



BERITA NEGARA REPUBLIK INDONESIA

No.843, 2020

BSSN. Rencana Strategis. Tahun 2020-2024.
Pencabutan.

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 5 TAHUN 2020
TENTANG
RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA
TAHUN 2020-2024

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

- Menimbang : a. bahwa ketentuan Pasal 19 ayat (2) Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional mengamanatkan kementerian/lembaga untuk menetapkan Rencana Strategis Kementerian/Lembaga;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024;
- 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. Peraturan Pemerintah Nomor 40 Tahun 2006 tentang Tata Cara Penyusunan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 97, Tambahan Lembaran Negara Republik Indonesia Nomor 4664);

3. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100) sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 277);
4. Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024 (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 10);
5. Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2018 Nomor 197);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2020-2024.

Pasal 1

Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 merupakan dokumen perencanaan Badan Siber dan Sandi Negara untuk Tahun 2020-2024 yang menjabarkan Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024.

Pasal 2

- (1) Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 sebagaimana dimaksud dalam Pasal 1 memuat:
 - a. pendahuluan;
 - b. visi, misi, dan tujuan;
 - c. arah kebijakan, strategi, kerangka regulasi, dan kerangka kelembagaan;

- d. target kinerja dan kerangka pendanaan;
 - e. penutup; dan
 - f. lampiran.
- (2) Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 3

- (1) Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 memuat data dan informasi kinerja.
- (2) Data dan informasi kinerja sebagaimana dimaksud pada ayat (1) termuat dalam Sistem Informasi KRISNA-Renstra.
- (3) Data dan informasi kinerja sebagaimana dimaksud pada ayat (2) merupakan bagian tidak terpisahkan dari dokumen Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 sebagaimana dimaksud dalam Pasal 2.

Pasal 4

Pada saat Peraturan Badan ini mulai berlaku, Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2018 tentang Visi Misi Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2018 Nomor 341), 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 17 Juli 2020

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 29 Juli 2020

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd.

WIDODO EKATJAHJANA

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 5 TAHUN 2020
TENTANG
RENCANA STRATEGIS BADAN SIBER DAN
SANDI NEGARA TAHUN 2020 – 2024

RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA
TAHUN 2020 – 2024

BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Paradigma pembangunan siber dan sandi nasional sesuai amanah Rencana Pembangunan Jangka Menengah Nasional (RPJMN) Tahun 2020–2024 untuk mewujudkan kedaulatan, ketahanan, dan perlindungan siber. Hal ini sesuai dengan tugas dan fungsi Badan Siber dan Sandi Negara (BSSN) dalam melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber yang tertuang di dalam Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Dalam rangka mewujudkan paradigma tersebut, perlu ditentukan strategi dan arah sebagai acuan dalam pengambilan kebijakan, keputusan, dan tindakan yang tepat di bidang keamanan siber yang dituangkan dalam dokumen Rencana Strategis (Renstra) BSSN. Penyusunan Renstra BSSN 2020–2024 berpedoman pada Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional dan Peraturan Presiden Nomor 18 Tahun 2020 tentang RPJMN 2020–2024. Renstra BSSN Tahun 2020–2024 disusun untuk menjamin keterkaitan dan konsistensi antara perencanaan, penganggaran, pelaksanaan, dan pengawasan serta menjamin

tercapainya penggunaan sumber daya secara efisien, efektif, berkeadilan, dan berkelanjutan serta menjadi pedoman bagi penyusunan dokumen perencanaan tahunan BSSN.

1.2. KONDISI UMUM

Keamanan ruang siber turut dipengaruhi beberapa isu-isu strategis diantaranya meningkatnya penetrasi internet dalam berbagai aspek kehidupan dan bergulirnya revolusi industri 4.0 yang menimbulkan berbagai ancaman di ruang siber. Dua tahun pasca dibentuknya, BSSN mulai menata pengelolaan tugas dan fungsi sehingga ancaman keamanan siber dapat diminimalisir. Pencapaian kinerja BSSN 2018-2019 semakin menguatkan posisi BSSN yang bertekad untuk melayani seluruh pemangku kepentingan baik disektor pemerintah, Infrastruktur Informasi Kritis Nasional (IIKN), dan ekonomi digital serta terus berusaha memenuhi harapan dari masyarakat untuk dapat menjaga stabilitas keamanan ruang siber.

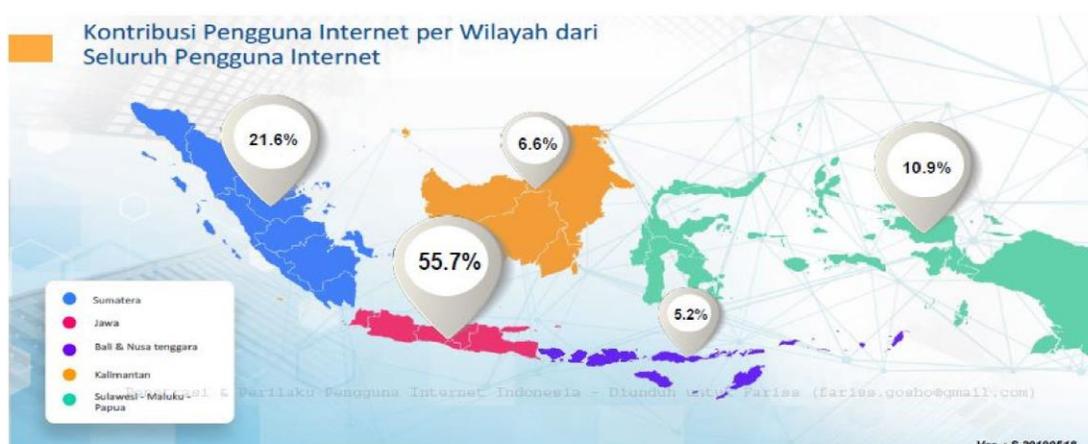
1.2.1. Penetrasi Internet

Miniwatts Marketing Group merilis statistik penggunaan internet oleh masyarakat dunia yang terus mengalami peningkatan signifikan yaitu sebesar 4,57 (empat koma lima tujuh) milyar pada tahun 2019 dari total 7,7 (tujuh koma tujuh) milyar populasi dunia. Selanjutnya berdasarkan wilayah geografis dapat dilihat, Asia menempati urutan pertama sebagai pengguna internet mencapai 55% (lima puluh lima per seratus) dari total populasi dunia atau terbanyak di dunia. Data statistik pengguna internet dunia dapat dilihat pada Tabel 1.1.

Tabel 1.1 Data Statistik Pengguna Internet Dunia

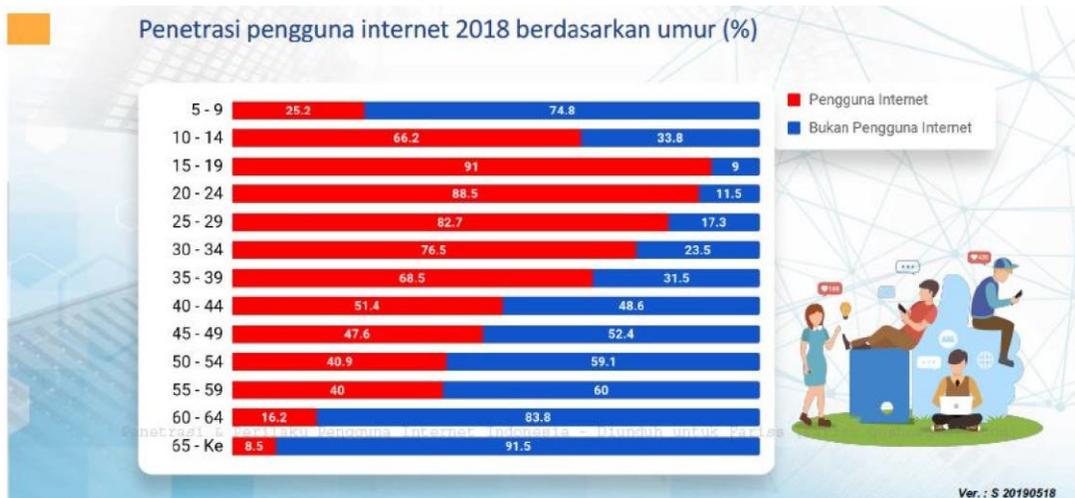
World Internet Usage and Population Statistics 2019-Year End Estimates						
World Regions	Population (2020 Est.)	Population % of World	Internet Users 31 Dec 2019	Penetration Rate (% Pop.)	Growth 2020-2020	Internet World %
Africa	1.340.598.447	17,2%	526.374.930	39,3%	11.159%	11,5%
Asia	4.294.516.659	55,1%	2300.469.859	53,6%	1.913%	50,3%
Europe	834.995.197	10,7%	727.814.272	87,2%	592%	15,9%
Latin America / Caribbean	658.345.826	8,5%	453.702.292	68,9%	2.411%	10,0%
Middle East	260.991.690	3,9%	180.498.292	69,2%	5.395%	3,9%
North America	368.869.647	4,7%	348.908.868	94,6%	222%	7,6%
Oceania/ Australia	42.690.838	0,5%	28.775.373	67,4%	277%	0,6%
World Total	7.796.615.710	100,0%	4.574.150.134	58,7%	1.167%	100,0%

Berdasarkan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2018, Indonesia sebagai salah satu negara dengan populasi terbanyak di Asia Tenggara, pada tahun 2018 memiliki pengguna internet aktif sebanyak 171,17 (seratus tujuh puluh satu koma satu tujuh) juta jiwa atau sebanyak 64,8% (enam puluh empat koma delapan per seratus) dari total populasi Indonesia sebanyak 264,16 (dua ratus enam puluh empat koma satu enam) juta. Hal tersebut mengalami peningkatan dari tahun sebelumnya yang hanya sebanyak 143,26 (seratus empat puluh tiga koma dua enam) juta jiwa pengguna internet aktif. Di antara pulau di seluruh Indonesia, Pulau Jawa sebagai pulau dengan kontribusi pengguna internet aktif terbanyak sebesar 55,7% (lima puluh lima koma tujuh per seratus) dari total populasi Indonesia, disusul dengan pulau Sumatera dan Papua. Persentase kontribusi pengguna internet per wilayah dapat dilihat pada Gambar 1.1.



Gambar 1.1 Kontribusi Pengguna Internet per Wilayah

Pengguna internet terbanyak ada pada rentang usia 15 (lima belas) hingga 19 (sembilan belas) tahun. Sementara itu, pengguna terbanyak kedua berada pada umur 20 (dua puluh) hingga 24 (dua puluh empat) tahun. Penetrasi pengguna internet 2018 berdasarkan umur selengkapnya diilustrasikan pada Gambar 1.2.



Gambar 1.2 Penetrasi Pengguna Internet 2018 berdasarkan Umur

Uraian di atas menunjukkan bahwa pengguna internet di Indonesia semakin meningkat, dimana segala aktivitas telah beralih dari manual menjadi digital. Tidak hanya terbatas pada masyarakat umum saja, peningkatan penggunaan internet pada sektor pemerintah dan sektor kritikal nasional juga sangat signifikan, karena dapat meningkatkan kapabilitas organisasi dan efisiensi dalam pelayanan publik yang berujung pada percepatan pertumbuhan ekonomi.

Indonesia sebagai negara dengan pertumbuhan pengguna internet terbesar keempat di dunia, menghadapi peluang sekaligus ancaman besar dengan perkembangan teknologi digital dan internet baik dari dimensi sosial, politik, dan ekonomi, seperti provokasi politik, hoaks, SARA, ujaran kebencian, ideologi radikalisme, terorisme, *hacking*, pencurian data, penipuan daring, dan tindak kejahatan lainnya di ruang siber. Hal tersebut harus dapat diantisipasi, dicegah, dan ditangani untuk menjamin kedaulatan bangsa.

1.2.2. Revolusi Industri 4.0

Revolusi Industri 4.0 ditandai dengan pesatnya perkembangan pemanfaatan teknologi digital di berbagai bidang. Gelombang transformasi teknologi telah menjadikan seluruh warga dunia terhubung dalam sebuah 'desa global'. Perpaduan teknologi telekomunikasi, internet, dan penyiaran, telah mendorong munculnya infrastruktur jaringan pita lebar yang mendorong lahirnya ekonomi baru. Jaringan pita lebar memberikan manfaat bagi peningkatan kualitas kehidupan sosial dan ekonomi dengan globalisasi ekonomi digital. Di sisi lain, keterhubungan dengan jaringan pita lebar global, memunculkan ancaman pada seluruh aset kritikal. Keterhubungan global ini

membentuk dunia siber dengan ciri interaksi daring. Keterhubungan daring memberi banyak kemudahan, sekaligus menghadirkan kerentanan dan ancaman baru. Virus serta *malware* dapat dengan mudah dikirimkan lewat internet yang akhirnya dapat menyebabkan kerusakan pada sistem dan kebocoran data.

Penetapan *roadmap* “*Making Indonesia 4.0*” dengan salah satu inisiatif lintas sektornya yaitu pembangunan infrastruktur digital nasional, memaksa Indonesia untuk siap dalam memasuki era industri 4.0 dan implementasinya. Tidak dapat dipungkiri bahwa bidang keamanan siber akan menjadi bagian penting dalam tatanan era revolusi Industri 4.0, dimana kejahatan siber semakin beragam dan berdampak masif secara nasional yang dapat mengancam kedaulatan bangsa.

1.2.3. Ancaman di Ruang Siber

Siber merupakan suatu arena virtual yang terbentuk akibat terkoneksi berbagai perangkat komputasi dalam sebuah jejaring digital raksasa yang tumbuh secara eksponensial. Ruang siber merupakan tempat maya dimana komunikasi tersebut terjadi. Dengan potensi berubahnya tren peperangan dari fisik menjadi non fisik atau dari konvensional menjadi modern, maka ruang siber dengan media internet akan menjadi ancaman baru bagi negara beserta infrastruktur kritis. Kerusakan maupun kerugian yang didapatkan dari peperangan modern sama besarnya dengan kerugian yang didapatkan dari peperangan konvensional.

Kejadian di Estonia pada Tahun 2007 dan Georgia pada Tahun 2008 merupakan contoh dari serangan kejahatan siber dengan memanfaatkan berbagai metode penyerangan seperti *Distributed Denial of Service* (DDoS), *web defacement*, *DNS server attacks*, *mass e-mail*, dan *comment spam*. Dengan adanya serangan tersebut mampu melumpuhkan negara dengan sasaran infrastruktur kritis. Serangan siber lainnya terjadi pada infrastruktur nuklir di Iran oleh Stuxnet pada tahun 2010 dengan menginfeksi lebih dari 60.000 (enam puluh ribu) komputer yang merupakan lebih dari setengah komputer yang ada di Iran yang efeknya pun menyebar ke Indonesia. Seperti dilansir oleh Symantec, Indonesia berada pada urutan kedua setelah Iran di antara 10 besar negara yang mengalami serangan Stuxnet. Serangan siber juga terjadi pada Pusat Kesehatan Singhealth di Singapura pada Juni 2018,

sebanyak 1,5 (satu koma lima) juta data kesehatan pribadi berhasil dicuri dan dibocorkan.

Pada tahun 2017, Indonesia mengalami insiden yang menyebabkan kerugian materi dan ekonomi yang tidak sedikit, yaitu serangan *ransomware wannacry* yang menyerang rumah sakit harapan kita dan rumah sakit dharmais Jakarta. *Malware* ini menyerang ratusan server dan komputer yang mengakibatkan terganggunya operasional rumah sakit. Kejadian lainnya adalah terganggunya sistem teknologi informasi untuk melayani tiket penumpang di Terminal 3 Bandara Soekarno-Hatta pada tanggal 23 Agustus 2019 dan padamnya listrik di wilayah Jabodetabek pada tanggal 4 Agustus 2019 selama beberapa jam. Walaupun kejadian tersebut bukan berasal dari aktivitas serangan siber, namun jika kemudian hari terjadi serangan siber pada titik vital yang sama, maka kerusakan dan kerugian akan sama seperti yang dialami pada kejadian tersebut.

Berdasarkan laporan monitoring tahunan yang dikeluarkan oleh Pusat Operasi Keamanan Siber BSSN, pada tahun 2019 terdapat sekitar 290 (dua ratus sembilan puluh) juta serangan siber yang berhasil diidentifikasi melalui sistem monitoring mata garuda. Jumlah serangan terbanyak adalah 137,4 (seratus tiga puluh tujuh koma empat) juta percobaan pembocoran data, disusul 117,9 (seratus tujuh belas koma sembilan) juta serangan *trojan*, 12,5 (dua belas koma lima) juta serangan terhadap *port* 80 (delapan puluh) serta 6,4 (enam koma empat) juta serangan ke *name server*. Selain melalui sistem monitoring mata garuda, BSSN juga menerima laporan aduan siber dengan jumlah total laporan baik dari sektor pemerintah, infrastruktur kritikal nasional, ekonomi digital, serta masyarakat umum sebanyak 4.224 (empat ribu dua ratus dua puluh empat) laporan aduan publik, 2.831 (dua ribu delapan ratus tiga puluh satu) laporan diantaranya terkait kerentanan. Laporan monitoring serangan siber selama tahun 2019 ditunjukkan pada Gambar 1.3.



Gambar 1.3 Serangan Siber periode Januari Desember 2019

Berbeda dengan kecenderungan tahun sebelumnya, serangan terbesar pada tahun 2019 yaitu serangan percobaan pembocoran data. Serangan ini tidak langsung membuktikan bahwa pengumpulan data informasi berhasil dilakukan sehingga terjadi kebocoran data, akan tetapi merupakan sinyal dan indikasi bahwa percobaan kearah pencurian data sudah dilakukan yang apabila kondisinya ternyata sesuai dengan harapan *hacker* maka memungkinkan terjadinya eskalasi ke arah pengambilalihan sistem dan kebocoran data penting. Di sisi lain, serangan *malware* merupakan serangan kedua terbesar tahun 2019.

Pada sektor perekonomian, serangan siber atau kejahatan siber memberikan dampak berupa kerugian finansial yang cukup besar kepada suatu negara. Kerugian yang dialami Indonesia juga tidak kecil. Pada 2013 Daka Advisory meluncurkan laporannya dengan menghitung perkiraan nilai kerugian siber berdasarkan 4 (empat) kategori sebagaimana tercantum dalam Tabel 1.2.

Tabel 1.2 Perkiraan Kerugian Ekonomi Akibat Kejahatan Siber

	Global (US\$)	Indonesia (US\$)
GDP (2012)	71.620 miliar	895 miliar
Persentase dari GDP global		1,20%
Kerugian akibat:		
• <i>Genuine cybercrime</i>	3.457 juta	43 juta
• <i>Transitional cybercrime</i>	46.600 juta	582 juta
• <i>Cybercriminal infrastructure</i>	24.840 juta	310 juta
• <i>Traditional crimes becoming cyber</i>	150.200 juta	2.748 juta

Berdasarkan tabel perkiraan diatas, Indonesia diprediksi menderita kerugian ekonomi dari kejahatan siber yang sebenarnya sebesar USD 43 (empat puluh tiga) juta, kejahatan transisional sebesar USD 582 (lima ratus delapan puluh dua) juta, kejahatan siber pada infrastruktur sebesar USD 310 (tiga ratus sepuluh) juta, dan kejahatan tradisional yang mengarah pada kejahatan siber sebesar USD 2.748 (dua ribu tujuh ratus empat puluh delapan) juta.

1.2.4. Pencapaian Kinerja BSSN 2018-2019

Terbentuknya BSSN pada tahun 2017 ditindaklanjuti dengan penyusunan Renstra BSSN 2018-2019 dengan berpedoman pada RPJMN 2015-2019 dan didasarkan pada tugas fungsi BSSN. Renstra BSSN Tahun 2018-2019 memuat 6 (enam) tujuan yang ingin dicapai yaitu tercapainya fondasi struktur, sistem dan budaya organisasi BSSN yang kuat, tersusunnya kebijakan, sistem dan prosedur berstandar global dalam bidang keamanan siber dan sandi di Indonesia, tersedianya sistem manajemen talenta untuk menarik, memelihara dan meretensi sumber daya manusia siber dan sandi terbaik, tercapainya kinerja pencegahan, deteksi, mitigasi, dan penanggulangan ancaman keamanan siber dan sandi, terselenggaranya kerjasama-kerjasama strategis dengan seluruh pihak untuk membangun keamanan siber dan sandi di Indonesia, dan terbentuknya kesadaran, perilaku dan budaya keamanan siber yang baik pada setiap warga negara Indonesia. Dalam rangka mencapai tujuan BSSN tersebut, telah ditetapkan sasaran strategis dan indikatornya dengan hasil capaian kinerja sebagaimana pada Tabel 1.3.

Tabel 1.3 Capaian Kinerja BSSN 2018–2019

SASARAN STRATEGIS	INDIKATOR	CAPAIAN					
		2018		2019			
		Target	Realisasi	Target	Realisasi		
1	Terselenggaranya Keamanan Siber secara Andal, Profesional dan Terpercaya	1.1	Peringkat Indonesia pada <i>Global Cybersecurity Index</i> (Publikasi ITU)	68	41	64	41
2	Terselenggaranya Pendayagunaan Kapabilitas Identifikasi dan Deteksi yang Andal	2.1	Tingkat Cakupan Penilaian Risiko Keamanan Siber Nasional	25%	37.18%	30%	44,77%
		2.2	Tingkat Cakupan Potensi Ancaman Siber yang Berhasil Dideteksi	20%	20%	25%	25,41%
3	Terselenggaranya Pengembangan Kapabilitas Proteksi yang Optimal	3.1	Tingkat Penerapan Proteksi Keamanan Siber	0.600	0.571	0,615	0,657
4	Terselenggaranya Pendayagunaan Kapabilitas Penanggulangan dan Pemulihan yang Kapabel	4.1	Tingkat Kesiapan Pemangku Kepentingan terhadap Insiden Keamanan Siber Nasional	60%	70.73%	70%	63,73%
5	Terselenggaranya Pendayagunaan Kapabilitas Pemantauan dan Pengendalian yang Profesional	5.1	Indeks Persepsi Publik terhadap Reputasi Pemerintah (BSSN) dalam Ranah Siber	3.00	4.21	3,20	4,32
6	Terselenggaranya Pengelolaan Sumber Daya Manusia, Organisasi, dan Tata Kelola yang Kompeten	6.1	Indeks Reformasi Birokrasi	74.54	75.02	77,11	76,53

Dalam periode 2018-2019, BSSN telah berhasil meningkatkan skor dan peringkat Indonesia pada *Global Cybersecurity Index* (GCI) dengan menempati peringkat ke 41 (empat puluh satu) dari 194 (serratus Sembilan puluh empat) negara anggota *The UN International Telecommunication Union* (ITU) dengan skor 0,776 (nol koma tujuh tujuh enam) dari sebelumnya pada tahun 2017 peringkat ke-70 dari 193

negara dengan perolehan skor 0,424 (nol koma empat dua empat). Peningkatan skor dan peringkat dalam GCI menunjukkan peningkatan komitmen negara Indonesia terhadap keamanan siber di tingkat global. Peningkatan berkelanjutan terus diupayakan, diantaranya dengan melakukan koordinasi dan kolaborasi dengan para pemangku kepentingan untuk membahas langkah-langkah yang perlu dilakukan pada instansi masing-masing. BSSN juga telah berhasil mencapai target output prioritas nasional pada Rencana Kerja Pemerintah (RKP) 2018-2019 khususnya pada prioritas nasional “Stabilitas Keamanan Nasional dan Kesuksesan Pemilu” dan berkontribusi aktif dalam suksesnya pelaksanaan *annual meeting international monetary fund world bank* 2018, asian games 2018, asian para games 2018, pemilihan kepala daerah serentak 2019, dan pemilihan presiden 2019.

Dalam hal pelaksanaan reformasi birokrasi dan tata kelola organisasi, BSSN berhasil meningkatkan kualitas penyelenggaraan reformasi birokrasi di BSSN yang ditandai dengan meningkatnya indeks reformasi birokrasi dari tahun 75,02 (tujuh puluh lima koma nol dua) pada tahun 2018 menjadi 76,53 (tujuh puluh enam koma lima tiga) pada tahun 2019. Hal tersebut tidak terlepas dari capaian akuntabilitas atas laporan keuangan BSSN yang mendapatkan opini Wajar Tanpa Pengecualian (WTP), Evaluasi atas Akuntabilitas Kinerja Instansi Pemerintah (AKIP) yang mengalami peningkatan nilai dari predikat Cukup (CC) pada tahun 2016 menjadi Baik (B) pada tahun 2018 dan 2019, serta inisiatif penataan pada delapan area perubahan reformasi birokrasi.

Selain pencapaian kinerja di atas, BSSN juga terlibat dalam berbagai pelaksanaan Instruksi Presiden diantaranya Instruksi Presiden Nomor 9 Tahun 2000 tentang Pengarusutamaan Gender yang telah menjadi pengarusutamaan pembangunan nasional sejak RPJMN I (2005-2009). Pengarusutamaan Gender (PUG) merupakan strategi untuk mewujudkan kesetaraan dan keadilan gender melalui kebijakan dan program yang diarahkan pada peningkatan kualitas hidup dan peran perempuan di berbagai bidang pembangunan. Dalam agenda pembangunan menjaga stabilitas keamanan nasional dengan mewujudkan keamanan ruang siber, isu kesetaraan gender masih perlu menjadi perhatian. Penelitian yang dilakukan Fortinet pada tahun 2019, dari 50% (lima puluh per seratus) keterwakilan wanita dari populasi

keseluruhan dan tenaga kerja global, hanya 11% (sebelas per seratus) diantaranya yang bekerja di bidang keamanan siber.

Pada periode Renstra BSSN Tahun 2018-2019, BSSN secara konsisten melaksanakan kebijakan dan program pengarusutamaan gender baik dalam bidang kesehatan, pendidikan, dan keterwakilan dalam jabatan. Pada periode 2020-2024 program dan kebijakan PUG juga harus mempertimbangkan isu-isu pemberdayaan perempuan maupun kualitas partisipasi mereka dalam keterlibatan pembangunan keamanan siber nasional.

1.2.5. Pemenuhan Aspirasi Pemangku Kepentingan

Sebagai koordinator dan konsolidator berbagai pemangku kepentingan di bidang siber dan sandi, dan dalam rangka melaksanakan amanat Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, BSSN menerbitkan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah. Tujuan diterbitkannya Peraturan tersebut antara lain:

1. menciptakan harmonisasi dalam melaksanakan persandian untuk pengamanan informasi antara Pemerintah Pusat dan pemerintah daerah;
2. meningkatkan komitmen, efektivitas, dan kinerja pemerintah daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi; dan
3. memberikan pedoman bagi pemerintah daerah dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah.

Selain itu, BSSN berperan aktif dalam memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik, melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi dan transaksi elektronik yang mengganggu ketertiban umum, dan mencegah penyebaran dan penggunaan informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan. Sesuai Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, BSSN melalui Balai Sertifikasi Elektronik memproduksi sertifikat elektronik yang dapat digunakan oleh

seluruh pemangku kepentingan disemua sektor maupun masyarakat. Dalam rangka penguatan pada aspek hukum, berikut peraturan turunan tentang mekanisme serta pemanfaatan sertifikat elektronik yang dapat menjangkau lebih luas lagi penggunaannya saat ini tengah dipersiapkan.

Salah satu upaya BSSN dalam mewujudkan asas manfaat dari penggunaan sertifikat elektronik adalah melakukan koordinasi dan kerjasama dalam bentuk *Memorandum of Understanding* (MoU) yang dituangkan dalam perjanjian kerjasama teknis dengan instansi pemerintah, baik di pusat maupun daerah, serta pemangku kepentingan di sektor IKN dan ekonomi digital. Selain upaya tersebut, dalam rangka pengendalian informasi, BSSN juga memperhatikan tuntutan masyarakat untuk memberikan edukasi dan literasi bidang siber dan sandi, sehingga masyarakat memahami tentang urgensi suatu informasi memiliki nilai yang dapat dipertanggungjawabkan kebenarannya dan disampaikan sesuai waktu yang dibutuhkan. Kegiatan dan indikator peningkatan kesadaran masyarakat yang telah dilakukan BSSN, antara lain kegiatan edukasi kesadaran keamanan informasi data pribadi kepada masyarakat umum dan literasi pengendalian informasi yang dilaksanakan di berbagai daerah di Indonesia dengan total peserta mencapai kurang lebih 20.000 (dua puluh ribu) orang yang berasal dari berbagai kalangan.

1.3. POTENSI DAN PERMASALAHAN

1.3.1. Potensi

1.3.1.1. BSSN sebagai Institusi Pengelola Keamanan Siber Nasional

Dalam upaya menjalankan amanah untuk melaksanakan keamanan siber dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan seluruh unsur terkait, BSSN mempunyai beberapa potensi yang dapat menjadi salah satu unsur pendorong terciptanya keamanan siber Indonesia, sebagai berikut:

1. memperkuat kebijakan di bidang keamanan siber dan sandi seluruh pemangku kepentingan di bidang siber.
2. memperkuat kolaborasi dan kerjasama antara institusi dan pemangku kepentingan di bidang keamanan siber dan sandi serta mengkonsolidasikan masyarakat, akademisi, praktisi, dan komunitas siber di dalam dan luar negeri dalam rangka menjaga keamanan siber Indonesia.

3. mengembangkan sumber daya manusia yang profesional di bidang keamanan siber di Indonesia. BSSN dapat membangun budaya dan perilaku untuk meningkatkan produktivitas dan profesionalisme sumber daya manusia, salah satunya dengan penyusunan peta okupasi nasional dalam kerangka kualifikasi nasional pada bidang keamanan siber serta menginisiasi pemberian penghargaan di bidang keamanan siber untuk berbagai organisasi, baik pemerintah maupun swasta bahkan untuk tingkat individu. BSSN di masa depan diharapkan dapat berperan besar dalam memberikan edukasi kepada masyarakat di bidang keamanan siber, dapat mengambil peran penting dalam pengendalian informasi dan berita palsu melalui literasi-literasi terkait.
4. melakukan inovasi untuk meningkatkan pertumbuhan organisasi dan menciptakan serta mendorong kemandirian teknologi keamanan siber dan sandi untuk mewujudkan kedaulatan siber.

Pelaksanaan tugas fungsi BSSN akan berkontribusi pada terwujudnya Indonesia yang berdaulat dan mandiri di bidang keamanan siber dan persandian. Berdaulat dalam hal ini memiliki sejumlah makna, antara lain:

1. pertama, BSSN merupakan institusi yang bertanggung jawab untuk menegakkan kedaulatan dalam melakukan penjaminan keamanan informasi dan keamanan siber nasional. Upaya penjaminan tersebut dilakukan untuk menjunjung tinggi keberlangsungan kepentingan nasional.
2. kedua, terkait dengan pemanfaatan peralatan keamanan siber dan persandian, seluruh peralatan keamanan siber dan persandian yang beredar di wilayah negara kesatuan republik Indonesia haruslah terlebih dahulu mendapatkan sertifikat kesesuaian dari BSSN.
3. ketiga, dalam hal penyiapan sumber daya manusia siber dan sandi yang profesional dan beretika, BSSN memiliki kewenangan penuh untuk memastikan bahwa proses pemenuhannya baik internal maupun eksternal dilakukan dengan sebaik-baiknya.

4. pengertian mandiri dalam konteks keamanan siber dan persandian, dapat dimaknai bahwa BSSN dapat mewujudkan kemandirian di dalam sejumlah hal, antara lain mandiri dalam hal sikap politik, cara bekerja, pengambilan keputusan, pengembangan karya, dan kapabilitas untuk menjaga keamanan siber dan persandian di Negara Indonesia.

1.3.1.2. Sumber Daya Manusia BSSN

Untuk melaksanakan tugas dan fungsi pengelolaan keamanan siber yang optimal, berdasarkan struktur organisasi yang tercantum dalam Peraturan BSSN Nomor 2 Tahun 2018, BSSN memiliki 5 (lima) unit eselon I dan 6 (enam) unit eselon II serta 1 (satu) unit eselon III yang langsung di bawah kepemimpinan Kepala BSSN.

BSSN memiliki sumber daya manusia keseluruhan sejumlah 1.149 (seribu seratus empat puluh sembilan) orang personel yang terdiri dari laki-laki sebanyak 809 (delapan ratus sembilan) dan perempuan sebanyak 340 (tiga ratus empat puluh) orang. Jumlah tersebut belum termasuk mahasiswa sejumlah 372 (tiga ratus tujuh puluh dua) orang yang masih dalam proses mengikuti perkuliahan di politeknik siber dan sandi negara.

Sumber daya manusia BSSN juga terdiri dari berbagai latar belakang pendidikan yang dapat mendukung tugas dan peran dalam perkuatan pelaksanaan tugas pokok dan fungsinya. Upaya peningkatan kapabilitas sumber daya manusia BSSN terus ditingkatkan, salah satunya adalah dengan penambahan alokasi beasiswa S2 dan S3 ke beberapa universitas terbaik di dalam dan luar negeri. Rincian potensi sumber daya manusia BSSN dapat dilihat pada Tabel 1.4.

Tabel 1.4 Dislokasi Pegawai Berdasarkan Latar Belakang Pendidikan dan Golongan

Orga- nisasi	Golongan						Jenjang Pendidikan							Total
	IV	III	II	I	Ho- norer	CPN S	S3	S2	S1	D3/ D2	SMA	SMP	SD	
Jumlah	89	764	168	-	-	128	6	236	585	99	214	6	3	1149
Per- sentase (%)	8	66	15	-	-	11	0.52	20.54	50.91	8.62	18.62	0,52	0,26	

Selain itu, BSSN juga telah menetapkan nilai-nilai inti yang menjadi dasar institusi BSSN, pimpinan, dan seluruh pegawai BSSN dalam berperilaku, bertindak, dan bersikap dalam kaitannya dengan upaya pencapaian visi dan misi BSSN melalui Peraturan BSSN Nomor 3 Tahun 2018 tentang Sistem Nilai BSSN yang meliputi:

1. Profesional

Profesional merupakan suatu nilai yang terdiri atas kompeten dalam bekerja, bekerja sama dengan pihak lain untuk mencapai tujuan, dan memiliki komitmen terhadap prosedur yang telah ditetapkan.

2. Integritas

Integritas merupakan suatu nilai yang terdiri dari perilaku terpuji dalam bekerja, disiplin dalam berperilaku, dan berdedikasi terhadap tugas dan pekerjaan.

3. Adaptabilitas teknologi

Adaptabilitas teknologi merupakan suatu nilai yang terdiri atas perilaku inovatif dan kekinian serta mengikuti dan tanggap terhadap perubahan teknologi.

4. Tepercaya

Tepercaya merupakan suatu nilai yang terdiri atas dapat dipercaya, berorientasi pada keamanan informasi, dan tidak berpihak pada kekuatan politik manapun.

Penanaman nilai-nilai BSSN kepada seluruh pegawai merupakan hal yang penting demi pencapaian visi, misi, dan tujuan organisasi. Untuk itu, dimunculkan singkatan sistem nilai BSSN yaitu PINTAR yang bertujuan agar mudah diingat, mudah disosialisasikan, mudah diartikulasikan, mudah dihayati, sehingga secara keseluruhan menjadi lebih mudah diimplementasikan. Selain menjadi tata cara atau perilaku organisasi atau individu, sistem nilai juga menggambarkan kinerja dan pelayanan, menjadi arah pengembangan kapabilitas organisasi, mencerminkan hubungan antar unsur BSSN serta memberikan jaminan dalam pemenuhan kebutuhan dan harapan pemangku kepentingan BSSN.

1.3.2. Permasalahan

Beberapa faktor penting yang menjadi pertimbangan dalam pelaksanaan tugas dan fungsi BSSN periode 2020-2024 sebagai berikut:

1. Geo-Ekonomi

Pada awal tahun 2019, ATKearney telah membuat beberapa prediksi yang semuanya diyakini memiliki implikasi yang penting bagi lingkungan perdagangan global. Diantaranya prediksinya bahwa perang dagang antara Tiongkok dan Amerika Serikat akan semakin meningkat intensitasnya. Kondisi ini tentunya juga akan berpengaruh terhadap laju perekonomian nasional, dimana Tiongkok dan Amerika Serikat masuk dalam 3 (tiga) besar tujuan ekspor Indonesia yang kontribusinya jika digabung mencapai 25% (dua puluh lima per seratus) terhadap total ekspor Indonesia. Sehingga pengambilan kebijakan ekonomi yang tepat menjadi salah satu kunci bagi Indonesia untuk bisa keluar dari himpitan pengaruh perang dagang raksasa ekonomi dunia tersebut.

2. Geo-Politik dan Strategi

Secara geografis Indonesia merupakan kepulauan yang terletak pada pertemuan 2 (dua) benua yaitu Benua Asia dan Benua Australia, serta 2 (dua) samudera yaitu Samudera Hindia dan Samudera Pasifik. Kondisi tersebut membuat Indonesia memiliki posisi strategis, wilayah alur laut kepulauan Indonesia merupakan bagian dari jalur perdagangan dan pelayaran internasional. Posisi silang Indonesia sebagai jalur perdagangan dan transportasi lalu lintas terpadat di dunia dapat menjadi sumber devisa di bidang perekonomian sekaligus ancaman jika ditinjau dari aspek pertahanan karena posisinya yang terbuka bagi negara lain untuk memasuki wilayah Indonesia. Selain itu, Indonesia yang berada pada pertemuan empat lempeng tektonik, yaitu lempeng Benua Asia, Benua Australia, lempeng Samudera Hindia dan Samudera Pasifik menjadi salah satu negara dengan tingkat risiko bencana yang tinggi di dunia, yaitu letusan gunung berapi, gempa bumi, tsunami, banjir, dan tanah longsor.

3. Bonus Demografi

Indonesia mempunyai peluang untuk dapat menikmati bonus demografi, yaitu kondisi yang ditandai dengan menurunnya rasio ketergantungan sehingga penduduk usia kerja terus meningkat.

Indonesia mempunyai potensi untuk memanfaatkan bonus demografi baik secara nasional maupun regional. Bonus demografi tidak didapat secara otomatis, tetapi harus diraih dengan arah kebijakan yang tepat, sehingga tidak timbul permasalahan baru. Berbagai kebijakan yang tepat diperlukan untuk menyiapkan kualitas sumber daya manusia yang akan masuk sebagai angkatan kerja, menjaga penurunan fertilitas, menyiapkan keterampilan dan kompetensi tenaga kerja, kebijakan ekonomi dalam menciptakan lapangan kerja, fleksibilitas pasar tenaga kerja, keterbukaan perdagangan serta dukungan sarana dan prasarana.

1.3.3. Analisis Lingkungan Strategis

BSSN terus berupaya berkembang untuk meningkatkan eksistensinya dalam memenuhi tuntutan lingkungan baik internal maupun eksternal sehingga organisasi perlu mengerahkan segala kemampuan dengan memperhatikan kelemahan, memanfaatkan peluang dan mengatasi tantangan yang kompleks. Guna mengetahui isu-isu strategis saat ini dilakukan analisis lingkungan strategis. Kekuatan dan peluang merupakan potensi yang dapat dikembangkan dalam rangka memperkuat organisasi, sedangkan kelemahan dan tantangan merupakan permasalahan yang perlu diantisipasi agar organisasi dapat terus berkembang.

Hasil analisis lingkungan strategis sebagai berikut:

1. Kekuatan

- a. tersedianya sumber daya manusia yang memiliki kompetensi khusus di bidang keamanan siber dan sandi.
- b. BSSN merupakan instansi pembina jabatan fungsional sandiman.
- c. BSSN memiliki kewenangan untuk melakukan pengaturan ekosistem ekonomi digital dan literasi publik.
- d. BSSN memiliki struktur organisasi yang sudah menangani cakupan penguatan keamanan siber dan sandi.
- e. BSSN memiliki kewenangan mengonsolidasikan semua unsur keamanan siber.
- f. BSSN merupakan satu-satunya instansi lembaga pendidikan dan pelatihan pengakreditasi lembaga pemerintah penyelenggara diklat sandi dan siber.

2. Kelemahan

- a. belum optimalnya pemenuhan jumlah sumber daya manusia dibandingkan kebutuhan sumber daya manusia.
 - b. belum optimalnya pemetaan jabatan dan penempatan sumber daya manusia.
 - c. belum optimalnya sistem pola karier di BSSN.
 - d. belum tersedianya standar kompetensi bidang Keamanan Siber yang masih dalam penyusunan.
 - e. belum optimalnya integrasi sistem informasi.
 - f. belum optimalnya pemanfaatan laboratorium untuk penelitian dan pengembangan.
 - g. belum tersedianya regulasi dan standar terkait keamanan siber dan sandi secara menyeluruh di BSSN.
3. Peluang Organisasi
- a. pemanfaatan teknologi era Industri 4.0 seperti *big data*, *artificial intelligence*, *drone*, dan sebagainya untuk peningkatan kinerja organisasi.
 - b. adanya amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik agar BSSN mengelola keamanan sistem pemerintahan berbasis elektronik, menyusun standar keamanan sistem pemerintahan berbasis elektronik Nasional, dan melaksanakan audit keamanan sistem pemerintahan berbasis elektronik.
 - c. adanya amanat pengamanan penyelenggaraan sistem dan transaksi elektronik berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
 - d. adanya proyek prioritas strategis nasional penguatan ketahanan dan keamanan siber pada RPJMN Tahun 2020-2024 yang salah satunya peningkatan kapasitas sumber daya manusia keamanan siber dari berbagai sektor seperti K/L/D, IKN, dan ekonomi digital.
 - e. adanya arahan presiden dalam RPJMN Tahun 2020-2024 sebagai strategi dalam pelaksanaan nawacita dan pencapaian sasaran pembangunan nasional, yaitu diantaranya penguatan implementasi manajemen aparatur sipil negara berbasis merit, penyederhanaan birokrasi, dan pengoptimalan manajemen kinerja agar lebih handal, efektif, dan akuntabel.

4. Ancaman Organisasi

- a. ancaman kebocoran data dan informasi diplomasi Indonesia melalui spionase siber.
- b. penerapan ekosistem teknologi jaringan nirkabel (5G) dengan kinerja yang menjanjikan kecepatan data tinggi, pengurangan latensi, penghematan energi, kapasitas sistem yang lebih tinggi, dan konektivitas perangkat secara masif akan menguraikan masalah keamanan siber yang baru.
- c. belum adanya penguatan terhadap pengesahan rancangan undang-undang tentang keamanan dan ketahanan siber.
- d. maraknya ancaman siber melalui *hacktivism*, kejahatan siber, serangan siber yang berdampak terhadap terhambatnya pertumbuhan ekonomi.
- e. rendahnya pengetahuan masyarakat terkait keamanan siber.
- f. terjadinya perang pikiran melalui berita bohong, *cyber bullying*, dan ujaran kebencian melalui media sosial.
- g. muncul dan berkembangnya masyarakat 5.0 yang mengadopsi teknologi informasi dan komunikasi (TIK). Hal ini berpotensi munculnya ancaman ketika TIK digunakan untuk kegiatan kejahatan siber.
- h. maraknya serangan siber yang semakin berkembang dan masif bahkan terhadap infrastruktur vital.
- i. keamanan siber belum menjadi perhatian utama bagi *startup* sehingga berdampak terhadap perkembangan sektor IKN. Hal ini berpotensi menimbulkan ancaman keamanan siber.
- j. koordinasi antar lembaga penanganan keamanan siber dan sandi yang belum optimal.

Hasil analisis lingkungan strategis secara ringkas ditunjukkan pada Gambar 1.4.

POTENSI DAN PERMASALAHAN



ANCAMAN

- Ancaman kebocoran data dan informasi diplomasi Indonesia melalui cyber spionase
- Adanya resistensi dari beberapa kelompok dan masyarakat terhadap pengesahan RUU Keamanan dan Ketahanan Siber (KKS)
- Potensi terpusatnya seluruh anggaran untuk riset keamanan siber dan sandi di Badan Riset dan Inovasi Nasional. Jika BSSN tidak menindaklanjuti dengan baik, porsi anggaran riset berpotensi menjadi lebih kecil
- UNICORN Indonesia dikuasai asing

KEKUATAN

- Tersedianya SDM yang memiliki kompetensi khusus di bidang keamanan siber dan sandi
- BSSN merupakan instansi pembina Jabatan Fungsional Sandiman
- BSSN memiliki struktur organisasi yang sudah menangani cakupan penguatan keamanan siber dan sandi
- BSSN memiliki kewenangan mengkonsolidasikan semua unsur terkait keamanan siber
- BSSN merupakan satu-satunya instansi lembaga pendidikan dan pelatihan (diklat) pengakreditasi lembaga pemerintah penyelenggara diklat sandi dan siber

KELEMAHAN

- Belum optimalnya pemenuhan jumlah SDM dibandingkan kebutuhan SDM
- Belum optimalnya pemetaan jabatan dan penempatan SDM
- Sistem pola karir BSSN belum optimal
- Belum tersedianya standar kompetensi bidang Keamanan Siber (Masih dalam penyusunan)
- Belum optimalnya integrasi sistem informasi
- Belum optimalnya pemanfaatan laboratorium untuk penelitian dan pengembangan
- Belum tersedianya regulasi dan standar terkait keamanan siber dan sandi secara menyeluruh di BSSN

PELUANG

- Pemanfaatan teknologi era Industri 4.0 seperti Big Data, AI, drone, dan sebagainya untuk peningkatan kinerja organisasi
- Adanya arahan Perpres 95 Tahun 2018 agar BSSN melaksanakan pengamanan SPBE, menyusun standar keamanan SPBE Nasional, dan melaksanakan audit keamanan SPBE
- Adanya arahan untuk pengamanan penyelenggaraan sistem dan transaksi elektronik berdasarkan PP No. 82 Tahun 2012 tentang Penyelenggaraan sistem dan transaksi elektronik
- Adanya arahan penguatan keamanan siber yang merupakan major project pada prioritas nasional. Salah satunya adalah peningkatan kapasitas SDM Kamsiber dari berbagai sektor seperti K/L/D, IIKN, dan ekonomi digital
- Adanya arahan RPJMN untuk memperkuat implementasi manajemen ASN berbasis merit
- Adanya arahan Presiden agar organisasi melakukan reformasi struktural dan mindset

Gambar 1.4 Hasil Analisis Lingkungan Strategis

Berdasarkan kekuatan, kelemahan, peluang dan ancaman di atas, dapat diidentifikasi tantangan-tantangan bagi BSSN dalam upaya mewujudkan keamanan siber Indonesia dalam periode 2020–2024 sebagai berikut:

1. Bergulirnya revolusi industri 4.0 yang menjadi pendukung lahirnya teknologi canggih dan peningkatan penetrasi penggunaan internet di Indonesia. Jika hal tersebut tidak diimbangi dengan peningkatan kesadaran keamanan siber dapat mengeskalasi ancaman keamanan siber yang semakin masif bahkan menyasar infrastruktur vital sehingga mengancam kedaulatan bangsa.
2. Tantangan pengelolaan keamanan siber nasional meliputi pengelolaan sumber daya manusia keamanan siber dan sandi, kebijakan atau regulasi keamanan siber dan sandi termasuk di dalamnya strategi keamanan siber nasional, kerjasama, serta kemandirian teknologi keamanan siber dan sandi dalam rangka mewujudkan kedaulatan siber Indonesia.

Di sisi lain, dalam rangka penyelenggaraan tugas dan fungsi BSSN diidentifikasi tantangan yang masih akan dihadapi internal organisasi BSSN meliputi:

1. Aspek kelembagaan yang masih perlu dievaluasi dalam pencapaian sasaran strategis.
2. Aspek Ketatalaksanaan pedoman dan standar operasional prosedur yang belum diterapkan secara menyeluruh.
3. Aspek sumber daya manusia yang kualitasnya perlu ditingkatkan dan
4. Aspek sarana dan prasarana yang terbatas serta sistem informasi yang belum terintegrasi sepenuhnya.

BAB II

VISI, MISI, TUJUAN, DAN SASARAN STRATEGIS

2.1. VISI BSSN

Visi pembangunan nasional tahun 2005-2025 dalam Rencana Pembangunan Jangka Panjang Nasional (RPJPN) yaitu “Indonesia yang Mandiri, Maju, Adil, dan Makmur”. RPJMN Tahun 2020–2024 merupakan tahapan terakhir dari RPJPN Tahun 2005-2025, yang akan mempengaruhi pencapaian target pembangunan nasional. RPJMN Tahun 2020-2024 merupakan penjabaran dari visi dan misi Presiden Joko Widodo dan Wakil Presiden Ma’ruf Amin. Visi Presiden dan Wakil Presiden Tahun 2020–2024 yaitu “Terwujudnya Indonesia Maju yang Berdaulat, Mandiri, dan Berkepribadian dengan Landasan Gotong Royong”. Upaya untuk mewujudkan visi tersebut ditempuh dengan 9 (sembilan) misi atau dikenal sebagai nawacita kedua yaitu :

1. peningkatan kualitas manusia indonesia.
2. struktur ekonomi yang produktif, mandiri, dan berdaya saing.
3. pembangunan yang merata dan berkeadilan.
4. mencapai lingkungan hidup yang berkelanjutan.
5. kemajuan budaya yang mencerminkan kepribadian bangsa.
6. penegakan sistem hukum yang bebas korupsi, bermartabat, dan terpercaya.
7. perlindungan bagi segenap bangsa dan memberikan rasa aman pada seluruh warga.
8. pengelolaan pemerintahan yang bersih, efektif, dan terpercaya.
9. sinergi pemerintah daerah dalam kerangka Negara Kesatuan.

Visi Misi Presiden dan Wakil Presiden di atas selanjutnya dijabarkan ke dalam janji Presiden, dimana dalam bidang pertahanan dan keamanan, BSSN mengampu janji penguatan dan pengembangan sumber daya manusia terutama dalam penguasaan teknologi keamanan siber yang sangat diperlukan dalam pertahanan negara dan mengembangkan sistem keamanan siber dalam kerangka menunjang sistem pertahanan nasional secara keseluruhan. Guna mempertajam visi pembangunan nasional di bidang keamanan siber dan persandian serta untuk menjawab berbagai tantangan dengan memperhatikan lingkungan strategis, maka BSSN menetapkan arah organisasi berupa

visi, misi, tujuan, dan sasaran sebagai suatu institusi yang menjamin kedaulatan siber di Indonesia.

Visi BSSN Tahun 2020–2024 dengan mengacu pada visi Presiden dan Wakil Presiden sebagai berikut:

“Badan Siber dan Sandi Negara yang Andal, Profesional, Inovatif, dan Berintegritas dalam Pelayanan kepada Presiden dan Wakil Presiden untuk Mewujudkan Visi Misi Presiden dan Wakil Presiden: Indonesia Maju yang Berdaulat, Mandiri, dan Berkepribadian Berlandaskan Gotong-Royong”.

Visi BSSN digunakan sebagai arahan kepada semua jajaran di BSSN dalam melaksanakan tugas dan fungsi yang diemban sesuai dengan peraturan dan kebijakan yang telah ada. Melalui pelaksanaan arah organisasi BSSN, diharapkan akan membangkitkan dan mendorong seluruh entitas untuk bersinergi dalam mewujudkan tujuan sebagai institusi pemerintah yang memiliki daya kreativitas penuh inovatif, berpegang teguh pada prinsip efektivitas, efisiensi, dan akuntabel serta diimbangi dengan nilai moral dan budaya kerja yang tinggi.

2.2. MISI BSSN

Misi BSSN Tahun 2020–2024 disusun dalam rangka memperjelas aspek-aspek penting yang perlu difokuskan dalam pencapaian visi BSSN. Misi BSSN Tahun 2020–2024 sebagai berikut:

1. memberikan dukungan teknis dan administrasi serta analisis yang cepat, akurat, dan responsif kepada pemerintah, sebagai bahan pengambilan kebijakan penyelenggaraan pemerintahan negara dalam rangka mewujudkan kedaulatan siber Indonesia berkelas dunia.

Misi nomor 1 (satu) di atas memiliki makna bahwa BSSN memberikan dukungan kepada pemerintah untuk mewujudkan kedaulatan siber Indonesia berkelas dunia dalam upaya memajukan dan menyejahterakan bangsa melalui komponen teknologi, ekonomi, politik dan budaya di Indonesia.

2. menyelenggarakan keamanan siber dan persandian secara efektif dan efisien.

Misi nomor 2 (dua) memiliki makna bahwa BSSN menyelenggarakan keamanan siber secara efektif dan efisien dengan cara, menyusun dan menerapkan kebijakan keamanan siber dan persandian nasional yang berkualitas, membangun sistem dan operasional keamanan siber

dengan menggunakan standar-standar terkini yang meliputi identifikasi, deteksi, proteksi, mitigasi, manajemen krisis, penanggulangan, dan pemulihan terhadap ancaman, insiden, dan/atau serangan siber dan sandi melalui koordinasi dan kolaborasi dengan pemangku kepentingan dan menjalin kerjasama internasional, berperan aktif dalam meningkatkan kompetensi sumber daya manusia nasional di bidang keamanan siber dan sandi serta kompetensi pendukung yang diakui secara global, membangun kondisi yang aman di ruang siber, menjamin perangkat teknologi yang aman, membangun kesadaran pengguna terhadap keamanan siber serta mendorong pemanfaatan teknologi secara aman dan tidak melawan hukum untuk mewujudkan ekosistem siber yang aman dan nyaman.

3. meningkatkan kualitas sumber daya BSSN.

Misi nomor 3 (tiga) memiliki makna bahwa penyelenggaraan keamanan siber dan persandian nasional perlu didukung sumber daya yang berkualitas dengan cara, melakukan inovasi secara terus menerus untuk meningkatkan pertumbuhan birokrasi organisasi, dan mendorong serta mengembangkan teknologi secara mandiri untuk mendukung pengembangan industri dalam negeri di bidang teknologi keamanan siber dan sandi, menyediakan sumber daya manusia, proses bisnis, sarana dan prasarana secara profesional dan akuntabel.

2.3. TUJUAN BSSN

Dalam rangka mencapai visi dan misi, BSSN berupaya memetakan visi dan misi tersebut dalam tujuan yang selanjutnya menjadi dasar dalam penetapan strategi BSSN pada periode tahun 2020–2024. Tujuan BSSN tahun 2020–2024 sebagai berikut:

1. terwujudnya kedaulatan keamanan siber Indonesia.

Keamanan siber saat ini telah menjadi isu prioritas seluruh negara di dunia semenjak TIK dimanfaatkan dalam berbagai aspek kehidupan, baik dalam aspek sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dan lain sebagainya. Langkah konkret yang diperlukan Indonesia saat ini dalam mengantisipasi perkembangan siber di dunia yang sangat cepat yaitu melalui kolaborasi antar pemangku kepentingan untuk menyinergikan dua aspek penting ranah siber yaitu ketahanan siber dan keamanan siber. Kedua aspek selanjutnya menjadi dasar dalam

mewujudkan kedaulatan siber di Indonesia melalui proses peningkatan pertumbuhan kesadaran dan mengubah perilaku seluruh sektor dan masyarakat dalam meningkatkan ketahanan dan keamanan siber di Indonesia.

Pencapaian tujuan “Terwujudnya kedaulatan keamanan siber Indonesia” ditandai dengan disusunnya Peta Jalan 2019-2045 “Mewujudkan Kedaulatan Siber Indonesia Berkelas Dunia”, dimana periode pertama (2019-2025) merupakan fase stabilisasi. Fokus BSSN pada periode pertama peta jalan yaitu menjadi fondasi dan stabilisasi teknologi siber dan sandi nasional melalui strategi penguatan dasar-dasar agar BSSN berjalan secara stabil sebagai institusi negara di bidang siber. Tujuan Strategis ini memastikan bahwa melalui tugas dan fungsi yang dijalankan BSSN akan mengantarkannya menjadi institusi yang diakui dan menjadi referensi di tingkat internasional. Implementasi ukuran keberhasilan BSSN dalam mewujudkan tujuan strategis pada periode pertama peta jalan sesuai dokumen RPJMN 2020-2024 yaitu menjadi pemimpin dalam mencapai kegiatan prioritas penguatan ketahanan dan keamanan siber yang ditandai dengan meningkatnya skor GCI dari 0,792 (nol koma tujuh sembilan dua) pada tahun 2020 menjadi 0.838 (nol koma delapan tiga delapan) pada tahun 2024.

Pada era di mana implementasi teknologi seperti 5G, *massive computing*, *nano satellite*, *next gen-fiber optic*, dan lainnya yang saat ini sudah begitu masif menimbulkan berbagai ancaman yang berpotensi mengganggu kedaulatan negara. Tentunya hal ini menjadi tantangan bagi BSSN dalam merumuskan rencana aksi yang akan diimplementasikan pada periode Renstra 2020-2024. Lima aspek yang menjadi variabel pada perwujudan rencana aksi periode pertama meliputi teknologi, pengembangan kapasitas sumber daya manusia, organisasi, Kerjasama, dan regulasi.

2. terwujudnya tata kelola pemerintahan yang baik di BSSN.

Modal penting dalam keberhasilan suatu organisasi meliputi manusia, informasi, dan organisasi itu sendiri. Melalui Renstra BSSN, telah ditetapkan satu tujuan yang menggambarkan kekuatan organisasi berupa budaya kerja, dimana seluruh komponen fokus pada pencapaian arah dan tujuan strategis yang telah ditetapkan. Implementasi reformasi birokrasi merupakan salah satu langkah aksi

BSSN untuk mencapai pemerintahan yang baik dan melakukan pembaharuan serta perubahan mendasar terhadap sistem penyelenggaraan pemerintahan secara efektif, efisien, dan akuntabel. Upaya pencapaian tujuan “Terwujudnya Tata Kelola Pemerintahan yang baik di BSSN” melalui peningkatan kualitas reformasi birokrasi di BSSN telah dimulai sejak tahun 2010 hingga saat ini dan telah diperoleh peningkatan indeks reformasi birokrasi dan hasil evaluasi akuntabilitas kinerja instansi pemerintah serta meningkatnya kematangan sistem pengawasan internal pemerintah BSSN. Berdasarkan capaian prestasi tersebut, BSSN melalui nilai reformasi birokrasi, BSSN terus berusaha melakukan perbaikan secara berkesinambungan dengan salah satunya berfokus dalam penyiapan pelaksanaan audit keamanan SPBE dalam mendorong terwujudnya perlindungan aset informasi sehingga akan mengefisienkan birokrasi tata kelola pemerintahan dan meningkatkan kualitas pelayanan dan kepercayaan publik pada implementasi SPBE. Implementasi ukuran keberhasilan BSSN dalam mewujudkan tujuan strategis “Terwujudnya Tata Kelola Pemerintahan yang baik di BSSN” ditandai dengan meningkatnya indeks reformasi birokrasi BSSN dari 70,01 ((tujuh puluh koma nol satu) pada tahun 2020 menjadi 84,36 (delapan puluh empat koma tiga puluh enam) pada tahun 2024.

2.4. SASARAN STRATEGIS BSSN

Dalam rangka mendukung pencapaian 2 (dua) tujuan sebagaimana disebutkan diatas, BSSN telah menetapkan 3 (tiga) sasaran strategis yang merupakan kondisi yang ingin dicapai oleh BSSN dalam kurun waktu 2020-2024. Adapun Sasaran Strategis BSSN Tahun 2020-2024 sebagai berikut:

1. meningkatnya maturitas keamanan siber di Indonesia.

Isu keamanan siber menjadi hal penting yang menjadi tanggung jawab seluruh komponen bangsa. Serangan siber di Indonesia dari tahun ke tahun mengalami peningkatan yang cukup signifikan. Berkembangnya teknologi internet menjadi latar belakang dalam peningkatan serangan siber di berbagai sektor kehidupan masyarakat. Dihadapkan dengan kondisi di atas, setiap entitas pada semua sektor di Indonesia, diharapkan mampu mengembangkan kemampuan dalam melakukan identifikasi risiko keamanan siber dan

melindungi seluruh aset yang dimiliki dari adanya ancaman/insiden siber sehingga akan terbentuk kematangan entitas dalam hal penanganan insiden siber secara sistematis dan terstruktur.

Pada era infrastruktur digital saat ini membuat Indonesia semakin rawan terhadap serangan siber. Transformasi digital yang makin pesat berpotensi meningkatkan serangan siber di Indonesia. Pengembangan sistem keamanan digital dapat dimulai dari memperbarui teknologi keamanan siber untuk mengakomodasi ancaman siber baru pada semua lini kehidupan berbasis digital. Melalui konsep maturitas penanganan insiden siber secara mandiri oleh semua sektor baik pemerintah, IKN, dan ekonomi digital, akan membentuk sebuah ekosistem siber yang terintegrasi, efektif, dan solid di wilayah Indonesia.

2. terwujudnya penyelenggaraan keamanan siber dan sandi yang prima. Dengan merujuk pada penilaian GCI yang telah diakui dan menjadi salah satu rujukan bagi seluruh negara terkait komitmen dan usaha dalam menjaga dan meningkatkan keamanan siber, Indonesia membutuhkan sebuah strategi keamanan siber nasional dengan tujuan untuk membangun dan menerapkan tata kelola keamanan siber yang efektif, membangun kemandirian teknologi keamanan siber, mencegah dan mengelola ancaman, insiden serangan siber, meningkatkan budaya keamanan dalam ruang siber, serta mengoptimalkan sumber daya keamanan siber.

Keberhasilan dalam penyusunan dan implementasi strategi keamanan siber nasional tidak terlepas dari koordinasi dan kolaborasi seluruh pemangku kepentingan keamanan siber nasional. Melalui peran aktif seluruh komponen bangsa akan mewujudkan tatanan penyelenggaraan keamanan siber dan sandi yang prima di Indonesia.

3. terwujudnya birokrasi BSSN yang bersih, akuntabel, berkinerja tinggi, efektif, efisien dan berorientasi pada pelayanan publik.

Pembaharuan tatanan birokrasi di BSSN untuk meningkatkan kualitas pelayanan publik yang didukung oleh birokrasi yang bersih, akuntabel, berkinerja tinggi, efektif serta efisien dalam rangka menuju pemerintahan yang dinamis dimulai melalui penerapan budaya birokrasi dalam menerjemahkan permasalahan dan kendala yang ada pada periode sebelumnya menjadi representasi

pembelajaran bersama secara adaptif dalam mewujudkan kedaulatan siber Indonesia berkelas dunia.

Pemetaan tujuan ke dalam sasaran strategis serta indikator dari setiap sasaran strategis dijelaskan pada Tabel 2.1.

Tabel 2.1 Tujuan, Sasaran Strategis, dan Indikator Kinerja Sasaran Strategis BSSN

No	Tujuan	Sasaran Strategis		Indikator Kinerja	
1	Terwujudnya kedaulatan keamanan siber Indonesia Indikator: (skor GCI) 2020 : 0,792 2021 : 0,792 2022 : 0,826 2023 : 0,826 2024 : 0,838	1	Meningkatnya Maturitas Keamanan Siber di Indonesia	1.1	Tingkat Maturitas Objek Keamanan Siber
		2	Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima	2.1	Persentase pemenuhan layanan keamanan siber dan sandi yang prima.
2	Terwujudnya Tata Kelola Pemerintahan yang baik di BSSN Indikator:	3	Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi,	3.1	Indeks Reformasi Birokrasi

(Indeks RB) 2020 : 70,01 2021 : 73,35 2022 : 77,21 2023 : 80,77 2024 : 84,36		Efektif, Efisien dan Berorienta si pada Pelayanan Publik		
---	--	---	--	--

Keterkaitan antara sasaran pembangunan nasional bidang keamanan siber dengan tujuan dan sasaran strategis BSSN diilustrasikan pada Gambar 2.1.



Gambar 2.1 Keterkaitan Sasaran Pembangunan Nasional Bidang Keamanan Siber dengan Tujuan dan Sasaran Strategis BSSN

BAB III

ARAH KEBIJAKAN, STRATEGI, KERANGKA REGULASI, DAN KERANGKA
KELEMBAGAAN

3.1. ARAH KEBIJAKAN DAN STRATEGI NASIONAL

Berdasarkan Peraturan Presiden Nomor 18 Tahun 2020 tentang RPJMN Tahun 2020-2024, dalam rangka pencapaian tujuan serta sasaran pembangunan nasional, ditetapkan 7 (tujuh) agenda pembangunan RPJMN Tahun 2020-2024 sebagai berikut:

1. memperkuat ketahanan ekonomi untuk pertumbuhan yang berkualitas dan berkeadilan.
2. mengembangkan wilayah untuk mengurangi kesenjangan dan menjamin pemerataan.
3. meningkatkan sumber daya manusia yang berkualitas dan berdaya saing.
4. revolusi mental dan pembangunan kebudayaan.
5. memperkuat infrastruktur untuk mendukung pengembangan ekonomi dan pelayanan dasar.
6. membangun lingkungan hidup, meningkatkan ketahanan bencana dan perubahan iklim.
7. memperkuat stabilitas politik, hukum, pertahanan dan keamanan dan transformasi pelayanan publik.

3.1.1. Arah Kebijakan dan Strategi RPJMN Tahun 2020-2024 Bidang Keamanan Siber

Dalam agenda pembangunan penguatan stabilitas politik, hukum, pertahanan dan keamanan Tahun 2020-2024 diarahkan pada pemantapan stabilitas keamanan nasional untuk mewujudkan rasa aman dan damai bagi seluruh rakyat, serta keutuhan wilayah negara kesatuan republik Indonesia dan kedaulatan negara dari berbagai ancaman, baik dari dalam maupun luar negeri. Kondisi tersebut merupakan prasyarat untuk mendukung terlaksananya pembangunan nasional.

Arah kebijakan dan strategi nasional untuk mengatasi isu-isu strategis dalam menjaga stabilitas keamanan nasional di ruang siber adalah penguatan keamanan dan ketahanan siber yang diwujudkan dengan strategi berikut:

1. penguatan pengamanan infrastruktur siber.
2. pembangunan dan penguatan *computer emergency response team*.
3. pencegahan kejahatan siber dan peningkatan kerjasama internasional bidang siber.
4. penguatan kapasitas sumber daya manusia keamanan siber.
5. penyelesaian kejahatan siber *clearance rate* tindak pidana siber.

Arah kebijakan di atas diperkuat dengan adanya proyek prioritas strategis penguatan ketahanan dan keamanan siber. Proyek prioritas strategis ini dimaksudkan sebagai penajaman proyek-proyek prioritas yang dianggap memiliki nilai strategis dan daya ungkit dalam mencapai sasaran prioritas pembangunan nasional di bidang keamanan nasional. Selain itu, dalam RPJMN Tahun 2020-2024 BSSN juga terlibat dalam manajemen keamanan informasi SPBE.

3.1.2. Proyek Prioritas Strategis RPJMN Tahun 2020-2024 Bidang Politik, Hukum, Pertahanan dan Keamanan

Pada RPJMN Tahun 2020-2024, BSSN menjadi *leading sector* proyek prioritas strategis bidang politik, hukum, pertahanan dan keamanan yaitu penguatan NSOC-SOC dan Pembentukan 121 (seratus dua puluh satu) CSIRT yang melibatkan Kementerian/Lembaga dan Pemerintah Daerah. Sesuai RPJMN Tahun 2020-2024, pembentukan proyek prioritas strategis ini dilatarbelakangi oleh isu-isu di bidang keamanan siber sebagai berikut:

1. fenomena digitalisasi pada sektor jasa dan keuangan serta meningkatnya pengguna internet.
2. serangan siber terbanyak sepanjang tahun 2019 berupa percobaan pembocoran data yang disusul dengan serangan trojan.
3. sistem monitoring keamanan siber mata garuda belum mampu mencakup seluruh titik rentan di Indonesia.
4. Indonesia belum memiliki pusat informasi terpadu yang dapat dimanfaatkan oleh masyarakat sebagai sumber informasi dan aduan keamanan siber.
5. belum ada mekanisme integrasi dan berbagi data informasi serangan siber antar pemangku kepentingan terkait.

Melalui penguatan NSOC-SOC dan pembentukan 121 (seratus dua puluh satu) CSIRT diharapkan dapat memberikan manfaat sebagai berikut:

1. menurunnya insiden serangan siber.

2. meningkatnya kemampuan bersama *multistakeholder* keamanan siber dalam melakukan deteksi dini serangan atau ancaman siber.
3. meningkatnya pelayanan *multistakeholder* keamanan siber melalui pusat informasi terpadu bagi masyarakat.
4. meningkatnya integrasi dan sharing data informasi antar pemangku kepentingan baik pemerintah, swasta, dan komunitas siber lainnya.

Latar belakang, tujuan, dan manfaat, *highlight project*, dan kementerian/ lembaga yang terlibat diilustrasikan pada Gambar 3.1.



Gambar 3.1 Proyek Prioritas Strategis Penguatan NSOC-SOC dan Pembentukan 121 CSIRT

Sesuai matriks pembangunan jangka menengah RPJMN Tahun 2020-2024, Kegiatan prioritas nasional penguatan ketahanan dan keamanan siber dijabarkan ke dalam proyek-proyek prioritas nasional, dimana BSSN mengampu 4 (empat) proyek prioritas nasional dengan rincian proyek sebagai berikut:

1. Penguatan pengamanan infrastruktur siber
 - a. perluasan cakupan area *national cybersecurity operation center*.
 - b. pembangunan kapasitas *national computer security incident response team*.
 - c. pembangunan sistem monitoring pengendalian informasi.
 - d. penguatan national data center.

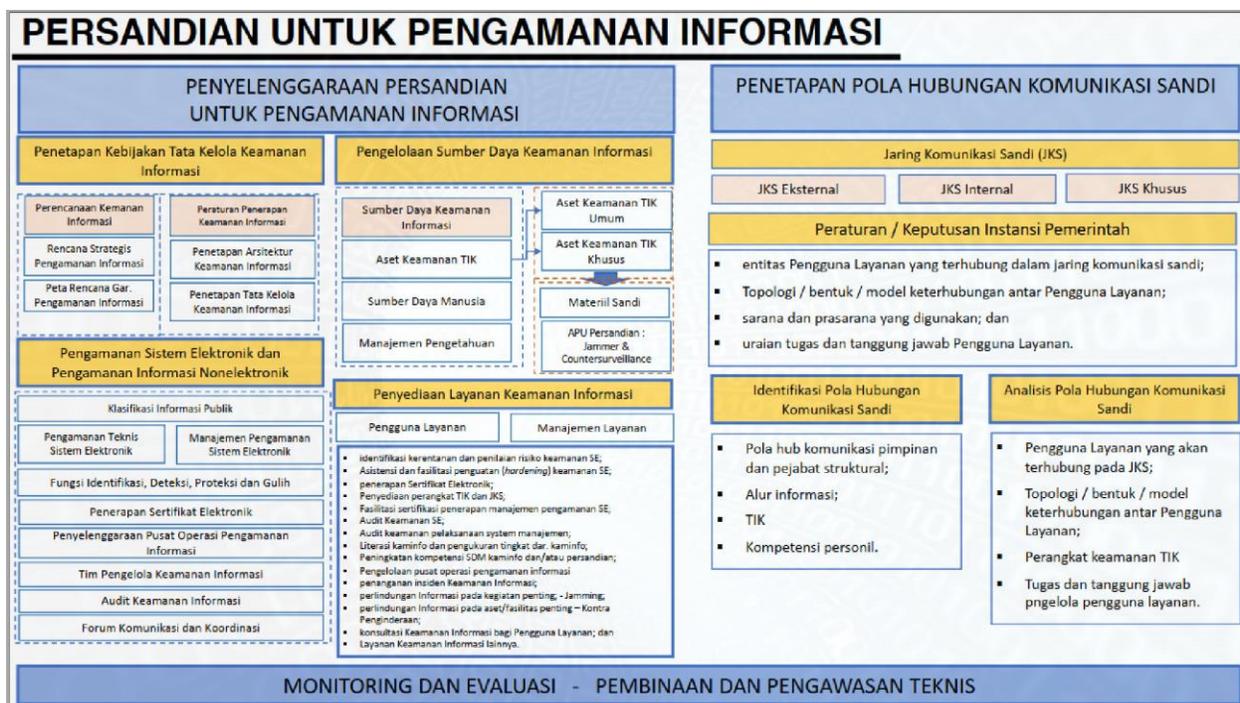
- e. pembangunan infrastruktur *voluntary vulnerability disclosure program*.
- f. pembangunan *information sharing and analysis center*.
2. Pembangunan dan penguatan *computer emergency response team*
 - a. pembentukan CSIRT pada sektor pemerintah.
 - b. pembentukan tim respon ancaman intelijen siber.
3. Pencegahan kejahatan siber dan peningkatan kerjasama internasional bidang siber, kerjasama regional, bilateral dan multilateral bidang keamanan siber.
4. penguatan kapasitas sumber daya manusia keamanan siber
 - a. peningkatan kompetensi sumber daya manusia pengelola keamanan SPBE pada K/L/D.
 - b. pengembangan sumber daya manusia di bidang keamanan siber.
 - c. penyelenggaraan program *born to defence* untuk sumber daya manusia pengelola keamanan siber sektor IKN.
 - d. *national cyber exercise drill test* jumlah peserta yang mengikuti *national cyber excercise drill test*.
 - e. peningkatan kualitas dan kuantitas sumber daya manusia bidang digital forensic.

Proyek prioritas strategis dan indikasi pendanaannya dapat dimutakhirkan melalui RKP dengan mempertimbangkan kesiapan pelaksanaan, pemutakhiran besaran dan sumber pendanaan serta direktif Presiden. Hal ini bertujuan agar proyek prioritas strategis dapat terlaksana secara lebih efektif dan efisien sesuai dengan perkembangan pembangunan.

Dengan ditetapkannya BSSN sebagai *leading sector* proyek prioritas strategis di atas, BSSN dituntut untuk dapat menjalin kolaborasi dengan semua pemangku kepentingan dalam membangun sistem dan tata kelola pelaksanaan penguatan keamanan siber yang terintegrasi. Fungsi BSSN yaitu menjadi pusat yang mengoordinasikan dan memberdayakan seluruh instansi yang berhubungan dengan ranah siber agar tidak terjadi tumpang tindih kewenangan di Indonesia. Pembangunan infrastruktur dan sistem keamanan siber dan sandi nasional merupakan salah satu bentuk inisiatif BSSN dalam membagi kewenangan antar instansi dan untuk mewujudkan tujuan dengan langkah nyata berupa membangun platform *information sharing and*

analysis center pada sektor pemerintah, IIKN, dan ekonomi digital. Tujuan pembangunan tersebut untuk menyediakan platform koordinasi terhadap ancaman dan serangan terkini yang terjadi pada ruang siber. *Information sharing and analysis center* berperan untuk membangun dan meningkatkan *shared situational awareness* terhadap kerawanan, kejadian, insiden, dan ancaman yang terjadi dan menjadi media kolaborasi menuju ketahanan siber nasional di Indonesia.

Selain Kementerian/Lembaga terkait, keterlibatan daerah juga perlu didorong dalam upaya mewujudkan keamanan siber nasional. Dengan berlakunya Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, menjadikan persandian sebagai urusan pemerintahan konkuren yang bertujuan menyelenggarakan pengamanan informasi dan mewujudkan tata kelola secara terpadu dalam proses manajemen SPBE yang efektif, efisien, berkesinambungan, dan berkualitas. BSSN telah menyusun peraturan pelaksanaan urusan pemerintahan bidang persandian di daerah melalui Peraturan BSSN Nomor 10 Tahun 2019. Peraturan dimaksud memuat norma, standar, prosedur, dan kriteria pelaksanaan urusan persandian yang secara ringkas diilustrasikan dalam Gambar 3.2.



Gambar 3.2 Persandian untuk Pengamanan Informasi Pada Pemerintah Daerah

Berdasarkan Peraturan BSSN Nomor 10 Tahun 2019, penyelenggaraan persandian untuk pengamanan informasi dilaksanakan melalui 4 (empat) aspek yaitu :

1. penetapan kebijakan tata kelola keamanan informasi.
2. pengelolaan sumber data keamanan informasi.
3. pengamanan sistem elektronik dan pengamanan informasi non elektronik.
4. penyediaan layanan keamanan informasi.

Fungsi fungsi dalam tata kelola keamanan siber khususnya penanggulangan dan pemulihan pada pemerintah daerah merupakan salah satu kegiatan dalam aspek pengamanan sistem elektronik dan pengamanan informasi non elektronik. Sejalan dengan proyek prioritas strategis penguatan NSOC-SOC dan pembentukan 121 (seratus dua puluh satu) CSIRT, maka di akhir periode Renstra, BSSN menargetkan terbentuknya CSIRT pada seluruh Pemerintah Provinsi untuk meningkatkan kesiapan daerah dalam penanggulangan dan pemulihan insiden siber.

Persandian tidak hanya memberikan jaminan pada keamanan informasi berklasifikasi, namun jaminan terhadap 4 (empat) aspek pengamanan yang meliputi keotentikan, keutuhan, ketersediaan, dan nir penyangkalan. Persandian di lingkungan pemerintah daerah harus berperan dalam mendukung penyelenggaraan *e-government* atau penyelenggaraan pemerintahan berbasis elektronik, dan penyelenggaraan sistem dan transaksi elektronik sesuai peraturan perundang-undangan lainnya.

Berdasarkan hal tersebut, pada faktanya belum seluruh fungsi Persandian pada Pemerintah Provinsi diselenggarakan dengan optimal. Hal ini ditunjukkan dengan beberapa uraian tugas yang belum dilaksanakan, diantaranya belum berfungsinya pengamanan sistem elektronik pada pemerintah provinsi yang tidak diiringi dengan implementasi teknis pengamanannya yang berupa tanda tangan elektronik tersertifikasi. Hal ini menjadi celah kerawanan keamanan karena konten dokumen elektronik dapat dengan mudah dirubah dan penerima tidak dapat melakukan verifikasi terhadap keaslian dokumen.

Berdasarkan data dari BSSN melalui Balai Sertifikasi Elektronik (BSrE), Kementerian/Lembaga/Daerah (K/L/D) yang telah menjalin kerjasama dengan BSSN melalui layanan sertifikat elektronik adalah

sebanyak 258 (dua ratus lima puluh delapan) instansi atau sebesar 27,69% (dua puluh tujuh koma enam sembilan per seratus). Hal ini menunjukkan bahwa masih terdapat 72,31% (tujuh puluh dua koma tiga satu per seratus) pengguna yang perlu mendapat perhatian baik melalui pembinaan maupun sosialisasi. Data K/L/D yang telah dan belum menjalin perjanjian kerjasama dengan BSSN terkait layanan sertifikat elektronik ditunjukkan pada Gambar 3.3.



Gambar 3.3 Data Implementasi Sertifikat Elektronik pada K/L/D

3.1.3. Manajemen Keamanan dalam Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik

Sebagaimana amanat dalam Peraturan Presiden Nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, BSSN diberikan mandat untuk mendukung terwujudnya penyelenggaraan SPBE dengan melaksanakan pengamanan SPBE, menyusun standar keamanan SPBE nasional, dan menetapkan manajemen dan melaksanakan audit keamanan SPBE. Hal ini diantaranya dimaksudkan untuk dapat meningkatkan keterpaduan pelaksanaan tata kelola SPBE, manajemen SPBE, dan audit teknologi informasi dan komunikasi, serta pemantauan dan evaluasi SPBE nasional. Dengan diterapkannya prinsip-prinsip keamanan dalam implementasi SPBE maka akan meningkatkan partisipasi sektor pemerintah baik di tingkat pusat maupun daerah dalam menjalankan tata kelola keamanan siber sehingga akan

berkontribusi pada peningkatan keamanan siber Indonesia di sektor pemerintah.

3.1.4. Pengarusutamaan Gender

Kebijakan PUG BSSN pada periode 2020-2024 dilaksanakan dengan melanjutkan program-program yang telah dilakukan secara konsisten pada periode sebelumnya yaitu PUG pada bidang kesehatan, pendidikan, dan keterwakilan dalam jabatan. Selain kebijakan dan program tersebut, untuk mengatasi isu keterwakilan wanita dalam bidang pekerjaan keamanan siber, BSSN juga menginisiasi penyelenggaraan *women in cybersecurity* untuk menumbuhkan ekosistem dimana wanita dan laki-laki memiliki profesionalitas yang sama dalam bidang keamanan siber.

1. Bidang kesehatan

Kebijakan yang telah dan tetap akan dilaksanakan pada periode 2020-2024 diantaranya pemberian cuti melahirkan sebagaimana diatur dalam Peraturan BSSN Nomor 3 Tahun 2020 dan kesetaraan dalam jaminan kesehatan melalui akses fasilitas kesehatan.

2. Bidang pendidikan

Kebijakan diarahkan untuk memastikan kesetaraan dalam kesempatan memperoleh pendidikan diantaranya pengembangan kompetensi melalui pendidikan, pelatihan, maupun tugas belajar/beasiswa untuk mendukung pelaksanaan tugas fungsi dan kesetaraan gender dalam proporsi penerimaan mahasiswa politeknik siber dan sandi negara dan pegawai BSSN.

3. Keterwakilan dalam jabatan

Kebijakan diarahkan untuk memastikan kesetaraan dalam kesempatan pengisian jabatan strategis melalui program lelang jabatan pimpinan tinggi pratama, serta berbagai penugasan atau penyelenggaraan kegiatan sesuai tugas dan fungsi.

4. *Women in cybersecurity summit*

Dalam upaya percepatan pelaksanaan pengarusutamaan gender, BSSN sesuai tugas dan fungsi dalam ranah siber, menggagas *women in cybersecurity summit* dalam rangka memberikan kesempatan perempuan untuk pertukaran informasi, penciptaan pengetahuan dan berbagi praktik terbaik, sambil mengidentifikasi tren yang

muncul dan membina kemitraan, dengan mempertimbangkan masyarakat informasi dan pengetahuan yang terus berkembang. Kegiatan ini akan membentuk ekosistem baru dimana perempuan mempunyai kesempatan yang sama dengan lelaki dalam hal pengetahuan maupun kemampuan dalam dunia *cybersecurity*. Beberapa sektor yang telah bergabung dalam embrio ekosistem ini yaitu sektor telekomunikasi, perbankan, perguruan tinggi atau akademisi, Kementerian dan Lembaga, dan akan bertambah lagi seiring dengan pergerakan dari komunitas yang sudah eksisting saat ini.

3.2. ARAH KEBIJAKAN DAN STRATEGI BSSN

Perkuatan stabilitas politik, hukum, pertahanan dan keamanan dan transformasi pelayanan publik merupakan agenda ketujuh yang mengedepankan bahwa negara wajib hadir dalam melayani dan melindungi segenap bangsa, serta menegakkan kedaulatan yang salah satunya diwujudkan melalui perbaikan tata kelola keamanan siber. Dalam rangka mendukung arah kebijakan RPJMN tersebut maka pembangunan di bidang keamanan siber diarahkan kepada terwujudnya kedaulatan siber Indonesia berkelas dunia. Untuk itu, dalam periode 2020-2024 BSSN telah menetapkan tema atau fokus pembangunan per tahunnya sesuai *roadmap* kedaulatan siber Indonesia berkelas dunia sebagaimana Gambar 3.4.



Gambar 3.4 Fokus Pembangunan BSSN Periode 2020-2024

Fokus pembangunan di atas menjadi pedoman bagi BSSN dalam menyusun kegiatan-kegiatan prioritas setiap tahunnya. Fokus pembangunan dapat dimutakhirkan dengan mempertimbangkan

perkembangan lingkungan strategis keamanan siber, arah kebijakan pembangunan nasional, direktif Presiden, perubahan kewenangan BSSN dan kesiapan pelaksanaan.

Arah Kebijakan dan Strategi BSSN Tahun 2020-2024 dalam rangka mendukung pencapaian tujuan BSSN sebagai berikut:

1. Arah kebijakan dalam mencapai tujuan terwujudnya kedaulatan keamanan siber Indonesia sebagai berikut:
 - a. meningkatkan agilitas operasional dalam rangka menghadapi perubahan yang dinamis.
 - b. menjaga stabilitas operasional BSSN.
2. Arah kebijakan dalam mencapai tujuan terwujudnya tata kelola pemerintahan yang baik dan berkualitas di BSSN melalui kebijakan tata kelola pemerintahan yang baik.

3.2.2. Peningkatan agilitas operasional dalam rangka menghadapi perubahan yang dinamis

Arah kebijakan ini bertujuan untuk membangun semangat bersinergi dan mengoptimalkan kolaborasi dengan lembaga-lembaga terkait, baik dari pemerintah ataupun swasta. Selain itu, arah kebijakan ini ditujukan untuk terus mengembangkan sumber daya manusia yang kompeten dalam bidang keamanan siber dan sandi nasional. Kehadiran sumber daya manusia yang kompeten, baik dari sisi kualitas dan kuantitas, sangat diperlukan untuk mendukung keberhasilan pelaksanaan tugas BSSN dalam menjaga keamanan siber dan sandi nasional. Kebijakan ini dilaksanakan dengan strategi sebagai berikut:

1. menyusun regulasi keamanan siber dan sandi, termasuk di dalamnya penyusunan rencana induk keamanan siber dan sandi nasional.
2. membangun dan mengembangkan ekosistem keamanan siber dan literasi publik.
3. membangun dan mengimplementasikan desain arsitektur *cyber awareness*.
4. meningkatkan kemandirian dalam pengembangan dan utilisasi teknologi keamanan siber dan sandi.
5. mengintegrasikan penelitian dan pengembangan bidang keamanan siber dan sandi.
6. mengoptimalkan kolaborasi antar organisasi di kalangan pemerintah maupun swasta, baik di dalam maupun luar negeri.

7. memastikan ketersediaan sumber daya manusia keamanan siber dan sandi yang profesional dan berintegritas.

3.2.2. Menjaga stabilitas operasional BSSN

Arah kebijakan ini bertujuan untuk menguatkan peran BSSN dalam memelihara keamanan siber dan sandi nasional dengan mengadakan dan mengembangkan sarana, prasarana dan teknologi yang diperlukan untuk meningkatkan keamanan siber dan sandi nasional. Di masa mendatang tantangan yang akan dihadapi BSSN akan sangat kompleks, dan membutuhkan kesiapan sarana dan prasarana serta dukungan teknologi yang memadai seiring dengan pesatnya perubahan teknologi siber dan sandi. Kebijakan ini dilaksanakan dengan strategi sebagai berikut:

1. memastikan penjaminan keamanan siber dan sandi nasional dalam level tertinggi.
2. memperkuat integrasi manajemen siber meliputi *identify, protect, detect, respond, dan recover*.
3. meningkatkan reputasi layanan keamanan siber dan sandi BSSN.

Berdasarkan agenda pembangunan nasional yang terdapat di didalam RPJMN 2020-2024, dan merujuk pada *roadmap* kedaulatan siber kelas dunia dimana pada periode 2019-2025 BSSN berada dalam periode penguatan fondasi dan stabilisasi. Pada periode ini dasar-dasar untuk berjalannya BSSN dengan stabil sebagai institusi negara di bidang siber dan sandi diletakkan. Untuk mendukung terwujudnya tujuan periode ini, BSSN telah menetapkan inisiatif strategi utama yang merupakan langkah inisiatif yang cepat, dalam mendukung arah pembangunan nasional sebagai berikut:

1. Pengembangan *National Security Operation Center (NSOC)* merupakan upaya BSSN membangun sistem proteksi dan *shared situational awareness* mengenai kondisi keamanan siber di Indonesia.
2. Perkuatan bidang penelitian dan pengembangan merupakan upaya BSSN dalam mewujudkan kemandirian dan kedaulatan teknologi siber dan sandi.
3. Pembangunan kapabilitas dan kapasitas sumber daya manusia siber dan sandi. Penyiapan sumber daya manusia untuk mengawaki pengembangan NSOC dan perkuatan bidang penelitian dan pengembangan.

3.2.2 Kebijakan Tata Kelola Pemerintahan Yang Baik

Penguatan fondasi organisasi dan optimalisasi reformasi birokrasi BSSN sangat diperlukan untuk mendukung pelaksanaan tugas BSSN, sebab dalam pelaksanaan tugasnya BSSN akan banyak berhadapan dengan lingkungan eksternal, selain itu diharapkan dapat terwujudnya pembagian kewenangan yang jelas dengan lembaga pemerintahan lain yang terkait dengan pelaksanaan tugas BSSN. Kebijakan ini dilaksanakan dengan strategi sebagai berikut:

- a. memastikan pemenuhan sumber daya manusia yang kompeten.
- b. menumbuhkan organisasi yang profesional dan handal melalui optimalisasi reformasi birokrasi BSSN.
- c. meningkatkan kualitas pengawasan internal.
- d. membangun budaya kerja yang baik dengan menerapkan sistem nilai PINTAR.
- e. meningkatkan efektivitas sinkronisasi kebijakan keamanan siber dan sandi.
- f. menumbuhkan hasil penelitian dan pengembangan yang implementatif.
- g. mengembangkan TIK untuk memperkuat kapabilitas strategis organisasi.

Berdasarkan uraian di atas, arah kebijakan dan strategi BSSN selama periode 2020-2024 diilustrasikan pada Gambar 3.5.



Gambar 3.5 Arah Kebijakan dan Strategi BSSN 2020-2024

3.3. KERANGKA REGULASI

Sebagaimana tertuang di dalam Peraturan Menteri PPN Nomor 5 Tahun 2019, penyusunan kerangka regulasi pada periode RPJMN Tahun 2020-2024 diarahkan untuk memfasilitasi, mendorong, dan/atau mengatur perilaku masyarakat, termasuk swasta dan penyelenggara negara dalam rangka mewujudkan tujuan bernegara sebagaimana tercantum pada UUD Tahun 1945. Dalam rangka mendukung strategi pembangunan di bidang keamanan siber dan sandi untuk mengatasi isu strategis keamanan siber, BSSN mendorong dan mendukung penyusunan kerangka regulasi sebagaimana tercantum pada Tabel 3.1.

Tabel 3.1 Kerangka Regulasi BSSN Tahun 2020-2024

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
Peraturan BSSN terkait Strategi Keamanan Siber Nasional	Melalui Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN) dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 membentuk BSSN menyusun Strategi Keamanan Siber Indonesia sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional dalam menyusun dan mengembangkan kebijakan keamanan siber di instansi masing-masing. Strategi keamanan siber nasional disusun selaras dengan nilai dasar kehidupan berbangsa dan bernegara, yaitu: Kedaulatan, Kemandirian, Keamanan, Kebersamaan, dan Adaptif.	Direktorat Proteksi Pemerintah		2020
Peraturan tentang Matriks Keamanan Siber	Tindak lanjut Agenda Pembangunan RPJMN IV Tahun 2020 - 2024 yaitu Memperkuat Stabilitas Polhukhankam dan	Direktorat Identifikasi Kerentanan dan Penilaian dan Penilaian Risiko		2021

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
Indonesia	Transformasi Pelayanan Publik yaitu Memperbaiki sistem peradilan, penataan regulasi dan tata kelola.	Ekonomi Digital		
Peraturan tentang Manajemen Krisis Keamanan Siber Nasional	Merupakan tindak lanjut Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 yang mengamanatkan BSSN menjadi pusat manajemen krisis siber sehingga perlu diatur organisasi dan tatakelola manajemen krisis siber di Indonesia.	Direktorat Penanggulangan dan Pemulihan Ekonomi Digital		2021
Peraturan BSSN terkait Tata Kelola Penanggulangan dan Pemulihan Insiden Siber Nasional	Tindak lanjut Finalisasi Penyusunan Kebijakan Tata Kelola Penanggulangan dan Pemulihan Insiden Keamanan Siber Nasional oleh oleh Deputi Bidang Penanggulangan dan Pemulihan BSSN menghasilkan kebijakan yang berskala nasional, komprehensif, dan implementatif, sehingga dapat menjadi acuan BSSN dan pemangku kepentingan dalam melakukan penanggulangan dan pemulihan insiden keamanan siber	Direktorat Penanggulangan dan Pemulihan Pemerintah	1. Direktorat Penanggula ngen dan Pemulihan Infrastrukt ur Informasi Kritisal Nasional; 2. Direktorat Penanggula ngen dan Pemulihan Ekonomi Digital; 3. Pusat Operasi Keamanan Siber Nasional.	2020
Peraturan BSSN terkait Rencana Strategis Keamanan Siber Sektor IIKN	Tindak Lanjut Sasaran Strategis 2: Terselenggaranya Pendayagunaan Kapabilitas Identifikasi dan Deteksi yang Andal pada Rencana Strategis BSSN 2018- 2019	Direktorat Proteksi Sektor Infrastruktur Informasi Kritisal Nasional	1. Direktorat Identifikasi dan Kerentanan Penilaian Risiko Infrastruktur Informasi	2021

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
			Kritikal Nasional 2. Direktorat Penanggulangan dan Pemulihan Infrastruktur Informasi Kritikal Nasional	
Peraturan BSSN terkait Standar Audit Keamanan Siber Pemerintah	Tindak Lanjut Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE dimana Audit Teknologi Informasi dan Komunikasi merupakan proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.	Direktorat Proteksi Sektor Pemerintah		2021
Peraturan BSSN tentang Pembinaan Sumber Daya Manusia Bidang Keamanan Siber	Pembangunan sumber daya manusia berkualitas menjadi prioritas utama Pemerintah Republik Indonesia dalam mewujudkan visi dan misi Pemerintah menuju "Sumber Daya Manusia Unggul Indonesia Maju". Pembangunan tersebut dapat terwujud melalui peningkatan daya saing dan pemerataan kualitas sumber daya manusia. Seiring dengan perkembangan TIK di era Revolusi Industri 4.0., ancaman dan tantangan	Direktorat Pengendalian Sumber Daya Manusia		2021

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
	<p>semakin nyata, sehingga perlu dipersiapkan pendekatan dan strategi yang tepat untuk menjembatani antara kualitas lulusan pendidikan dengan kebutuhan sumber daya manusia di dunia kerja, sehingga tercipta link and match diantara keduanya.</p> <p>Menyadari pentingnya isu strategis di atas, perlu dikembangkan berbagai macam metode untuk menyiapkan sumber daya manusia di bidang keamanan siber, sehingga dapat menjawab kebutuhan akan sumber daya manusia keamanan siber yang berdaya saing dan profesional. Untuk itulah BSSN perlu menyusun peraturan tentang peta jalan pembinaan sumber daya manusia di bidang keamanan siber dan sandi periode tahun 2020-2024.</p>			
Peraturan tentang Jabatan Fungsional Sumber Daya Manusia Bidang Keamanan Siber dan Sandi	Menindaklanjuti Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara dan peraturan perubahannya Peraturan Presiden Nomor 133 Tahun 2017 yang mengamanatkan penyusunan kebijakan, koordinasi, dan pelaksanaan, pengendalian serta evaluasi terhadap sumber daya keamanan siber dan persandian termasuk sumber daya manusia	Direktorat Pengendalian Sumber Daya Manusia	1. Biro Organisasi dan Sumber Daya Manusia; 2. Biro Hukum dan Hubungan Masyarakat.	2022

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
	bidang keamanan siber dan sandi, dan Permenpan RB Nomor 13 Tahun 2019 yang mengamanahkan BSSN menjadi instansi pembina Jabatan Fungsional yang memiliki kewajiban-kewajiban yang melekat, yang secara hirarki Permenpan tersebut menelurkan permenpan Nomor 18 Tahun 2019 tentang Jabatan Fungsional Sandiman dan Permenpan Nomor 6 Tahun 2020 tentang Jabatan Fungsional Manggala Informatika. Berdasarkan hal tersebut maka perlu ada peraturan BSSN yang mengatur tentang Jabatan Fungsional yang dibinanya.			
Peraturan BSSN terkait Monitoring Keamanan Siber Nasional	Peraturan BSSN tentang Pemantauan Keamanan Siber Nasional merupakan turunan dari Peraturan Pemerintah Nomor 52 Tahun 2000 tentang penyelenggaraan telekomunikasi yang mengamanatkan pemasangan perangkat deteksi dini, perangkat pemantau, dan perangkat pencegah terjadinya gangguan penyelenggaraan telekomunikasi sehingga diperlukan regulasi tentang Monitoring Keamanan Siber Nasional.	Pusat Operasi Keamanan Siber Nasional		2022
Peraturan BSSN terkait Keamanan	Tindak lanjut Peraturan Presiden Nomor 53 Tahun 2017 dan Perubahan	Direktorat Pengendalian Informasi,		2020

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
Informasi pada Literasi Keamanan Siber dan Pengendalian Informasi.	Peraturan Presiden Nomor 133 Tahun 2017 tentang Badan Siber dan Sandi Negara	Investigasi, Dan Forensik Digital		
Peraturan BSSN terkait Penyelenggaraan Sertifikat Elektronik	Peraturan Kepala Badan Siber dan Sandi Negara tentang Penyelenggaraan Sertifikat Elektronik merupakan revisi atas Peraturan Kepala Lemsaneg Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik. Peraturan tersebut sebagai turunan dari peraturan di atasnya (UU ITE, PP PSTE, Perpres SPBE). Sehubungan dengan hal tersebut perlu pengaturan tentang tata kelola penyelenggaraan sertifikat elektronik dalam rangka dukungan keamanan informasi dalam pelaksanaan <i>e-government</i> .	Balai Sertifikasi Elektronik (BSrE)		2021
Peraturan BSSN terkait <i>Voluntary Vulnerability Disclosure Program</i> (VVDP)	Tindak lanjut dasar hukum dan panduan penyelenggaraan Program serta untuk memberikan kepastian hukum kepada pencari kerentanan yang berpartisipasi di dalam Program dalam rangka finalisasi Rancangan Peraturan BSSN tentang Penyelenggaraan Program VVDP.	Direktorat Proteksi Infrastruktur Informasi Kritis Nasional		2021
Penyusunan peraturan CSIRT Sektoral (CII SIRT)	Tindak lanjut Naskah Akademik tentang Keamanan dan Ketahanan Siber dalam mengoordinasikan kejadian yang berkaitan dengan keamanan siber.	Direktorat Penanggulangan dan Pemulihan Infrastruktur Informasi Kritis Nasional		2022

Arah Kerangka regulasi/ kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
	CERT berfungsi untuk memonitor ancaman yang berimbas pada sistem komputer, berkolaborasi secara internasional dalam merespon ancaman keamanan siber, menelusuri insiden keamanan siber yang berdampak baik pada sektor publik dan privat.			
Peraturan BSSN terkait manajemen keamanan SPBE	Tindak lanjut dari Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE dimana BSSN menjadi <i>leading sector</i> dalam menangani masalah manajemen keamanan Sistem Pemerintahan Berbasis Elektronik.	Direktorat Proteksi Pemerintah	1. Direktorat Identifikasi dan Kerentanan Penilaian Risiko Pemerintah; 2. Direktorat Penanggulangan dan Pemulihan Pemerintah	2020

3.4. KERANGKA KELEMBAGAAN

Perubahan lingkungan strategis yang begitu cepat, ancaman siber yang makin masif dan canggih serta arah kebijakan pemerintah yang berubah menuntut BSSN sebagai perangkat pemerintah perlu menyesuaikan dengan situasi dan tuntutan perubahan. Selang berjalan 2 (dua) tahun sejak pembentukan BSSN sesuai dengan Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, BSSN telah melakukan evaluasi organisasi sebagai upaya terwujudnya organisasi BSSN yang berfokus pada strategi dan berkinerja tinggi dalam rangka mencapai tujuan dan sasaran BSSN.

Penyempurnaan organisasi Badan Siber dan Sandi Negara berpedoman pada prinsip “*structure follow process follow strategy*” yang artinya strategi menjadi acuan dilakukannya penataan proses bisnis dan penyesuaian struktur organisasi. Struktur organisasi BSSN kedepan harus dapat menjamin terjadinya penyelarasan proses bisnis lintas unit

kerja dalam suatu arsitektur proses bisnis yang tuntas. Sehingga tercipta mekanisme kerja lintas unit kerja yang optimal dalam pelaksanaan tugas pokok melalui pengurangan duplikasi dan tumpang tindih antar fungsi serta terciptanya *teamwork* dan koordinasi yang semakin baik dengan menghilangkan silo antar unit kerja atau satuan kerja.

3.4.1. Evaluasi Organisasi dan Kebutuhan Penyempurnaan Organisasi BSSN

Proses penyempurnaan organisasi BSSN dilakukan berdasarkan beberapa tahapan sebagai berikut:

1. Evaluasi organisasi melalui survey atau pendistribusian kuesioner dan *Focus Group Discussion* di lingkup internal BSSN.
2. *Focus Group Discussion* dengan pemangku kepentingan BSSN dari sektor pemerintah, sektor infrastruktur informasi kritikal nasional, dan sektor ekonomi digital.
3. Kajian kesesuaian dan penyelarasan pada Visi Misi Presiden 2019-2024, amanat Presiden kepada Kepala BSSN, sasaran pembangunan nasional dalam RPJMN Tahun 2020-2024, tujuan dan sasaran strategis BSSN, serta amanat peraturan dan ketentuan perundang-undangan terkait yang mempengaruhi pelaksanaan tugas dan fungsi BSSN serta mempertimbangkan proses bisnis BSSN.

Berdasarkan tahapan di atas, dapat disimpulkan kebutuhan penyempurnaan organisasi BSSN sebagai berikut:

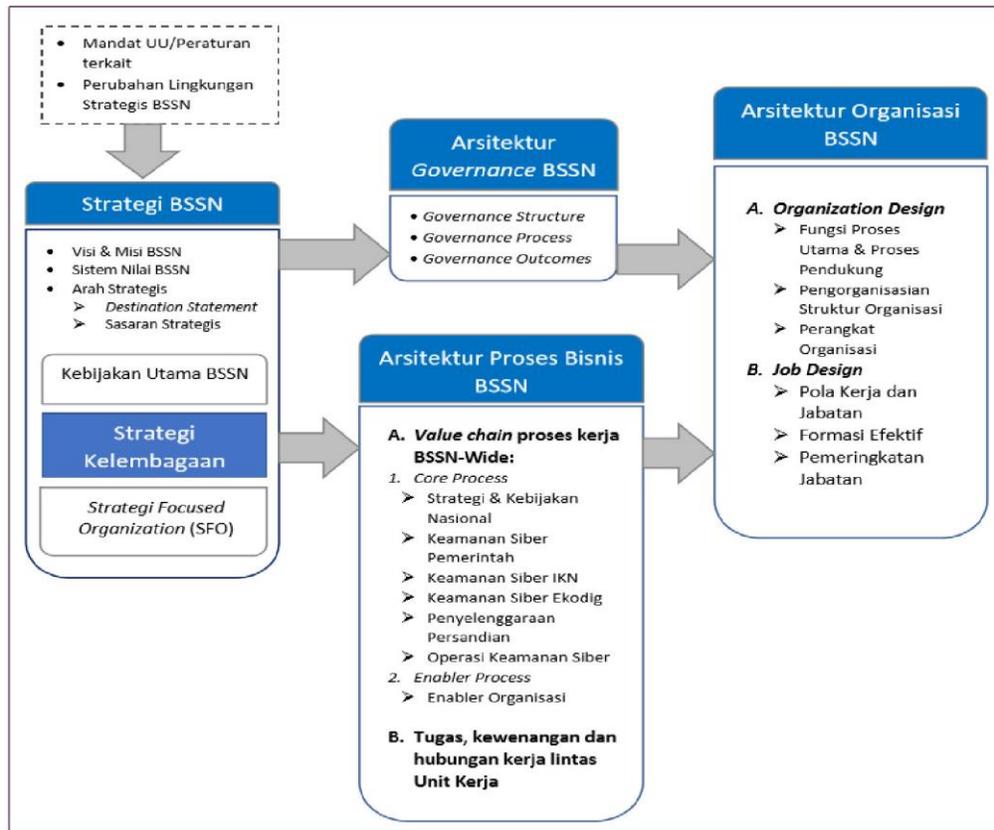
1. Struktur organisasi BSSN sesuai Peraturan Presiden Nomor 53 Tahun 2017 dimana unit Eselon I dikelompokkan berdasarkan fungsi yaitu identifikasi dan deteksi, proteksi, dan penanggulangan pemulihan, sementara di tingkat Eselon II dikelompokkan berdasarkan sektor yaitu pemerintah, IKN, dan ekonomi digital berdampak pada kurang efektifnya pola koordinasi dan kolaborasi dalam proses kerja karena harus melalui lintas kedeputan sehingga prosesnya panjang. Dampak lainnya yaitu sulit membentuk maturitas keamanan siber secara penuh pada setiap pemangku kepentingan karena setiap Deputi hanya bertanggungjawab pada satu fungsi saja. Selain itu diidentifikasi masih terdapat tumpang tindih dan duplikasi fungsi. Berdasarkan hal tersebut, BSSN perlu memetakan kembali fungsi yang saling terkait, yaitu dengan

mengelompokkan unit Eselon I yang semula berbasis fungsi ke berbasis sektor yaitu pemerintah, IKN, dan ekonomi digital

2. BSSN perlu membentuk unit kerja khusus yang berfokus dan melaksanakan tugas dan fungsi terkait strategi dan kebijakan nasional bidang keamanan siber. Dengan dibentuknya unit kerja tersebut diharapkan dapat menyiapkan strategi keamanan siber nasional yang dapat mengarahkan dan mendorong bertambahnya legislasi terkait keamanan siber nasional.
3. BSSN perlu membentuk dan mendefinisikan secara tertulis unit kerja yang mampu tugas dan fungsi yang bertanggungjawab pada terbentuknya CERT/CIRT/CSIRT, serta CERT National, CERT Sektoral dan Gov-CERT/Gov-CSIRT.
4. BSSN perlu melakukan penguatan dan penajaman fungsi terkait kerjasama yang meliputi kerja sama publik privat dan kerja sama internasional. Dari sisi strategi perumusan kerja sama akan dilakukan oleh unit kerja yang membidangi strategi, dari sisi koordinasi dan administrasi akan dilaksanakan oleh Sekretariat Utama yang membidangi bidang administrasi kerja sama dan hubungan antar Lembaga.
5. BSSN perlu melakukan penajaman fungsi dan penulisan peran dan tanggung jawab tugas terkait *child online protection* pada unit kerja tertentu di BSSN.
6. BSSN perlu melakukan penajaman fungsi dan penulisan peran dan tanggung jawab terkait kurikulum siber pada unit kerja yang membidangi sumber daya manusia.

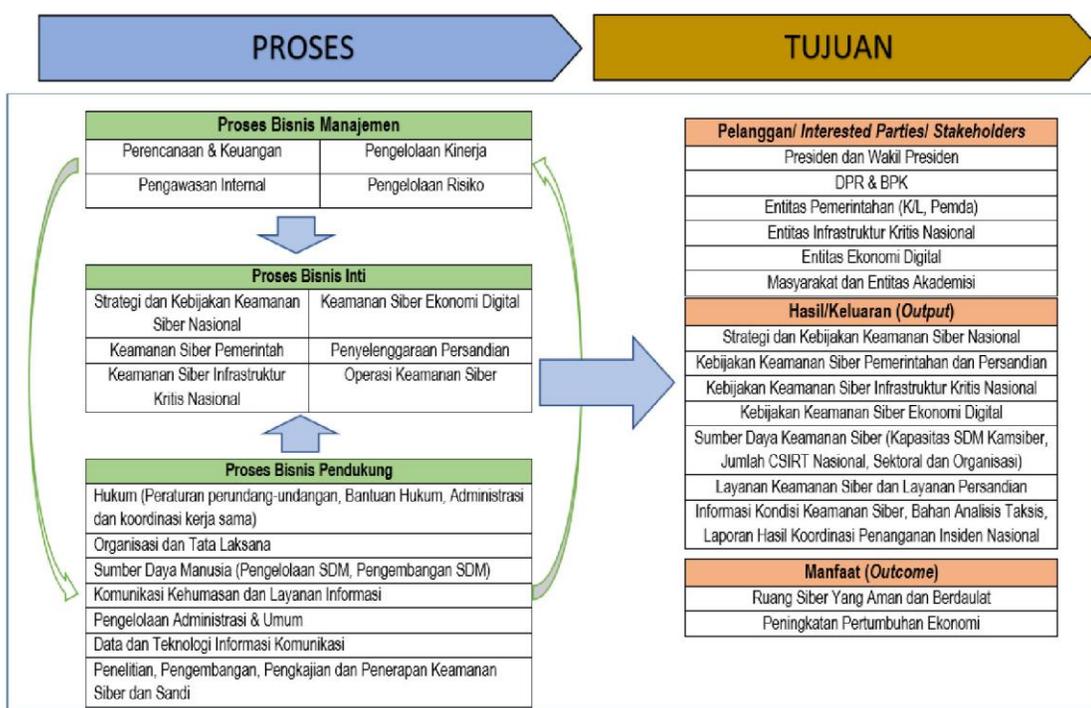
3.4.2. Rancangan Arsitektur Proses Bisnis BSSN

Penyusunan proses bisnis mengacu kepada 3 (tiga) prinsip dasar, yaitu proses bisnis yang utuh, efektif, dan efisien, penerapan prinsip keselarasan proses bisnis secara horizontal untuk mewujudkan cara kerja yang terintegrasi, dan penyerumpunan fungsi. Gambar 3.6 menunjukkan kerangka pikir pengorganisasian BSSN.



Gambar 3.6 Kerangka Pikir Pengorganisasian BSSN

Berdasarkan keseluruhan tugas dan fungsi sesuai peraturan perundang-undangan, BSSN melakukan berbagai kegiatan atau aktivitas sebagai penyelenggara dan pengelola keamanan siber Indonesia guna pencapaian output dan pemberian layanan. Dari keseluruhan kegiatan atau aktivitas tersebut, dapat dikelompokkan menjadi 3 (tiga) proses bisnis, yaitu proses operasional atau inti, proses manajemen, dan proses pendukung. Penyusunan arsitektur proses bisnis BSSN akan terus disempurnakan secara bertahap yang dimulai sejak tahun 2018 dan akan disempurnakan kembali sejalan dengan proses evaluasi dan penyempurnaan struktur organisasi 2020 serta ditetapkannya Renstra BSSN 2020-2024. Rancangan peta proses bisnis BSSN ditunjukkan pada Gambar 3.7.



Gambar 3.7 Rancangan Peta Proses Bisnis BSSN

3.4.3. Keselarasan Penataan Organisasi dengan Visi, Misi, dan Tujuan BSSN

Visi, misi, dan tujuan BSSN yang menjadi kerangka dalam pengembangan strategi BSSN telah terimplementasi dalam penataan struktur organisasi BSSN. Sebagaimana dalam kaidah pembentukan organisasi bahwa *structure follows strategy*, BSSN telah mengembangkan struktur organisasi berdasarkan strategi atau tujuan yang akan dicapai BSSN.

1. Misi BSSN ke-1: memberikan dukungan teknis dan administrasi serta analisis yang cepat, akurat, dan responsif kepada pemerintah, sebagai bahan pengambilan kebijakan penyelenggaraan pemerintahan negara dalam rangka mewujudkan kedaulatan siber Indonesia berkelas dunia akan dijawab dalam fungsi Deputy Strategi dan Sistem, Deputy Keamanan Siber Pemerintah dan Persandian, Deputy Keamanan Siber Infrastruktur Kritis Nasional, Deputy Keamanan Siber Ekonomi Digital, dan Pusat Operasi Keamanan Siber Nasional (NSOC).
2. Misi BSSN ke-2: menyelenggarakan keamanan siber dan persandian secara efektif dan efisien, dilaksanakan dengan:
 - a) menyusun dan menerapkan kebijakan keamanan siber dan persandian nasional yang berkualitas akan dijawab dalam fungsi organisasi Deputy Strategi dan Sistem.

- b) membangun sistem dan operasional keamanan siber dengan menggunakan standar-standar terkini melalui koordinasi dan kolaborasi dengan pemangku kepentingan dan menjalin kerjasama internasional akan dijawab dalam fungsi Deputy Keamanan Siber Pemerintah dan Persandian, Deputy Keamanan Siber Infrastruktur Kritis Nasional, Deputy Keamanan Siber Ekonomi Digital, dan Pusat Operasi Keamanan Siber Nasional (NSOC).
 - c) berperan aktif dalam meningkatkan kompetensi sumber daya manusia nasional di bidang keamanan siber dan sandi akan dijawab dalam fungsi Deputy Strategi dan Sistem yang didukung oleh Pusat Pendidikan dan Pelatihan dan Politeknik Siber dan Sandi (PSSN).
 - d) Membangun kondisi yang aman di ruang siber, menjamin perangkat teknologi yang aman, membangun kesadaran pengguna terhadap keamanan siber serta mendorong pemanfaatan teknologi secara aman dan tidak melawan hukum untuk mewujudkan ekosistem siber yang aman dan nyaman akan dijawab dalam fungsi organisasi Deputy Strategi dan Sistem.
3. Misi BSSN ke-3: meningkatkan kualitas sumber daya BSSN, dilaksanakan melalui:
- a) melakukan inovasi secara terus menerus untuk meningkatkan pertumbuhan birokrasi organisasi dan mendorong serta mengembangkan teknologi secara mandiri akan dijawab dalam fungsi Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi.
 - b) menyediakan sumber daya manusia, proses bisnis, sarana dan prasarana secara profesional dan akuntabel akan dijawab dalam fungsi Sekretariat Utama yang didukung oleh Pusat Data dan Teknologi Informasi Komunikasi, dan Inspektorat.

Selain menyusun organisasi berdasarkan strategi, penataan organisasi BSSN juga memperhatikan fungsi-fungsi yang sebelumnya telah dijalankan BSSN untuk menjamin keberlangsungan proses yang telah ada sejak tahun 2017. Fungsi-fungsi BSSN dalam Peraturan Presiden Nomor 53 Tahun 2017 telah terpetakan dalam penataan organisasi dan tata kerja BSSN yang dilakukan saat ini. Fungsi-fungsi

telah dikelompokkan berdasarkan kesamaan, kedekatan, dan tujuan yang akan dicapai untuk menghindari terjadinya duplikasi fungsi.

Adanya perkembangan situasi dan regulasi, terdapat beberapa fungsi-fungsi yang diamanat dalam kerangka regulasi setelah pembentukan organisasi BSSN. Beberapa amanat fungsi yang menjadi kewenangan BSSN terdapat dalam penyelenggaraan SPBE. Selain itu, arahan Presiden terkait penyederhanaan birokrasi ditindaklanjuti BSSN dengan meniadakan beberapa jabatan pengawas dan administrator dan menggantinya dengan mengoptimalkan jabatan fungsional sehingga akan terbentuk *talent-talent* organisasi BSSN yang memiliki daya saing. Dengan penyederhanaan birokrasi ini, BSSN mengedepankan aspek profesionalitas yang tinggi dalam pelaksanaan tugas dan fungsi, terlebih BSSN telah memiliki jabatan fungsional Sandiman sebagai kompetensi inti organisasi BSSN.

BAB IV
TARGET KINERJA DAN KERANGKA PENDANAAN

4.1. TARGET KINERJA

Keberhasilan pencapaian Renstra BSSN Tahun 2020 – 2024 yang mendukung RPJMN Tahun 2020-2024, dimana BSSN berkontribusi dalam agenda pembangunan penguatan stabilitas politik, hukum, pertahanan dan keamanan dan transformasi pelayanan publik, diukur dengan menetapkan sasaran pembangunan yaitu “Menjaga Stabilitas Keamanan Nasional” dengan indikator dan targetnya yaitu “Skor *Global Cybersecurity Index*” sebesar 0,838 (nol koma delapan tiga delapan) pada tahun 2024.

4.1.1. Sasaran Strategis, Indikator Kinerja Sasaran Strategis, dan Target

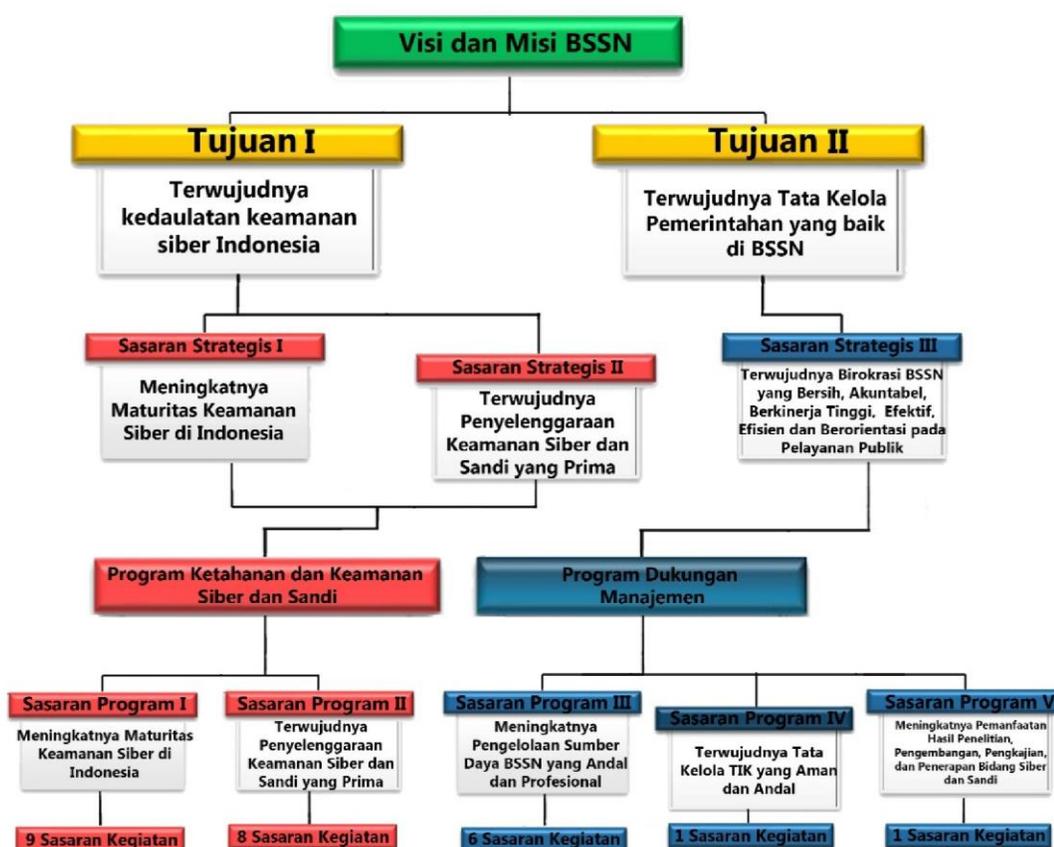
Indikator Kinerja Sasaran Strategis BSSN Tahun 2020-2024 beserta target kinerja per tahun tercantum pada Tabel 4.1.

Tabel 4.1 Sasaran Strategis, Indikator Kinerja Sasaran Strategis dan Target
BSSN Tahun 2020-2024

No	Sasaran Strategis	Indikator Kinerja Sasaran Strategis	Target				
			2020	2021	2022	2023	2024
1	Meningkatnya Maturitas Keamanan Siber di Indonesia	1.1. Tingkat Maturitas Objek Keamanan Siber	Level II	Level II	Level II+	Level II+	Level III
2	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima	2.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima	90%	91%	92%	93%	95%
3	Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien dan Berorientasi	3.1. Indeks Reformasi Birokrasi	70,01	73,35	77,21	80,77	84,36

No	Sasaran Strategis	Indikator Kinerja Sasaran Strategis	Target				
			2020	2021	2022	2023	2024
	pada Pelayanan Publik						

Keterkaitan antara Tujuan, Sasaran Strategis, Sasaran Program dan Sasaran Kegiatan BSSN Tahun 2020-2024 ditunjukkan pada Gambar 4.1.



Gambar 4.1 Keterkaitan antara Tujuan, Sasaran Strategis, Sasaran Program, dan Sasaran Kegiatan

4.1.1.2. Sasaran Program, Indikator Kinerja Sasaran Program, dan Target

BSSN mengampu 2 (dua) program yaitu keamanan dan ketahanan siber dan sandi negara dan program dukungan manajemen. Tolak ukur keberhasilan pencapaian sasaran program ditetapkan dengan indikator kinerja program. Sasaran program dan indikator kinerja sasaran program beserta targetnya untuk program keamanan dan ketahanan siber dan sandi negara dapat dilihat pada Tabel 4.2.

Tabel 4.2 Sasaran Program, Indikator Kinerja Sasaran Program, dan Target Program Keamanan dan Ketahanan Siber dan Sandi Negara

No	Sasaran Program	Indikator Kinerja Sasaran Program	Target				
			2020	2021	2022	2023	2024
1	Meningkatnya Maturitas Keamanan Siber di Indonesia	1.1. Tingkat Maturitas Objek Keamanan Siber	Level II	Level II	Level II+	Level II+	Level III
2	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima	2.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima	90%	91%	92%	93%	95%

Program dukungan manajemen merupakan program yang mendukung pelaksanaan tugas fungsi BSSN. Sasaran program, indikator kinerja sasaran program beserta targetnya untuk program dukungan manajemen dapat dilihat pada Tabel 4.3.

Tabel 4.3 Sasaran Program, Indikator Kinerja Sasaran Program, dan Target Program Dukungan Manajemen

No	Sasaran Program	Indikator Kinerja Sasaran Program	Target				
			2020	2021	2022	2023	2024
1	Meningkatnya Pengelolaan Sumber Daya BSSN yang Andal dan Profesional	1.1. Indeks Reformasi Birokrasi	70,01	73,35	77,21	80,77	84,36
		1.2. Opini Badan Pemeriksa Keuangan (BPK)	WDP	WDP	WTP	WTP	WTP
		1.3. Nilai AKIP BSSN	65,86	67,43	69,14	71,00	72,00

No	Sasaran Program	Indikator Kinerja Sasaran Program	Target				
			2020	2021	2022	2023	2024
2	Terwujudnya Tata Kelola TIK yang Aman dan Andal	2.1. Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)	3,1	3,3	3,5	3,8	4
		2.2. Skor Tingkat Kematangan Tata Kelola Informasi (Indeks KAMI)	310	360	420	490	585
3	Meningkatnya Pemanfaatan Hasil Penelitian, Pengembangan, Pengkajian, dan Penerapan Bidang Siber dan Sandi	3.1 Persentase Penelitian, Pengembangan, Pengkajian, dan Penerapan yang diimplementasikan oleh Pemangku Kepentingan.	60%	70%	75%	80%	90%

4.1.3. Sasaran Kegiatan, Indikator Kinerja Sasaran Kegiatan, dan Target

Program keamanan dan ketahanan siber dan sandi negara terdiri dari 17 (tujuh belas) kegiatan setingkat eselon II yang masing-masing memiliki sasaran kegiatan, indikator kinerja sasaran kegiatan, dan target untuk mendukung tercapainya sasaran program. Sasaran kegiatan, indikator kinerja sasaran kegiatan beserta targetnya yang berada di bawah program keamanan dan ketahanan siber dan sandi negara dapat dilihat pada Tabel 4.4.

Tabel 4.4 Sasaran Kegiatan, Indikator Kinerja Sasaran Kegiatan, dan Target
Program Keamanan dan Ketahanan Siber dan Sandi Negara

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
3080	Identifikasi Kerentanan dan Penilaian Risiko pada Sektor Pemerintah Unit Kerja: Direktorat Identifikasi Kerentanan dan Penilaian Risiko Pemerintah						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Pemerintah	1.1. Tingkat Maturitas Objek Keamanan Siber Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Pemerintah	Level II	Level II	Level II+	Level II+	Level III
3081	Identifikasi Kerentanan dan Penilaian Risiko pada Sektor Infrastruktur Informasi Kritis Nasional Unit Kerja: Direktorat Identifikasi Kerentanan dan Penilaian Risiko pada Sektor Infrastruktur Informasi Kritis Nasional						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor IIKN	1.1. Tingkat Maturitas Objek Keamanan Siber Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor IIKN	Level III	Level III	Level III	Level III+	Level III+
3082	Identifikasi Kerentanan dan Penilaian Risiko pada Sektor Ekonomi Digital Unit Kerja: Direktorat Identifikasi Kerentanan dan Penilaian Risiko Ekonomi Digital						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Ekonomi Digital	1.1. Tingkat Maturitas Objek Keamanan Siber Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Ekonomi Digital	Level III	Level III	Level III	Level III+	Level III+
3083	Deteksi Terhadap Ancaman Siber Unit Kerja: Direktorat Deteksi Ancaman						
1	Terwujudnya Penyelenggaraa	1.1. Persentase Pemenuhan	90%	91%	92%	93%	95%

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
	n Keamanan Siber dan Sandi yang Prima Bidang Deteksi Ancaman Siber	Layanan Keamanan Siber dan Sandi yang Prima Bidang Deteksi Ancaman Siber					
3085	Proteksi Keamanan Informasi Pemerintah Unit Kerja: Direktorat Proteksi Pemerintah						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Proteksi Sektor Pemerintah	1.1. Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Proteksi Sektor Pemerintah	Level II	Level II	Level II+	Level II+	Level III
3086	Proteksi Infrastruktur Informasi Kritis Nasional Unit Kerja: Direktorat Proteksi Infrastruktur Informasi Kritis Nasional						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Proteksi Sektor IIKN	1.1. Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Proteksi Sektor IIKN	Level III	Level III	Level III	Level III+	Level III+
3092	Proteksi Ekonomi Digital Unit Kerja: Direktorat Proteksi Ekonomi Digital						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Proteksi Sektor Ekonomi Digital	1.1. Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Proteksi Sektor Ekonomi Digital	Level III	Level III	Level III	Level III+	Level III+
3093	Penanggulangan dan Pemulihan Keamanan Siber dan Sandi Sektor Pemerintah Unit Kerja: Direktorat Penanggulangan dan Pemulihan Pemerintah						
1	Meningkatnya Maturitas Keamanan Siber di	1.1 Tingkat Maturitas Objek Keamanan	Level II	Level II	Level II+	Level II+	Level III

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
	Indonesia Bidang Penanggulangan dan Pemulihan Sektor Pemerintah	Siber di Indonesia Bidang Penanggulangan dan Pemulihan Sektor Pemerintah					
3094	Penanggulangan dan Pemulihan Keamanan Siber dan Sandi Sektor Infrastruktur Informasi Kritis Nasional Unit Kerja: Direktorat Penanggulangan dan Pemulihan Infrastruktur Informasi Kritis Nasional						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Penanggulangan dan Pemulihan Sektor IIKN	1.1. Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Penanggulangan dan Pemulihan Sektor IIKN	Level III	Level III	Level III	Level III+	Level III+
3095	Penanggulangan dan Pemulihan Keamanan Siber dan Sandi Sektor Ekonomi Digital Unit Kerja: Direktorat Penanggulangan dan Pemulihan Ekonomi Digital						
1	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Penanggulangan dan Pemulihan Sektor Ekonomi Digital	1.1. Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Penanggulangan dan Pemulihan Sektor Ekonomi Digital	Level III	Level III	Level III	Level III+	Level III+
3101	Pengendalian Sumber Daya Manusia Siber dan Sandi Nasional Unit Kerja: Direktorat Pengendalian Sumber Daya Manusia						

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
1	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima Bidang Pengendalian Sumber Daya Manusia	1.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima Bidang Pengendalian Sumber Daya Manusia	90%	91%	92%	93%	95%
3102	Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi Unit Kerja: Direktorat Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi						
1	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima Bidang Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi	1.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima Bidang Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi	90%	91%	92%	93%	95%
3106	Pengendalian Informasi, Investigasi, dan Forensik Digital Unit Kerja: Direktorat Pengendalian Informasi, Investigasi, dan Forensik Digital						
1	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima Bidang Pengendalian Informasi, Investigasi, dan Forensik Digital	1.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima Bidang Pengendalian Informasi, Investigasi, dan Forensik Digital	90%	91%	92%	93%	95%
3118	Penyelenggaraan Operasi Keamanan Siber Unit Kerja: Pusat Operasi Keamanan Siber Nasional						
1	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima Bidang Operasional Keamanan	1.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima Bidang Operasional Keamanan	90%	91%	92%	93%	95%

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
	Siber Nasional	Siber Nasional					
		1.2. Persentase Pemenuhan Monitoring Keamanan Jaringan yang Berkualitas	13%	36%	65%	88%	100%
3121	Pendidikan dan Pelatihan Bidang Siber dan Sandi Unit Kerja: Pusat Pendidikan dan Pelatihan						
1	Terwujudnya Layanan Kamsiber dan Sandi Bidang Pendidikan dan Pelatihan Sumber Daya Manusia Siber dan Sandi	1.1. Persentase Lulusan Sumber Daya Manusia Siber dan Sandi berstandarkan nilai minimal "Baik"	82%	83%	84%	85%	85%
		1.2. Indeks Kepuasan Layanan Diklat	80	83	85	87	89
3123	Pendidikan Profesional di Bidang Siber dan Sandi Unit Kerja: Politeknik Siber dan Sandi Negara						
1	Terwujudnya Layanan Kamsiber dan Sandi Bidang Pendidikan Profesional Sumber Daya Manusia Siber dan Sandi yang berkualitas	1.1. Tingkat Kepuasan Pengguna Terhadap Kompetensi Lulusan	95%	95%	95%	95%	95%
		1.2. Persentase Lulusan dari Mahasiswa yang Naik Tingkat	90%	90%	91%	91%	91%
3124	Penyelenggaraan Sertifikasi Elektronik Unit Kerja: Balai Sertifikasi Elektronik						
1	Terwujudnya Layanan Keamanan Siber dan Sandi yang Prima Bidang Sertifikasi Elektronik	1.1. Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Berkualitas Bidang Sertifikasi	100%	100%	100%	100%	100%

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
		Elektronik					

Program dukungan manajemen terdiri dari 7 (tujuh) kegiatan setingkat eselon II. Sasaran kegiatan, indikator kinerja sasaran kegiatan, dan target yang berada di bawah program dukungan manajemen dapat dilihat pada Tabel 4.5.

Tabel 4.5 Sasaran Kegiatan, Indikator Kinerja Sasaran Kegiatan, dan Target Program Dukungan Manajemen

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
3075	Penyelenggaraan Perencanaan dan Keuangan Unit Kerja: Biro Perencanaan dan Keuangan						
1	Terselenggaranya Perencanaan, Pengelolaan Kinerja, dan Keuangan yang Andal dan Profesional	1.1. Nilai Kinerja Anggaran BSSN	85	88	90	93	93
		1.2. Indeks RB Area Penguatan Akuntabilitas	4,45	4,62	4,78	4,94	5,11
		1.3. Nilai Indikator Kinerja Pelaksanaan Anggaran BSSN	93	95	97	98	98
		1.4. Nilai AKIP BSSN	65,86	67,43	69,14	71,00	72,00
3076	Penyelenggaraan Organisasi dan Sumber Daya Manusia Unit Kerja: Biro Organisasi dan Sumber Daya Manusia						
1	Terselenggaranya Pengelolaan Organisasi dan Tata Laksana yang Andal	1.1. Indeks RB Area Penataan dan Penguatan Organisasi	5,01	5,42	5,57	5,84	6,52
		1.2. Tingkat Pemenuhan Proses Bisnis	70%	75%	80%	85%	90%
		1.3. Indeks RB Area Manajemen Perubahan	4,36	4,39	4,42	4,45	4,48

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
2	Terselenggaranya Manajemen Aparatur Sipil Negara yang Profesional	2.1. Indeks Profesionalitas Aparatur Sipil Negara	85,00	85,21	85,50	86,00	86,50
		2.2. Indeks RB Area Penataan Sistem Manajemen Sumber Daya Manusia	7,26	7,29	7,41	7,43	7,44
3077	Penyelenggaraan Hukum dan Hubungan Masyarakat Unit Kerja: Biro Hukum dan Hubungan Masyarakat						
1	Terselenggaranya Hukum, Komunikasi Publik, dan Dukungan Strategis Pimpinan yang Andal dan Profesional	1.1. Indeks RB Area Deregulasi Kebijakan	3,75	3,80	3,85	4,00	4,05
		1.2. Indeks RB Area Peningkatan Kualitas Pelayanan Publik	5,70	5,98	6,09	6,38	6,56
		1.3. Indeks Persepsi Kualitas Pelayanan	8,24	8,29	8,56	8,78	8,90
		1.4. Indeks Keterbukaan Informasi Publik BSSN	80,55	83,05	85,55	87,77	90,65
		1.5. Persentase Pemenuhan Layanan Dukungan Strategis Pimpinan	100%	100%	100%	100%	100%
3078	Penyelenggaraan Dukungan Administratif Bidang Ketatausahaan dan Kearsipan, Kerumahtanggaan, Pengelolaan BMN, dan Layanan Pengadaan Unit Kerja: Biro Umum						
1	Terselenggaranya Dukungan Administratif Bidang Ketatausahaan dan Kearsipan, Kerumah-	1.1. Hasil Pengawasan Arsip	90,01	91,00	92,00	93,00	94,00
		1.2. Tingkat Kematangan UKPBJ BSSN	Pro aktif (4/9)	Pro aktif (9/9)	Strategis (3/9)	Strategis (6/9)	Strategis (9/9)

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target				
			2020	2021	2022	2023	2024
	tangganan, Pengelolaan BMN, dan Layanan Pengadaan yang andal dan profesional	1.3. Tingkat Akuntabilitas Pengelolaan BMN	90%	91%	92%	93%	94%
		1.4. Pemenuhan dan Pemeliharaan Sarana dan Prasarana	85%	85%	90%	90%	95%
3079	Pengawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara Unit Kerja: Inspektorat						
1	Terselenggaranya Pengawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara	1.1. Indeks RB area Penguatan Pengawasan	5,02	5,92	6,82	7,72	8,62
		1.2. Opini BPK	WDP	WDP	WTP	WTP	WTP
3138	Pengelolaan Data dan Teknologi Informasi Komunikasi Unit Kerja: Pusat Data dan Teknologi Informasi Komunikasi						
1	Terwujudnya Tata Kelola TIK yang aman dan andal	1.1. Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)	3,1	3,3	3,5	3,8	4
		1.2. Skor Tingkat kematangan Tata Kelola (Indeks KAMI)	310	360	420	490	585
3139	Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi Unit Kerja: Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi						
1	Meningkatnya Pemanfaatan Hasil Penelitian, Pengembangan Pengkajian, dan Penerapan Bidang Siber dan Sandi	1.1. Persentase Penelitian, Pengembangan, Pengkajian, dan Penerapan yang diimplementasikan oleh Pemangku Kepentingan	60%	70%	75%	80%	90%

4.2. KERANGKA PENDANAAN

Indikasi kebutuhan pendanaan untuk mencapai tujuan dan sasaran strategis BSSN dalam kurun 2020-2024 tertuang dalam matriks kerangka pendanaan jangka menengah sebagaimana pada Tabel 4.6.

Tabel 4.6 Kerangka Pendanaan BSSN Tahun 2020-2024

Program	Indikasi Kebutuhan Pendanaan (dalam jutaan rupiah)				
	2020	2021	2022	2023	2024
Dukungan Manajemen	1.162.289,253	1.392.695,362	1.271.364,757	1.242.548,310	1.057.145,070
Keamanan dan Ketahanan Siber dan Sandi Negara	3.294.855,880	1.899.994,724	2.000.298,626	1.787.425,407	1.846.616,273
Total	4.457.145,133	3.292.690,086	3.271.663,383	3.029,973,717	2.903.761,343

Penyusunan kerangka pendanaan BSSN tahun 2020-2024 tersebut di atas telah merujuk pada indikasi pendanaan BSSN dalam RPJMN Tahun 2020-2024, dan dengan mempertimbangkan hal-hal sebagai berikut:

1. pendanaan kegiatan prioritas nasional tahun 2020-2024 sebagaimana matriks pembangunan jangka menengah BSSN pada RPJMN 2020-2024.
2. pendanaan inisiatif strategis BSSN Tahun 2020-2024 dalam rangka pencapaian tujuan dan sasaran strategis BSSN.
3. pendanaan pemenuhan kebutuhan dasar penyelenggaraan perkantoran BSSN Tahun 2020-2024.

Rincian target kinerja dan indikasi kebutuhan anggaran masing-masing program dan kegiatan BSSN tahun 2020 sampai dengan 2024 tertuang dalam matriks kinerja dan kerangka pendanaan.

BAB V
PENUTUP

Renstra BSSN Tahun 2020-2024 telah dijabarkan ke dalam visi, misi, tujuan, sasaran strategis, arah kebijakan, strategi, program, dan kegiatan pembangunan yang bersifat strategis dan indikatif sesuai tugas dan fungsi BSSN. Selanjutnya, Renstra ini harus dijabarkan lagi oleh setiap satuan unit kerja BSSN untuk menyusun lebih detail secara teknis operasional pada setiap tahunnya dan secara berkesinambungan.

Renstra ini disusun dengan mempertimbangkan potensi, peluang, serta kendala, dan permasalahan yang dihadapi sehingga penetapan target-target yang berorientasi pada hasil dan diharapkan dapat dicapai dalam kurun waktu 5 (lima) tahun. Untuk menjamin akuntabilitas dan konsistensi arah pembangunan BSSN, Renstra BSSN Tahun 2020-2024 perlu dievaluasi setiap tahunnya. Mengingat lingkungan strategis BSSN yang sangat dinamis, dan dengan mempertimbangkan hasil evaluasi tahunan, maka substansi dan indikator kinerja yang ditetapkan pada Renstra BSSN periode Tahun 2020-2024 ini, dapat direvisi atau diubah, sesuai dengan kebutuhan dan mekanisme yang berlaku.

Keberhasilan penerapan Renstra tergantung dari komitmen dan konsistensi organisasi untuk mengimplementasikannya. Target pembangunan BSSN yang telah ditetapkan, hanya dapat diwujudkan melalui sinergi dan kolaborasi yang baik antara instansi pemerintah pusat, pemerintah daerah, dan sektor terkait. Sinergi dan kolaborasi eksternal ini harus diimbangi dengan keterpaduan, kerjasama, keterbukaan, dan etos kerja yang baik pula dari seluruh personel dan unit kerja di lingkungan internal BSSN. Akhir kata, semoga stabilitas keamanan nasional negara dan bangsa Indonesia dapat diwujudkan melalui pembangunan siber dan persandian tahun 2020-2024.

**MATRIKS KINERJA DAN PENDANAAN BADAN SIBER DAN SANDI NEGARA
TAHUN 2020-2024**

Program / Kegiatan	Sasaran Program (Outcome)/Sasaran Kegiatan (Output)/Indikator	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit Organisasi Pelaksana		
			2020	2021	2022	2023	2024	2020	2021	2022	2023	2024			
BADAN SIBER DAN SANDI NEGARA	Meningkatnya Maturitas Keamanan Siber di Indonesia														
	- Tingkat Maturitas Objek Keamanan Siber		Level II	Level II	Level II +	Level II +	Level III								
	Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima														
	- Persentase pemenuhan layanan keamanan siber dan sandi yang prima		90%	91%	92%	93%	95%								
	Terwujudnya Birokrasi BSSN yang Efektif, Profesional dan berorientasi pada pelayanan publik														
	- Indeks Reformasi Birokrasi		70,01	73,35	77,21	80,77	84,36								
PROGRAM DUKUNGAN MANAJEMEN															
	Meningkatnya Pengelolaan Sumber Daya BSSN yang andal dan profesional														
	- Indeks Reformasi Birokrasi		70,01	73,35	77,21	80,77	84,36	1.162.289,253	1.392.695,362	1.271.364,757	1.242.548,310	1.057.145,070			
	- Opini BPK		WDP	WDP	WTP	WTP	WTP								
	- Nilai Akuntabilitas Kinerja Instansi Pemerintah (AKIP)		65,86	67,43	69,14	71,00	72,00								
	Terwujudnya Tata Kelola														

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit	
	TIK yang aman dan andal													
	- Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)		3,1	3,3	3,5	3,8	4							
	- Skor Tingkat kematangan Tata Kelola (Indeks KAMI)	310	360	420	490	585								
	Meningkatnya pemanfaatan hasil penelitian, pengembangan, pengkajian, dan penerapan bidang siber dan sandi													
	- Persentase penelitian, pengembangan, pengkajian, dan penerapan yang diimplementasikan oleh pemangku kepentingan		60%	70%	75%	80%	90%							
3075 : Penyelenggaraan Perencanaan dan Keuangan								209.642,037	234.469,380	246.192,848	258.502,489	271.427,612	Biro Perencanaan dan Keuangan	
	Terselenggaranya Perencanaan, Pengelolaan Kinerja, dan Keuangan yang Andal dan Profesional													
	- Nilai Kinerja Anggaran		85	88	90	93	93							
	- Indeks RB Area		4,45	4,62	4,78	4,94	5,11							
	- Penguatan Akuntabilitas													
	- Nilai Indikator Kinerja Pelaksanaan Anggaran BSSN		93	95	97	98	98							
	- Nilai Akuntabilitas Kinerja Instansi Pemerintah (AKIP)		65,86	67,43	69,14	71,00	72,00							
3076 : Penyelenggaraan Organisasi dan Sumber Daya Manusia								21.302,528	27.498,372	31.930,535	38.066,318	45.560,255	Biro Organisasi dan Sumber Daya Manusia	
	Terselenggaranya Pengelolaan Organisasi dan Tata Laksana yang Andal													
	- Indeks RB Area Penataan dan Penguatan Organisasi		5,01	5,42	5,57	5,84	6,52							
	- Tingkat Pemenuhan		70%	75%	80%	85%	90%							

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit	
	Proses Bisnis													
	- Indeks RB Area Manajemen Perubahan		4,36	4,39	4,42	4,45	4,48							
	Terselenggaranya Manajemen Aparatur Sipil Negara yang Profesional													
	- Indeks Profesionalitas Aparatur Sipil Negara (ASN)		85,00	85,21	85,50	86,00	86,50							
	- Indeks RB Area Penataan Sistem Manajemen Sumber Daya Manusia		7,26	7,29	7,41	7,43	7,44							
3077 : Penyelenggaraan Hukum dan Hubungan Masyarakat								11.199,954	13.402,028	14.072,129	14.775,736	15.514,521		Biro Hukum dan Hubungan Masyarakat
	Terselenggaranya Hukum, Komunikasi Publik, dan Dukungan Strategis Pimpinan yang Andal dan Profesional													
	- Indeks RB Area Deregulasi Kebijakan		3,75	3,80	3,85	4,00	4,05							
	- Indeks RB Area Peningkatan Kualitas Pelayanan Publik		5,70	5,98	6,09	6,38	6,56							
	- Indeks Persepsi Kualitas Pelayanan		8,24	8,29	8,56	8,78	8,90							
	- Indeks Keterbukaan Informasi Publik BSSN		80,55	83,05	85,55	87,77	90,65							
	- Persentase Pemenuhan Layanan Dukungan Strategis Pimpinan		100%	100%	100%	100%	100%							
3078 : Penyelenggaraan Dukungan Administratif Bidang Ketausahaan dan Kerasipan, Kerumahantangan, Pengelolaan BMN, dan Layanan Pengadaan								258.256,336	271.169,153	284.727,610	298.963,991	313.912,190		Biro Umum
	Terselenggaranya													

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit	
	Dukung Administraf Bidang Ketatausahaan dan Kerasipan, Kerumahantagaan, Pengelolaan BMN, dan Layanan Pengadaan yang andal dan profesional		90,01	91,00	92,00	93,00	94,00							
	- Hasil Pengawasan Atsrip - Tingkat Kematangan UKPBJ BSSN	Proaktif (4/9)	Proaktif (9/9)	Strategis (3/9)	Strategis (6/9)	Strategis (9/9)								
	- Tingkat Akuntabilitas Pengelolaan BMN	90%	91%	92%	93%	94%								
	- Pemenuhan dan Pemeliharaan Sarana dan Prasarana	85%	85%	90%	90%	95%								
	3079 : Penguawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara						4.111,060	5.150,000	5.304,500	5.463,635	5.627,544		Inspektorat	
	Terselenggaranya Penguasaan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara													
	- Indeks RB area Penguatan Penguasaan	5,02	5,92	6,82	7,72	8,62								
	- Opini BPK	WDP	WDP	WTP	WTP	WTP								
	3038 : Pengelolaan Data dan Teknologi Informasi Komunikasi						550.635,128	731.006,429	589.137,135	546.776,141	320.102,948		Pusat Data dan Teknologi Informasi Komunikasi	
	Terwujudnya Tata Kelola TIK yang aman dan andal													
	- Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)	3,1	3,3	3,5	3,8	4								
	- Skor Tingkat Kematangan Tata Kelola (Indeks KAMI)	310	360	420	490	585								

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit
3039 : Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi	Meningkatnya pemanfaatan hasil penelitian, pengembangan, pengkajian, dan penerapan bidang siber dan sandi						107.142,210	110.000,000	100.000,00	80.000,000	85.000,000		Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi
PROGRAM KEAMANAN DAN KETAHANAN SIBER DAN SANDI NEGARA	- Persentase penelitian, pengembangan, pengkajian, dan penerapan yang diimplementasikan oleh pemangku kepentingan						60%	70%	75%	80%	90%		
Meningkatnya Maturitas Keamanan Siber di Indonesia	- Tingkat Maturitas Objek Keamanan Siber												
Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima	- Persentase pemenuhan layanan keamanan siber dan sandi yang prima						90%	91%	92%	93%	95%		
3080: Identifikasi Kerentanan dan Penilaian Risiko Sektor Pemerintahan							8.825,053	10.336,000	10.500,000	11.000,000	11.500,000		Direktorat Identifikasi Kerentanan dan Penilaian Risiko Pemerintahan

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit	
	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Pemerintah													
	- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor IIKN		Level II	Level II	Level II +	Level II +	Level II +	Level III						
3081: Identifikasi Kerentanan dan Penilaian Risiko Sektor Infrastruktur Informasi Kritis Nasional (IIKN)														Direktorat Identifikasi Kerentanan dan Penilaian Risiko Informasi Kritis Nasional
	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor IIKN													
	- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor IIKN		Level III	Level III	Level III	Level III +	Level III +	Level III						
3082: Identifikasi Kerentanan dan Penilaian Risiko Ekonomi Digital														Direktorat Identifikasi Kerentanan dan Penilaian Risiko Ekonomi Digital
										118.972,845	36.000,000	35.000,000	37.000,000	37.000,000

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit	
	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Ekonomi Digital													
	- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Identifikasi Kerentanan dan Penilaian Risiko Sektor Ekonomi Digital	Level III	Level III	Level III	Level III +	Level III +								
3083: Deteksi Ancaman Siber							10.172,773	364.847,450	456.100,000	533.000,000	633.000,000		Direktorat Deteksi Ancaman	
	Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima Bidang Deteksi Ancaman Siber													
	- Persentase pemenuhan layanan keamanan siber dan sandi yang prima Bidang Deteksi Ancaman Siber	90%	91%	92%	93%	95%								
3085: Proteksi Sektor Pemerintah							225.954,039	81.044,916	116.603,887	99.642,836	136.772,332		Direktorat Proteksi Pemerintah	
	Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Proteksi Sektor Pemerintah													
	- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Proteksi Sektor Pemerintah	Level II	Level II	Level II +	Level II +	Level III								
3086: Proteksi Sektor Infrastruktur Informasi Kritis Nasional (IIKN)							202.390,317	137.951,856	42.522,191	46.774,410	51.451,851		Direktorat Proteksi Infrastruktur Informasi Kritis Nasional	

Program / Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)							Unit Nasional				
Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Proteksi Sektor IKN																		
- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Proteksi Sektor IKN		Level III	Level III	Level III	Level III +	Level III +												
3092: Proteksi Sektor Ekonomi Digital																		Direktorat Proteksi Ekonomi Digital
Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Proteksi Ekonomi Digital																		
- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Proteksi Ekonomi Digital		Level III	Level III	Level III	Level III +	Level III +												
3093: Peningkatan dan Pemulihan Keamanan Siber dan Sandi Sektor Pemerintah																		Direktorat Peningkatan dan Pemulihan Pemerintah
Meningkatnya Maturitas Keamanan Siber di Indonesia Bidang Peningkatan dan Pemulihan Sektor Pemerintah																		
- Tingkat Maturitas Objek Keamanan Siber di Indonesia Bidang Peningkatan dan Pemulihan Sektor Pemerintah		Level II	Level II	Level II +	Level II +	Level III												
3094: Peningkatan dan Pemulihan Keamanan Siber dan Sandi Sektor Infrastruktur Informasi Kritis Nasional																		Direktorat Peningkatan dan
							34.157,857	18.593,600	21.572,300	20.906,700	24.246,000							

Program / Sumber Daya Manusia	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit	
- Persentase pemenuhan layanan keamanan siber dan sandi yang prima Bidang Pengendalian Sumber Daya Manusia		90%	91%	92%	93%	95%							
3102: Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi							5.268,665	9.240,000	9.482,000	10.893,000	12.332,000		Direktorat Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi
Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima Bidang Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi		90%	91%	92%	93%	95%							
3106: Pengendalian Informasi, Investigasi, dan Forensik Digital							715.851,367	162.320,034	165.318,751	168.253,751	21.353,751		Direktorat Pengendalian Informasi, Investigasi, dan Forensik Digital
Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima Bidang Pengendalian Informasi, Investigasi dan Forensik Digital													

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)						Unit		
			90%	91%	92%	93%	95%									
3118: Penyelenggaraan Operasi Keamanan Siber Nasional	layanan keamanan siber dan sandi yang prima Bidang Pengendalian Informasi, Investigasi dan Forensik Digital															Pusat Operasi Keamanan Siber Nasional
	Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima Bidang Operasional Keamanan Siber Nasional															
	- Persentase pemenuhan layanan keamanan siber dan sandi yang prima Bidang Operasional Keamanan Siber		90%	91%	92%	93%	95%									
	- Persentase pemenuhan monitoring keamanan jaringan yang berkualitas		13%	36%	65%	88%	100%									
3121: Pendidikan dan Pelatihan Bidang Siber dan Sandi	Terwujudnya Layanan Kansiber dan Sandi Bidang Pendidikan dan Pelatihan Sumber Daya Manusia Siber dan Sandi															Pusat Pendidikan dan Pelatihan
	- Persentase Lulusan Sumber Daya Manusia Siber dan Sandi berstandarkan nilai minimal "Baik"		82%	83%	84%	85%	85%									
	- Indeks Kepuasan Layanan Diklat		80	83	85	87	89									
3123: Pendidikan Profesional di Bidang Siber dan Sandi	Layanan Diklat															Sekolah Tinggi Sandi
									778.918,020	54.000,000	132.556,000	77.334,000	93.747,000			
									151.446,983	65.000,000	71.500,000	78.650,000	82.582,500			

Program /	Sasaran Program	Lokasi	Target					Alokasi (dalam juta rupiah)					Unit		
	Terwujudnya Layanan Keamanan Siber dan Sandi Bidang Pendidikan Profesional Sumber Daya Manusia Siber dan Sandi yang berkualitas														
	- Tingkat Kepuasan Pengguna Terhadap Kompetensi Lulusan		95%	95%	95%	95%	95%								
	- Persentase Lulusan dari Mahasiswa yang Naik Tingkat		90%	90%	91%	91%	92%								
3124: Penyelenggaraan Sertifikasi Elektronik	Terwujudnya penyelenggaraan keamanan siber dan sandi yang prima Bidang Sertifikasi Elektronik														Balai Sertifikasi Elektronik
	- Persentase pemenuhan layanan keamanan siber dan sandi yang prima Bidang Sertifikasi Elektronik		100%	100%	100%	100%	100%								

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN