transportasi	Pusat	-	42	24	26	28	-	4.740	3.760	4.136	4.549	
	Program peningkatan pengetahuan keamanan siber dan sandi Sektor Industri dan Jasa Konstruksi	Pusat	-	85	95	105	115	-	4.742	3.104	3.725	4.470	
	Program tindak lanjut kerja sama terkait peningkatan kapasitas keamanan siber PSE sektor Keuangan, Perdagangan dan Pariwisata	Pusat	-	-	2	2	2	-	-	3.995	4.394	4.834	
	Program tindak lanjut kerja sama terkait peningkatan kapasitas keamanan siber PSE sektor Energi dan Sumber Daya Alam	Pusat	-	-	2	2	2	-	-	1.202	1.650	1.235	
	Program tindak lanjut kerja sama terkait peningkatan kapasitas keamanan siber PSE sektor TIK, Media dan Transportasi	Pusat	-	2	2	2	2	-	287	1.202	1.650	1.235	
	Program tindak lanjut kerja sama terkait peningkatan kapasitas keamanan siber PSE sektor Industri	Pusat	-	2	2	2	2	-	1.295	1.307	1.321	1.334	
KRO	Fasilitasi dan Pembinaan Lembaga (RPJMN)												
	Pembinaan Kematangan Keamanan Siber Sektor Keuangan (RPJMN)	Pusat	60	50	60	60	60	2.668	8.740	4.061	4.467	4.913	
	Pembinaan Kematangan Keamanan Siber Sektor ESDM dan Pangan (RPJMN)	Pusat	45	82	45	45	45	3.125	19.859	6.776	7.668	7.835	
	Pembinaan Kematangan Keamanan Siber Sektor TIK dan Transportasi (RPJMN)	Pusat	50	60	70	80	90	2.875	6.603	10.158	10.844	13.489	
	Tim Tanggap Insiden Siber (CSIRT) IIV Sektor Keuangan yang teregistrasi (RPJMN)	Pusat	-	-	-	-	1	-	-	-	-	1.200	
	Tim Tanggap Insiden Siber (CSIRT) IIV Sektor ESDM dan Pangan yang teregistrasi (RPJMN)	Pusat	-	1	-	1	-	-	895	-	732	-	

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
	Tim Tanggap Insiden Siber (CSIRT) IIV Sektor TIK dan Transportasi yang teregistrasi (RPJMN)	Pusat	-	1	-	-	1	-	666	-	-	1.200	
	Pembinaan Kematangan Keamanan Siber Sektor Kesehatan (RPJMN)	Pusat	-	40	60	80	100	-	1.343	1.881	2.633	3.686	
KRO	Kebijakan Bidang Pertahanan dan Keamanan												
	Rekomendasi kebijakan untuk penerapan standar keamanan pada Sektor Transportasi dan TIK	Pusat	1	-	-	-	-	94	-	-	-	-	
KRO	Kebijakan Bidang Pertahanan dan Keamanan (RPJMN)												
	Peta Jalan Pelindungan IIV Sektor Keuangan (RPJMN)	Pusat	1	-	-	-	1	659	-	-	-	1,952	
	Peta Jalan Pelindungan IIV Sektor ESDM dan Pangan (RPJMN)	Pusat	1	-	1	-	-	621	-	4,475	-	-	
	Peta Jalan Pelindungan IIV Sektor TIK dan Transportasi (RPJMN)	Pusat	1	-	-	-	1	431	-	-	-	630	
KEGIATAN : PENGEMBANGAN SDM KEAMANAN SIBER DAN SANDI								14.717	19.788	21.723	23.849	26.186	
SK 1	Meningkatnya Kompetensi SDM Keamanan Siber dan Sandi												Pusat Pengembangan SDM
IKK 1.1	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi		16%	14%	12%	10%	8%						
IKK 1.2	Persentase lulusan pelatihan SDM Keamanan Siber dan Sandi dengan nilai minimal memuaskan		75%	76%	77%	78%	79%						
KRO	Sertifikasi Profesi dan SDM												
	Sertifikasi SDM Keamanan Siber dan Sandi	Pusat	245	245	245	245	245	667	876	920	966	1.015	
KRO	Sertifikasi Profesi dan SDM (RPJMN)												
	Sertifikasi SDM Berdasarkan Standar Kompetensi Keamanan Siber dan Sandi (RPJMN)	Pusat	360	360	360	360	360	498	813	895	984	1.083	
KRO	Pelatihan Bidang Politik, Hukum, Pertahanan dan Keamanan												
	Lulusan Pendidikan dan Pelatihan SDM Keamanan Siber dan Sandi	Pusat	1.219	1.219	1.219	1.219	1.219	9.562	11.638	12.801	14.082	15.490	
KRO	Pelatihan Bidang Politik, Hukum, Pertahanan dan Keamanan (RPJMN)												
	Pelatihan bagi SDM Keamanan SPBE (RPJMN)	Pusat	300	300	300	300	300	1.155	1.874	2.061	2.267	2.494	
	Pelatihan Peningkatan Kompetensi SDM Berdasarkan Standar Kompetensi Keamanan Siber dan Sandi (RPJMN)	Pusat	325	325	325	325	325	1.121	1.236	1.360	1.496	1.645	
	Pelatihan Teknis Bidang Keamanan Siber dan Sandi (RPJMN)	Pusat	325	275	275	275	275	1.714	2.434	2.677	2.945	3.240	
KRO	Pemantauan dan Evaluasi Serta Pelaporan												
	Evaluasi Penyelenggaraan Sertifikasi Kompetensi SDM Keamanan Siber dan Sandi	Pusat	-	1	1	1	1	-	313	345	379	417	
KRO	Akreditasi Lembaga												
	Akreditasi Program Pelatihan Teknis KSS	Pusat	-	1	1	1	1	-	209	229	252	278	
KRO	Fasilitasi dan Pembinaan Lembaga												
	Fasilitasi dan Pembinaan Lembaga dalam rangka tindak lanjut kerja sama	Pusat	-	4	4	4	4	-	395	434	478	526	
KEGIATAN : PENDIDIKAN PROFESIONAL DI BIDANG SIBER DAN SANDI								34.064	250.450	157.248	67.209	94.302	
SK 1	Meningkatnya pendidikan profesional SDM siber dan sandi yang berkualitas												Politeknik Siber dan Sandi Negara
IKK 1.1	Persentase lulusan SDM siber dan sandi dengan nilai pendidikan minimum “Baik”		75%	77%	79%	81%	83%						
IKK 1.2	Tingkat penerimaan (*acceptance rate*) publikasi penelitian bidang Keamanan Siber dan Kriptografi terakreditasi Nasional atau Internasional		70%	71%	73%	75%	77%						
IKK 1.3	Persentase program pengabdian kepada masyarakat yang termanfaatkan oleh masyarakat		80%	81%	83%	85%	87%						
IKK 1.4	Persentase ketercapaian standar mutu pendidikan		75%	77%	79%	81%	83%						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
KRO	Kerja sama												
	Kerja sama Pendidikan Tinggi	Pusat	4	2	3	3	3	292	336	580	667	767	
KRO	Konferensi dan Event												
	Konferensi dan Event Poltek SSN	Pusat	3	4	5	4	5	1.062	2.582	3.378	3.415	4.397	
KRO	Promosi												
	Promosi Poltek SSN	Pusat	2	3	3	3	3	122	141	162	186	214	
KRO	Sarana Bidang Pendidikan												
	Sarana Pendidikan Poltek SSN	Pusat	1	14	8	5	4	2.500	18.857	9.581	3.300	19.960	
KRO	Pendidikan Tinggi												
	Taruna Yang Naik Tingkat dan Lulusan Politeknik Siber dan Sandi Negara	Pusat	423	476	630	755	900	30.064	42.320	47.396	54.705	62.060	
	Penelitian Dosen Poltek SSN	Pusat	-	54	57	60	62	-	3.513	3.947	4.456	4.770	
	Pengabdian Poltek SSN Kepada Masyarakat	Pusat	-	4	4	4	4	-	320	400	480	560	
KRO	Prasarana Bidang Pendidikan Tinggi (RPJMN)												
	Fasilitas Pembangunan Sumber Daya Manusia Keamanan Siber dan Sandi Yang Terbangun di Poltek SSN (RPJMN)	Pusat	-	7	3	-	1	-	182.381	91.804	-	1.573	
KEGIATAN : PENYELENGGARAAN SERTIFIKASI ELEKTRONIK								32.657	347.475	337.598	317.170	341.875	
SK 1	Meningkatnya kualitas layanan sertifikat elektronik BSSN												Balai Besar Sertifikasi Elektronik
IKK 1.1	Persentase ketersediaan sistem sertifikasi elektronik		98.00%	98.50%	99.00%	99.05%	99.10%						
IKK 1.2	Rata-rata waktu yang dibutuhkan untuk menerbitkan sertifikat elektronik		60 detik	55 detik	50 detik	45 detik	40 detik						
IKK 1.3	Rata-rata waktu pemanfaatan layanan sertifikat elektronik		2 detik	1,8 detik	1,6 detik	1,4 detik	1,2 detik						
IKK 1.4	Persentase sertifikat elektronik yang dimanfaatkan terhadap total sertifikat elektronik yang diterbitkan		50%	55%	60%	65%	70%						
SK 2	Meningkatnya kepuasan pengguna Layanan Sertifikat Elektronik												Balai Besar Sertfikasi Elektronik
IKK 2.1	Tingkat kepuasan atas Layanan Sertifikat Elektronik		88,00%	89,00%	90,00%	90,05%	90,10%						
KRO	Pelayanan Publik kepada Lembaga (RPJMN)												
	Optimalisasi Pemanfaatan Sertifikat Elektronik dalam Mendukung Pemerintahan Digital (RPJMN)	Pusat	-	18	40	68	100	-	4.380	8.400	11.900	15.400	
KRO	Pelayanan Publik kepada masyarakat												
	Layanan Sertifikasi Elektronik	Pusat	800.000	900.000	1.000.000	1.100.000	1.200.000	21.689	108.668	123.500	134.000	144.500	
KRO	Prasarana Bidang Pertahanan dan Keamanan (RPJMN)												
	Penerapan Sertifikat Elektronik pada Pelayanan Publik (RPJMN)	Pusat	-	2	1	1	1	-	204.095	176.698	139.270	146.975	
KRO	OP Sarana Bidang Pertahanan dan Keamanan												
	Pemeliharaan sarana bidang pertahanan dan keamanan sertifikasi elektronik	Pusat	1	1	1	1	1	10.968	30.332	29.000	32.000	35.000	
KEGIATAN : PEMELIHARAAN PERALATAN KEAMANAN SIBER DAN SANDI								203.546	189.821	1.016.715	1.301.233	1.859.531	
SK 1	Terpeliharanya Peralatan Keamanan Siber dan Sandi												
IKK 1.1	Persentase Pemenuhan Pemeliharaan Perangkat Keamanan Siber dan Sandi		100%	100%	100%	100%	100%						
KRO	OP Sarana Bidang Pertahanan dan Keamanan												
	Dukungan Pemeliharaan Peralatan Keamanan Siber dan Sandi	Pusat	2	3	3	3	3	200.095	188.836	517.362	776.961	1.309.094	
KRO	Sarana Bidang Pertahanan dan Keamanan												
	Dukungan Sarana Keamanan Data Strategis	Pusat	8	-	-	-	-	3.451	-	-	-	-	

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
	Penguatan dan Pembangunan Pusat Data sebagai Rekam Cadang Data Elektronik Strategis Nasional	Pusat	-	-	1	1	1	-	-	498.370	523.288	549.452	
KRO	Sistem Informasi Pemerintahan												
	Sistem Informasi Eksternal	Pusat	-	5	5	5	5	-	984	984	984	984	
KEGIATAN : PENYELENGGARAAN SERTIFIKASI TEKNOLOGI KEAMANAN SIBER DAN SANDI								5.709	19.973	16.201	19.265	87.859	
SK 1	Meningkatnya Produk Teknologi Keamanan Siber dan Sandi yang Tersertifikasi												Pusertif
IKK 1.1	Persentase produk teknologi keamanan siber dan sandi yang tersertifikasi tepat waktu dari total pengajuan sertifikasi		80%	81%	82%	84%	86%						
SK 2	Meningkatnya Produk Teknologi Keamanan Siber dan Sandi yang telah Lulus Uji												Pusertif
IKK 2.1	Persentase produk teknologi keamanan siber dan sandi yang lulus uji tepat waktu dari total pengajuan pengujian		82%	83%	84%	86%	88%						
SK 3	Meningkatnya Pemanfaatan Rekomendasi Hasil Pemutakhiran dan Inovasi Hasil Perekayasaan Keamanan Siber dan Sandi												Pusertif
IKK 3.1	Persentase rekomendasi hasil pemutakhiran sistem keamanan siber dan sandi yang dimanfaatkan K/L		80%	81%	82%	83%	84%						
IKK 3.2	Persentase pemanfaatan inovasi hasil perekayasaan di bidang keamanan siber dan sandi		33%	50%	50%	60%	66,70%						
IKK 3.3	Tingkat kepuasan atas layanan pusat sertifikasi teknologi keamanan siber dan sandi		81	82	83	84	85						
KRO	Kebijakan Bidang Pertahanan dan Keamanan												
	Rekomendasi kebijakan terkait pemutakhiran sistem dan informasi keamanan siber dan sandi	Pusat	6	2	2	2	2	870	1.224	1.285	1.350	1.568	
	Rekomendasi kebijakan terkait inovasi hasil perekayasaan di bidang keamanan siber dan sandi	Pusat	-	4	4	5	6	-	2.573	2.708	3.525	4.509	
KRO	Sertifikasi Produk												
	Sertifikasi Produk Teknologi Keamanan Siber dan Sandi	Pusat	2	1	1	1	1	614	770	847	931	1.024	
KRO	Penyidikan dan Pengujian Produk												
	Pengujian Produk Teknologi Keamanan Siber dan Sandi	Pusat	8	8	8	8	9	644	2.226	3.113	3.424	4.237	
KRO	Sertifikasi Produk (RPJMN)												
	Sertifikasi produk teknologi keamanan siber dan sandi berdasarkan standar yang diakui oleh BSSN dalam rangka menjamin keamanan Infrastruktur Informasi Vital (IIV) (RPJMN)	Pusat	2	2	3	3	4	2.927	13.181	3.634	4.959	1.966	
KRO	Sarana Bidang Pertahanan dan Keamanan												
	Revitalisasi Laboratorium Pengujian Produk Teknologi Keamanan Siber dan Sandi	Pusat	2	-	2	2	2	654	-	4.614	5.076	5.583	
KRO	Sarana Bidang Pertahanan dan Keamanan (RPJMN)												
	Pengembangan Laboratorium Sertifikasi dan Pengujian Produk Keamanan BSSN (RPJMN)	Pusat	-	-	-	-	1	-	-	-	-	68.972	
PROGRAM DUKUNGAN MANAJEMEN								473.173	692.082	1.077.367	1.101.992	1.150.149	
SP 1	Meningkatnya hasil pelaksanaan RB General												Sekretariat Utama
IKP 1.1	Nilai RB General BSSN		83,06	83,73	85,82	86,62	87,80						
KEGIATAN : PENYELENGGARAAN PERENCANAAN DAN KEUANGAN								285.275	307.004	314.606	326.302	338.853	
SK 1	Meningkatnya Perencanaan, Pengelolaan Kinerja, dan Keuangan yang Andal dan Profesional												Biro Perencanaan dan Keuangan
IKK 1.1	Nilai SAKIP		70,01	71,15	72,50	74,00	75,35						
IKK 1.2	Indeks perencanaan pembangunan		100	100	100	100	100						
IKK 1.3	Indikator Kinerja Pelaksanaan Anggaran (IKPA)		96,30	96,50	96,75	97,00	97,25						
IKK 1.4	Capaian prioritas nasional		100	100	100	100	100						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
IKK 1.5	Capaian IKU		100	100	100	100	100						
IKK 1.6	Opini BPK		WTP	WTP	WTP	WTP	WTP						
IKK 1.7	Tingkat kepuasan terhadap layanan internal Biro Perencanaan dan Keuangan		88	89	90	91	92						
KRO	Peraturan Menteri												
	Peraturan BSSN tentang Rencana Strategis BSSN Tahun 2025-2029	Pusat	1	-	-	-	-	39	-	-	-	-	
KRO	Peraturan Lainnya												
	Peraturan Kepala tentang Manajemen Resiko BSSN	Pusat	1	-	-	-	-	73	-	-	-	-	
KRO	Kebijakan Bidang Tata Kelola Pemerintahan												
	Rekomendasi Kebijakan Bidang Perencanaan, Pengelolaan Kinerja dan Risiko, dan Keuangan	Pusat	-	2	2	1	3	-	1.030	427	1.495	3.427	
KRO	Layanan Manajemen Kinerja Internal												
	Layanan Perencanaan dan Penganggaran	Pusat	92	92	98	98	98	826	926	972	995	1.072	
	Layanan Pemantauan dan Evaluasi	Pusat	12	12	12	12	12	2.563	2.174	2.204	2.316	2.358	
	Layanan Manajemen Keuangan	Pusat	5	5	9	9	9	1.523	2.721	2.857	3.000	3.150	
KRO	Layanan Dukungan Manajemen Internal												
	Layanan Perkantoran	Pusat	12	12	12	12	12	280.250	300.153	308.146	318.496	328.847	
KEGIATAN : PENYELENGGARAAN ORGANISASI DAN SDM								14.115	21.555	22.633	23.765	24.953	
SK 1	Terwujudnya penyederhanaan birokrasi serta Pelaksanaan Reformasi Birokrasi General BSSN												Biro Organisasi dan SDM
IKK 1.1	Persentase penyederhanaan struktur organisasi		100	100	100	100	100						
IKK 1.2	Tingkat capaian sistem kerja untuk penyederhanaan birokrasi		4	4	5	5	5						
IKK 1.3	Rencana Aksi Pembangunan RB general		2,75	2,77	2,79	2,81	2,83						
SK 2	Meningkatnya Pengelolaan ASN BSSN secara Profesional dan Komprehensif												Biro Organisasi dan SDM
IKK 2.1	Indeks Sistem Merit		333	333	374	374	389						
IKK 2.2	Indeks BerAKHLAK		79,13	80,75	81,75	83,38	84,38						
IKK 2.3	Tingkat Kepuasan terhadap Layanan Internal Biro Organisasi dan SDM		88,4	88,5	88,6	88,7	88,8						
KRO	Peraturan Menteri												
	Peraturan Bidang Organisasi dan Sumber Daya Manusia	Pusat	1	2	-	-	-	63	88	-	-	-	
KRO	Kebijakan Bidang Tata Kelola Pemerintahan												
	Rekomendasi Kebijakan Bidang Organisasi dan Sumber Daya Manusia	Pusat	1	1	-	-	-	99	100	-	-	-	
KRO	Layanan Dukungan Manajemen Internal												
	Layanan Organisasi dan Tata Kelola Internal	Pusat	3	3	3	3	3	1.010	1.379	1.645	1.727	1.813	
	Layanan Perkantoran	Pusat	1	-	-	-	-	4.441	-	-	-	-	
KRO	Layanan Manajemen SDM Internal												
	Layanan Manajemen SDM	Pusat	13	13	13	13	13	6.576	16.241	17.053	17.906	18.801	
	Layanan Pendidikan dan Pelatihan	Pusat	3	3	3	3	3	1.926	3.748	3.935	4.132	4.338	
KEGIATAN : PENYELENGGARAAN HUKUM DAN KOMUNIKASI PUBLIK								20.273	41.562	52.180	59.991	68.975	
SK 1	Meningkatnya kualitas kebijakan, reformasi hukum, penyelenggaraan pelayanan publik dan kearsipan yang andal dan profesional												Biro Hukum dan Komunikasi Publik
IKK 1.1	Indeks Reformasi Hukum		97,52	97,53	97,54	97,55	97,56						
IKK 1.2	Indeks Kualitas Kebijakan		66,00	66,00	66,50	66,50	67,00						
IKK 1.3	Tingkat digitalisasi arsip		83,80	85,90	88,00	90,10	92,20						
IKK 1.4	Tingkat Kepatuhan Standar Pelayanan Publik		75,25	75,50	75,50	76,00	76,00						
IKK 1.5	Indeks Pelayanan Publik		4,55	4,75	4,75	4,90	4,90						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
IKK 1.6	Tingkat Tindak Lanjut Pengaduan Masyarakat (LAPOR) yang sudah diselesaikan		4	4	5	5	5						
IKK 1.7	Survey Kepuasan Masyarakat		90,19	90,50	90,50	91,00	91,00						
IKK 1.8	Tingkat Kepuasan Terhadap Layanan Internal Biro Hukum dan Komunikasi Publik		87	88	89	90	91						
KRO	Peraturan Menteri												
	Peraturan Kepala BSSN di Bidang Hukum dan Komunikasi Publik	Pusat	1	-	1	1	1	100	-	100	100	100	
KRO	Norma, Standard, Prosedur dan Kriteria												
	Penyusunan NSPK BSSN	Pusat	1	1	1	1	1	49	45	64	74	85	
KRO	Layanan Dukungan Manajemen Internal												
	Layanan Protokoler	Pusat	1	1	1	1	1	3.817	10.429	13.038	14.994	17.243	
	Layanan Hukum	Pusat	2	2	2	2	2	1.891	5.240	6.538	7.519	8.647	
	Layanan Hubungan Masyarakat dan Informasi	Pusat	12	12	12	12	12	4.065	5.805	6.210	7.141	8.212	
	Layanan Perkantoran	Pusat	1	1	1	1	1	9.840	19.123	25.177	28.953	33.296	
KRO	Layanan Manajemen Kinerja Internal												
	Layanan Penyelenggaraan Kearsipan	Pusat	1	1	1	1	1	513	920	1.053	1.211	1.393	
KEGIATAN : PENYELENGGARAAN DUKUNGAN ADMINISTRATIF BIDANG KERUMAHTANGGAAN, PENGELOLAAN BMN, DAN LAYANAN PENGADAAN								127.976	193.743	206.363	223.129	241.528	
SK 1	Meningkatnya Kualitas Pengadaan Barang dan Jasa, Pengelolaan BMN serta Layanan Umum BSSN												Biro Umum
IKK 1.1	Indeks Tata Kelola Pengadaan		86,20	86,40	86,60	86,80	87,00						
IKK 1.2	Indeks Pengelolaan Aset		3,64	3,65	3,66	3,67	3,68						
IKK 1.3	Tingkat Kepuasan terhadap Layanan Internal Biro Umum		86,00	86,50	87,00	87,50	88,00						
KRO	Layanan Dukungan Manajemen Internal												
	Layanan BMN	Pusat	13	13	13	13	13	1.340	6.809	7.490	8.239	9.063	
	Layanan Umum	Pusat	2	2	2	2	2	2.594	2.883	3.172	3.489	3.838	
	Layanan Perkantoran	Pusat	1	1	1	1	1	116.209	150.625	165.688	182.256	200.482	
KRO	Layanan Sarana dan Prasarana Internal												
	Layanan Sarana Internal	Pusat	4	4	4	4	4	7.833	12.925	9.014	8.145	8.145	
	Layanan Prasarana Internal	Pusat	-	1	1	1	1	-	20.500	21.000	21.000	20.000	
KEGIATAN : PENGAWASAN DAN PENINGKATAN AKUNTABILITAS APARATUR BADAN SIBER DAN SANDI NEGARA								2.265	4.024	4.225	4.436	4.658	
SK 1	Meningkatnya Kualitas Pengawasan Internal di Lingkungan BSSN												Inspektorat
IKK 1.1	Persentase Pelaksanaan Tindak Lanjut Rekomendasi BPK		92,00	92,50	93,00	93,50	94,00						
IKK 1.2	Tingkat Maturitas Penyelenggaraan SPIP		3,30	3,40	3,50	3,60	3,70						
IKK 1.3	Tingkat Implementasi Rencana Aksi RB General		96,50	97,00	97,50	98,00	98,50						
IKK 1.4	Tingkat Keberhasilan Pembangunan Zona Integritas		3	3	3	3	3						
IKK 1.5	Survei Penilaian Integritas		82,76	83,00	84,00	85,00	86,00						
KRO	Peraturan Menteri												
	Revisi Peraturan BSSN Nomor 6 Tahun 2020 tentang Pengendalian Gratifikasi di BSSN	Pusat	1	-	-	-	-	8	-	-	-	-	
KRO	Layanan Manajemen Kinerja Internal												
	Layanan Audit Internal	Pusat	26	26	26	26	26	2.257	4.024	4.225	4.436	4.658	
KEGIATAN : PENGELOLAAN DATA DAN TEKNOLOGI INFORMASI KOMUNIKASI								23.269	120.594	473.039	459.185	464.960	
SK 1	Meningkatnya Hasil Pelaksanaan SPBE, Implementasi Kebijakan Arsiktektur SPBE dan Kematangan Statistik Sektoral												Pusat Data dan TIK
IKK 1.1	Indeks SPBE		4,06	4,09	4,09	4,12	4,14						
IKK 1.2	Indeks Pembangunan Statistik		2,31	2,40	2,40	2,50	2,50						

PROGRAM/ KEGIATAN/ KODE	SASARAN PROGRAM (*OUTCOME*)/ SASARAN KEGIATAN (*OUTPUT*)/INDIKATOR	LOKASI	TARGET					ALOKASI (dalam juta rupiah)					UNIT ORGANISASI PELAKSANA
			2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	
IKK 1.3	Tingkat Implementasi Kebijakan Arsitektur SPBE		3	3	4	4	5						
KRO	Layanan Dukungan Manajemen Internal												
	Sarana Teknologi Informasi dan Komunikasi	Pusat	1	1	1	1	1	1.391	85.734	430.157	411.157	411.157	
	Layanan Data dan Informasi	Pusat	4	4	4	4	4	4.045	13.935	14.880	15.825	16.770	
	Layanan Perkantoran	Pusat	1	1	1	1	1	17.833	20.926	28.003	32.203	37.034	
KEGIATAN : PENYELENGGARAAN DUKUNGAN LAYANAN PERKANTORAN SERTIFIKASI ELEKTRONIK								-	3.600	4.320	5.184	6.221	
SK 1	Meningkatnya Efisiensi dan Efektifitas Pengelolaan Sumber Daya Balai Besar Sertifikasi Elektronik												Balai Besar Sertifikasi Elektronik
IKK 1.1	Indikator Kinerja Pelaksanaan Anggaran (IKPA) Satker		96,30	96,50	96,75	97,00	97,25						
KRO	Layanan Dukungan Manajemen Internal												
	Layanan Perkantoran	Pusat	-	1	1	1	1	-	3.600	4.320	5.184	6.221	

Keterangan:

Indikasi Target dan Pendanaan dapat dimutakhirkan melalui Rencana Kerja (Renja) dengan mempertimbangkan: a) Kesiapan dan Kapasitas Pelaksanaan; b) Ketersediaan dan Sumber Pendanaan; serta c) Keterlibatan Peran Pemerintah Daerah, Badan Usaha, dan Masyarakat.

Lampiran 2 : Matriks Pendanaan Anggaran Pendapatan Dan Belanja Negara Dan Sumber Pendanaan Lainnya Yang Sah

Terhadap Kegiatan Prioritas/ Proyek Prioritas Badan Siber Dan Sandi Negara

KEGIATAN PRIORITAS/ PROYEK PRIORITAS	PENUGASAN INDIKATOR	TARGET					ALOKASI APBN (dalam juta rupiah)					ALOKASI NON-APBN (dalam juta rupiah)					TOTAL (dalam juta rupiah)	UNIT KERJA
		2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	2025	2026	2027	2028	2029		
Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	1	1	1	1	1	945	3.507	947	6.841	6.841	-	-	-	-	-	19.081	Direktorat Strategi Keamanan Siber dan Sandi
Kerja sama Bilateral dan Multilateral di Bidang Keamanan Siber (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	1	2	1	3	3	603	803	603	1.077	841	-	-	-	-	-	3.926	Direktorat Strategi Keamanan Siber dan Sandi
Operasi Audit Keamanan SPBE (RPJMN)	Indeks Kesiapsiagaan dan Ketahanan Siber Nasional	13	15	18	20	23	2.242	8.032	9.161	10.234	11.094	-	-	-	-	-	40.763	Direktorat Operasi Keamanan dan Pengendalian Informasi
Operasi Penanganan perkara cyber related crime (RPJMN)	Indeks Kesiapsiagaan dan Ketahanan Siber Nasional	1	1	1	1	1	488	586	704	845	1.013	-	-	-	-	-	3.636	Direktorat Operasi Keamanan dan Pengendalian Informasi
Peningkatan Budaya Keamanan Siber + Pengukuran Tingkat Kesadaran Kamsiber (RPJMN)	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi	4	4	4	4	–	366	439	527	632	758	-	-	-	-	-	2.722	Direktorat Operasi Keamanan dan Pengendalian Informasi
Operasi Pengamanan Siber dan Sandi pada Penyelenggaraan Pemilu Tahun 2029 (RPJMN)	Indeks Kesiapsiagaan dan Ketahanan Siber Nasional	-	-	-	58	53	-	-	-	29.000	27.800	-	-	-	-	-	56.800	Direktorat Operasi Keamanan Siber
Operasi Dukungan Penyidikan dalam rangka Pengungkapan Perkara Siber (RPJMN)	Indeks Kesiapsiagaan dan Ketahanan Siber Nasional	-	3	3	3	3	-	1.500	1.500	1.500	1.500	-	-	-	-	-	6.000	Direktorat Operasi Keamanan Siber
Operasi Profiling Sinyal di Kawasan Indo-Pasifik (RPJMN)	Indeks Kesiapsiagaan dan Ketahanan Siber Nasional	-	3	3	3	3	-	4.020	1.190	1.433	1.326	-	-	-	-	-	7.968	Balai Deteksi Sinyal
Roadmap Peningkatan Budaya Keamanan Informasi (RPJMN)	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi	1	-	-	-	-	197	-	-	-	-	-	-	-	-	-	197	Direktorat Operasi Keamanan dan Pengendalian Informasi
Penguatan National Security Operation Center (NSOC) (PHLN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	–	1	1	1	1	-	628.929	628.929	628.929	628.929	-	-	-	-	-	2.515.716	Direktorat Operasi Keamanan Siber
Sistem Pemantauan dan Deteksi Serangan Siber Sosial (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	3	3	3	3	3	90.000	15.000	15.000	15.000	15.000	-	-	-	-	-	150.000	Direktorat Operasi Keamanan dan Pengendalian Informasi
Perluasan Cakupan Perangkat Traffic analysis National Security Operation Center (NSOC) (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	1	3	3	3	3	255.487	975.000	1.121.250	1.289.438	1.482.853	-	-	-	-	-	5.124.028	Direktorat Operasi Keamanan Siber
Peralatan Operasi Pengamanan Sinyal (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	–	1	1	1	1	-	250.000	108.149	67.738	67.738	-	-	-	-	-	493.625	Direktorat Operasi Sandi
Infrastruktur Kriptografi Nasional (Cryptography as a Service) (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	1	–	1	-	1	45.569	-	36.109	-	36.109	-	-	-	-	-	117.786	Direktorat Operasi Sandi
Sistem Pelindungan Infrastruktur Informasi Vital (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	–	1	-	-	-	-	110.000	-	-	-	-	-	-	-	-	110.000	Direktorat Operasi Keamanan Siber
Platform National Cyber Threat Database (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	-	-	2	2	-	-	-	50.000	50.000	-	-	-	-	-	100.000	Direktorat Operasi Keamanan Siber

KEGIATAN PRIORITAS/ PROYEK PRIORITAS	PENUGASAN INDIKATOR	TARGET					ALOKASI APBN (dalam juta rupiah)					ALOKASI NON-APBN (dalam juta rupiah)					TOTAL (dalam juta rupiah)	UNIT KERJA
		2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	2025	2026	2027	2028	2029		
Sistem Penelusuran Indikasi Potensi Ancaman Siber (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	1	-	-	-	-	5.001	-	-	-	-	-	-	-	-	5.001	Direktorat Operasi Keamanan Siber
Sistem Terintegrasi Audit Keamanan SPBE (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	2	1	1	1	-	60.000	5.000	5.000	5.000	-	-	-	-	-	75.000	Direktorat Operasi Keamanan dan Pengendalian Informasi
Penguatan Perangkat Command Center Kriptografi (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	-	-	1	1	-	–	–	50.000	50.000	-	-	-	-	-	100.000	Direktorat Operasi Sandi
Sarana Operasi Analisis Sinyal (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	1	1	1	1	1	100.000	200.000	200.000	200.000	200.000	-	-	-	-	-	900.000	Balai Deteksi Sinyal
Pembangunan SSOC IKN (Perpres 63 2022)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	–	1	1	1	1	-	690.041	102.946	9.679	9.679	-	-	-	-	-	812.345	Direktorat Operasi Keamanan Siber
Penguatan Ekosistem Keamanan Siber di Indonesia (PHLN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	1	-	-	-	-	0,10	-	-	-	-	-	-	-	-	-	0,10	Direktorat Operasi Keamanan Siber
Optimalisasi Sistem Pemantauan dan Deteksi Ancaman Siber Sosial (PHLN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	1	-	-	-	-	0,10	-	-	-	-	-	-	-	-	-	0,10	Direktorat Operasi Keamanan dan Pengendalian Informasi
Pembangunan National Signal Analysis (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	–	1	1	1	1	-	350.000	350.000	350.000	350.000	-	-	-	-	-	1.400.000	Balai Deteksi Sinyal
Peraturan BSSN tentang Peta Jalan Pelindungan IIV Sektor Administrasi Pemerintahan Tahun 2030-2034 (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	-	-	-	-	1	-	-	-	-	350	-	-	-	-	-	350	Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
Penyusunan Peta Jalan Pelindungan IIV Sektor Pertahanan (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	1	-	-	-	-	257	-	-	-	-	-	-	-	-	-	257	Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
Pembinaan Peningkatan Kapasitas Keamanan SPBE Lingkup Instansi Pengelola Aplikasi Umum dan Inisiatif Strategis Arsitektur SPBE Nasional (RPJMN)	Persentase ASN dengan kompetensi digital optimal (BKN)	24	32	32	32	32	1.161	3.211	3.471	3.087	2.985	-	-	-	-	-	13.914	Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
Pembinaan Kematangan Keamanan Siber Sektor Administrasi Pemerintahan : Pemerintah Pusat (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	105	160	160	160	160	5.962	18.784	25.235	30.959	34.989	-	-	-	-	-	115.928	Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
Pembinaan Kematangan Keamanan Siber Sektor Kesehatan (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	–	40	60	80	100	-	1.343	1.881	2.633	3.686	-	-	-	-	-	9.544	Direktorat Keamanan Siber dan Sandi Pembangunan Manusia
Pembinaan Kematangan Keamanan Siber Sektor Administrasi Pemerintahan: Pemerintah Daerah (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	7	14	21	28	34	3.212	4.423	4.192	4.483	4.159	-	-	-	-	-	20.470	Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Penguatan Ekosistem Keamanan Siber dan Sandi pada Provinsi Baru (RPJMN))	Persentase instansi K/L/Prov yang terhubung dengan JIP; dan Persentase K/L/D yang mengimplementasikan SPLP	4	4	4	4	4	1.033	1.166	1.913	2.056	2.799	-	-	-	-	-	8.966	Direktorat Keamanan Siber dan Sandi Pemerintah Daerah

KEGIATAN PRIORITAS/ PROYEK PRIORITAS	PENUGASAN INDIKATOR	TARGET					ALOKASI APBN (dalam juta rupiah)					ALOKASI NON-APBN (dalam juta rupiah)					TOTAL (dalam juta rupiah)	UNIT KERJA
		2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	2025	2026	2027	2028	2029		
Sistem Pengawasan Kepatuhan Penanganan Insiden pada TTIS Organisasi Sektor Administrasi Pemerintahan (RPJMN)	Persentase instansi K/L/Prov yang terhubung dengan JIP; dan Persentase K/L/D yang mengimplementasikan SPLP	-	1	1	1	1	-	13.008	11.789	15.325	19.923	-	-	-	-	-	60.045	Direktorat Keamanan Siber dan Sandi Pemerintah Pusat
Pembinaan Kematangan Keamanan Siber Sektor Keuangan (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	60	50	60	60	60	2.668	8.740	4.061	4.467	4.913	-	-	-	-	-	24.849	Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata
Pembinaan Kematangan Keamanan Siber Sektor ESDM dan Pangan (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	45	82	45	45	45	3.125	19.859	6.776	7.668	7.835	-	-	-	-	-	45.263	Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam
Pembinaan Kematangan Keamanan Siber Sektor TIK dan Transportasi (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	50	60	70	80	90	2.875	6.603	10.158	10.844	13.489	-	-	-	-	-	43.968	Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi
Tim Tanggap Insiden Siber (CSIRT) IIV Sektor Keuangan yang teregistrasi (RPJMN)	Persentase ASN dengan kompetensi digital optimal (BKN)	-	-	-	-	1	-	-	-	-	1.200	-	-	-	-	-	1.200	Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata
Tim Tanggap Insiden Siber (CSIRT) IIV Sektor ESDM dan Pangan yang teregistrasi (RPJMN)	Persentase ASN dengan kompetensi digital optimal (BKN)	-	1	-	1	-	-	895	-	732	-	-	-	-	-	-	1.626	Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam
Tim Tanggap Insiden Siber (CSIRT) IIV Sektor TIK dan Transportasi yang teregistrasi (RPJMN)	Persentase ASN dengan kompetensi digital optimal (BKN)	-	1	-	-	1	-	666	-	-	1.200	-	-	-	-	-	1.866	Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi
Peta Jalan Pelindungan IIV Sektor Keuangan (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	1	-	-	-	1	659	-	-	-	1.952	-	-	-	-	-	2.610	Direktorat Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata
Peta Jalan Pelindungan IIV Sektor ESDM dan Pangan (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	1	-	1	-	-	621	-	4.475	-	-	-	-	-	-	-	5.096	Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam
Peta Jalan Pelindungan IIV Sektor TIK dan Transportasi (RPJMN)	Nilai Kematangan Keamanan Siber PSE dan Nilai Kematangan Penyelenggara Persandian	1	-	-	-	1	431	-	-	-	630	-	-	-	-	-	1.061	Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi
Sertifikasi SDM Berdasarkan Standar Kompetensi Keamanan Siber dan Sandi (RPJMN)	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi	360	360	360	360	360	498	813	895	984	1.083	-	-	-	-	-	4.274	Pusat Pengembangan SDM

KEGIATAN PRIORITAS/ PROYEK PRIORITAS	PENUGASAN INDIKATOR	TARGET					ALOKASI APBN (dalam juta rupiah)					ALOKASI NON-APBN (dalam juta rupiah)					TOTAL (dalam juta rupiah)	UNIT KERJA
		2025	2026	2027	2028	2029	2025	2026	2027	2028	2029	2025	2026	2027	2028	2029		
Pelatihan bagi SDM Keamanan SPBE (RPJMN)	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi	300	300	300	300	300	1.155	1.874	2.061	2.267	2.494	-	-	-	-	-	9.850	Pusat Pengembangan SDM
Pelatihan Peningkatan Kompetensi SDM Berdasarkan Standar Kompetensi Keamanan Siber dan Sandi (RPJMN)	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi	325	325	325	325	325	1.121	1.236	1.360	1.496	1.645	-	-	-	-	-	6.858	Pusat Pengembangan SDM
Pelatihan Teknis Bidang Keamanan Siber dan Sandi (RPJMN)	Rata-rata Competency Gap Index (CGI) SDM Siber dan Sandi	325	275	275	275	275	1.714	2.434	2.677	2.945	3.240	-	-	-	-	-	13.011	Pusat Pengembangan SDM
Fasilitas Pembangunan Sumber Daya Manusia Keamanan Siber dan Sandi Yang Terbangun di Poltek SSN (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	7	3	-	1	-	182.381	91.804	-	1.573	-	-	-	-	-	275.758	Politeknik Siber dan Sandi Negara
Optimalisasi Pemanfaatan Sertifikat Elektronik dalam Mendukung Pemerintahan Digital (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	18	40	68	100	-	4.380	8.400	11.900	15.400	-	-	-	-	-	40.080	Balai Besar Sertifikasi Elektronik
Penerapan Sertifikat Elektronik pada Pelayanan Publik (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	2	1	1	1	-	204.095	176.698	139.270	146.975	-	-	-	-	-	667.038	Balai Besar Sertifikasi Elektronik
Sertifikasi produk teknologi keamanan siber dan sandi berdasarkan standar yang diakui oleh BSSN dalam rangka menjamin keamanan Infrastruktur Informasi Vital (IIV) (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	2	2	3	3	4	2.927	13.181	3.634	4.959	1.966	-	-	-	-	-	26.667	Pusat Sertifikasi Teknologi Keamanan Siber dan Sandi
Pengembangan Laboratorium Sertifikasi dan Pengujian Produk Keamanan BSSN (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	-	-	-	1	-	-	-	-	68.972	-	-	-	-	-	68.972	Pusat Sertifikasi Teknologi Keamanan Siber dan Sandi
Peningkatan kapasitas sistem pengalihan serangan siber (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	-	-	1	1	-	-	-	27.000	5.000	-	-	-	-	-	32.000	Direktorat Operasi Keamanan Siber
Sistem Pangkalan Data Insiden Siber (RPJMN)	Persentase Pemanfaatan Inovasi Hasil Perekayasaan di Bidang Keamanan Siber dan Sandi	-	-	-	1	1	-	-	-	35.000	24.500	-	-	-	-	-	59.500	Direktorat Operasi Keamanan Siber
TOTAL ANGGARAN							525.313	3.791.950	2.943.491	3.025.422	3.289.942	-	-	-	-	-	13.605.618	

Keterangan:

Indikasi Target dan Pendanaan dapat dimutakhirkan melalui Rencana Kerja (Renja) dengan mempertimbangkan: a) Kesiapan dan Kapasitas Pelaksanaan; b) Ketersediaan dan Sumber Pendanaan; serta c) Keterlibatan Peran Pemerintah Daerah, Badan Usaha, dan Masyarakat.

Lampiran 3 : Matriks Kerangka Regulasi BSSN Tahun 2025 - 2029

No	Arah Kerangka Regulasi dan/atau Kebutuhan Regulasi	Urgensi Pembentukan Berdasarkan Evaluasi Regulasi Eksisting, Kajian dan Penelitian	Unit Penanggung Jawab	Unit Terkait/ Institusi	Target Penyelesaian
1	Penyusunan RUU tentang Keamanan dan Ketahanan Siber	• Memenuhi dan melaksanakan hak konstitusional dan untuk memenuhi kekosongan hukum terkait perlindungan keamanan dan ketahanan siber nasional • Sebagai bentuk respons atas berbagai insiden siber yang menjadi atensi nasional • Belum adanya peraturan yang memadai dalam melindungi dalam memberikan keamanan dan ketahanan siber untuk melindungi keamanan Masyarakat	Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi	• Kemenkopolkam • Kemenkumham • Kemenkomdigi • BIN • Kemenhan • TNI • Polri • Kemendikti • Kemenperin • Kemenpan RB • K/L pembina sektor IIV	• 2025-2026 (penyusunan nasmik) • 2027 (penyusunan) • 2028 (PAK dan Harmon) • 2029 (pembahasan di DPR)
2	Penyusunan RUU tentang Persandian	• Sebagai bentuk respons atas berbagai insiden siber yang menjadi atensi nasional • Adanya kebutuhan hukum untuk mengatur persandian dalam lingkup privat dan publik secara seimbang antara penghormatan atas hak asasi manusia dan kewajiban setiap warga negara dalam menjaga pertahanan dan keamanan negara/keamanan nasional	Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi	• Kemenkopolkam • Kemenkumham • Kemenkomdigi • BRIN • Kemendagri • Kemenhan • TNI • Polri • Kemenperin • Kemenpan RB	Saat ini sudah masuk prolegnas jangka menengah dan menunggu pembahasan di DPR
3	Rancangan Peraturan BSSN tentang Peraturan Pelaksanaan Peraturan Pemerintah tentang Pelaksanaan Undang-Undang tentang Keamanan dan Ketahanan Siber	• Melaksanakan beberapa ketentuan dalam Rancangan Peraturan Pemerintah tentang Pelaksanaan Undang-Undang tentang Keamanan dan Ketahanan Siber yang bersifat teknis operasional	Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi	• Kemenhum • Kementerian/Lembaga lain terkait substansi pengaturan (sesuai kebutuhan pengaturan)	2029 (setelah Rancangan PP tentang Pelaksanaan UU tentang Keamanan dan Ketahanan Siber diundangkan)
4	Penyusunan Rperpres tentang perubahan Perpres nomor 28 tahun 2021 tentang Badan Siber dan Sandi Negara	• Memberikan penguatan terhadap dasar hukum terkait tugas dan fungsi BSSN • Mewujudkan keamanan, pelindungan dan kedaulatan siber nasional serta meningkatkan pertumbuhan ekonomi nasional perlu dilakukan penataan organisasi BSSN • Mengoptimalkan pelaksanaan tugas dan fungsi di bidang keamanan siber dan sandi diperlukan organisasi BSSN yang lebih efektif dan efisien • Pasca diundangkannya RUU tentang Keamanan dan Ketahanan (Resilensi) Siber, Peraturan Presiden Nomor 28 Tahun 2021 tentang BSSN sudah tidak sesuai dengan dinamika dan kebutuhan organisasi •	Sekretariat Utama	• Kemenpolkam • Kemenkokumham • Kemenhum • Kemenkeu • Bappenas • Kemenpan RB • Kemensetneg	2029 (setelah Rancangan UU tentang Keamanan dan Ketahanan Siber diundangkan)
5	Penyusunan Rancangan Peraturan BSSN tentang perubahan Peraturan BSSN Nomor 6 tahun 2021 tentang Organisasi dan Tata Kerja BSSN	• Mengoptimalkan pelaksanaan tugas pemerintahan di bidang keamanan siber dan sandi diperlukan penataan kembali terhadap tugas, fungsi, susunan organisasi dan tata kerja BSSN yang lebih efektif dan efisien. • Melaksanakan ketentuan terkait pembentukan lembaga sesuai Rancangan UU tentang Keamanan dan Ketahanan Siber	Sekretariat Utama	• Kemenhum • Kemenpan RB	2029 (setelah rancangan Perpres tentang BSSN diundangkan)
6	Penyusunan rancangan Peraturan BSSN tentang Penerapan dan pelaporan hasil penerapan manajemen risiko keamanan siber	• Pemerintah berperan melindungi kepentingan umum dari segala jenis gangguan terhadap Infrastruktur Informasi Vital (IIV) sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum • Gangguan terhadap IIV dapat menimbulkan kerugian dan dampak yang serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan serta perekonomian nasional • Melaksanakan ketentuan Pasal 10 ayat (5) Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital	Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi	• Kemenhum • Kementerian/Lembaga lain terkait substansi pengaturan (sesuai kebutuhan pengaturan)	2026
7	Rancangan Peraturan Presiden tentang Audit Keamanan Informasi	• Adanya kebutuhan terhadap dasar hukum/acuan/pedoman untuk melakukan Audit Keamanan Informasi kepatuhan (audit internal/eksternal), audit investigasi (investigasi pasca insiden), dan audit sertifikasi.	Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi	• Kemenhum • Kemenham • Kemenkomdigi • BIN • Kemenhan • TNI • Polri • Kemenlu • BSN/KAN • BRIN	2029

				• BPKP • Setneg • Setkab • KSP	

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

NUGROHO S. BUDI