BERITA NEGARA REPUBLIK INDONESIA

No. 1461, 2021 BSSN. Renstra. BSSN. Tahun 2020-2024. Perubahan.

PERATURAN BADAN SIBER DAN SANDI NEGARA

NOMOR 10 TAHUN 2021

TENTANG

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

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : a. bahwa dengan adanya perubahan organisasi dan tata kerja untuk penguatan tugas dan fungsi Badan Siber dan Sandi Negara di bidang keamanan siber dan sandi, perlu dilakukan penyesuaian terhadap rencana strategis Badan Siber dan Sandi Negara Tahun 2020-2024;

b. bahwa perubahan rencana strategis Badan Siber dan Sandi Negara Tahun 2020–2024 disusun untuk menjamin keterkaitan dan konsistensi antara perencanaan, penganggaran, pelaksanaan, dan pengawasan dalam menjamin tercapainya penggunaan sumber daya secara efisien, efektif, berkeadilan, dan berkelanjutan serta menjadi pedoman bagi penyusunan dokumen perencanaan tahunan Badan Siber dan Sandi Negara;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf b, Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana

Strategis Badan Siber dan Sandi Negara tahun 2020-2024 perlu diubah;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 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 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
4. Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 (Berita Negara Republik Indonesia Tahun 2020 Nomor 843);
5. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PERUBAHAN ATAS PERATURAN BADAN SIBER DAN SANDI NEGARA NOMOR 5 TAHUN 2020 TENTANG RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2020-2024.

Pasal I

Ketentuan dalam Lampiran Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 (Berita Negara Republik Indonesia Tahun 2020 Nomor 843) diubah sehingga menjadi sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal II

1. Pada saat Peraturan Badan ini mulai berlaku:
   a. pelaksanaan Program dan kegiatan yang telah dilaksanakan sebelum diundangkannya Peraturan Badan ini, tetap didasarkan pada Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 yang ditetapkan berdasarkan Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024; dan
   b. pelaksanaan Program dan kegiatan yang masih berjalan tetap dapat dilaksanakan sampai dengan akhir tahun anggaran 2021 dan didasarkan pada Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024 yang ditetapkan berdasarkan Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis Badan Siber dan Sandi Negara Tahun 2020-2024.

2. 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 27 Desember 2021

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 30 Desember 2021

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

ttd

BENNY RIYANTO

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2021
TENTANG
PERUBAHAN ATAS PERATURAN BADAN SIBER DAN SANDI NEGARA NOMOR 5 TAHUN 2020 TENTANG RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2020-2024

PERUBAHAN RENCANA STRATEGIS BADAN SIBER DAN SANDI NEGARA TAHUN 2020 – 2024

BAB I
PENDAHULUAN

1.1. KONDISI UMUM

Paradigma pembangunan siber dan sandi nasional sesuai amanah Rencana Pembangunan Jangka Menengah Nasional (RPJMN) Tahun 2020–2024 adalah mewujudkan keamanan, perlindungan, dan kedaulatan siber nasional serta meningkatkan pertumbuhan ekonomi nasional. Hal ini selaras dengan tugas dan fungsi Badan Siber dan Sandi Negara (BSSN) sebagaimana telah ditetapkan oleh Presiden Republik Indonesia Joko Widodo pada tanggal 13 April 2021 melalui Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Peraturan Presiden tersebut mengganti 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, sebagai upaya untuk menghadapi tantangan dan dinamika keamanan siber saat ini dan ke depan.

Dalam rangka mewujudkan amanat yang telah ditetapkan tersebut, maka terdapat konsekuensi terhadap perubahan dokumen Rencana Strategis (Renstra) BSSN yang telah diterbitkan sebelumnya. Sehingga dalam menyelaraskan arah dan tujuan sesuai yang termaktub dalam Peraturan Presiden 28 Tahun 2021 tentang Badan Siber dan

Sandi Negara, diperlukan penetapan strategi dan langkah sebagai acuan dalam pengambilan kebijakan, keputusan, dan tindakan yang tepat di bidang keamanan siber dan sandi yang selanjutnya dituangkan dalam dokumen Perubahan Renstra BSSN. Penyusunan Perubahan 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 Tahun 2020–2024.

Perubahan Renstra BSSN Tahun 2020–2024 disusun untuk menjamin keterkaitan dan konsistensi antara perencanaan, penganggaran, pelaksanaan, dan pengawasan dalam menjamin tercapainya penggunaan sumber daya secara efisien, efektif, berkeadilan, dan berkelanjutan serta menjadi pedoman bagi penyusunan dokumen perencanaan tahunan BSSN.

Penyempurnaan organisasi BSSN melalui penataan kembali fungsi-fungsi yang ada berdasar prinsip "*structure follow process follow strategy*" yang ditetapkan melalui Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara merupakan upaya untuk mewujudkan organisasi BSSN yang berfokus pada strategi dan berkinerja tinggi dalam rangka mencapai tujuan dan sasaran BSSN. Perubahan struktur organisasi pada BSSN tersebut mengacu pada konsep *mission oriented* dimana penekanannya terdapat pada penguatan tata kelola dan operasional keamanan siber. Berdasarkan hasil evaluasi organisasi terhadap struktur organisasi BSSN sesuai Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Sabar dan Sandi Negara yang mengacu pada bisnis proses *cyber security framework*, menunjukkan hasil yang belum optimal dalam menjawab tantangan keamanan siber yang semakin berkembang. Penyempurnaan organisasi BSSN ini yang mendasari perlunya dilakukan perubahan terhadap Renstra BSSN Tahun 2020-2024 yang akan tetap fokus pada upaya-upaya mewujudkan kedaulatan siber Indonesia berkelas dunia. Selain itu, Perubahan Renstra BSSN juga memuat restrukturisasi data dan informasi kinerja BSSN *pasca* reorganisasi BSSN.

Dalam Bab I ini disajikan kondisi umum yang meliputi gambaran terkait kondisi keamanan siber nasional, dan pencapaian Renstra BSSN pada tahun 2020 sebagai pijakan dalam merumuskan kebijakan untuk periode mendatang. Selain capaian-capaian BSSN, sebagai bentuk

implementasi perencanaan partisipatif yaitu perencanaan yang berbasis pada partisipasi masyarakat yang merupakan harapan pemangku kepentingan kepada BSSN akan dijabarkan sebagai masukan penyusunan Perubahan Renstra BSSN 2020-2024.

Keamanan ruang siber turut dipengaruhi beberapa isu-isu strategis diantaranya meningkatnya penetrasi internet, bergulirnya revolusi industri 4.0, dan kondisi pandemi *covid-19*, telah mengakibatkan percepatan digitalisasi ditandai dengan meningkatnya penggunaan akses internet dan pemanfaatan teknologi informasi sebagai implikasi dari adaptasi kebiasan baru. Meningkatnya penggunaan internet ini memiliki potensi yang berbanding lurus dengan adanya serangan siber yang dapat mempengaruhi keamanan dan perkembangan dari ekosistem digital serta menimbulkan ancaman, tantangan yang berdampak besar bagi suatu negara. BSSN menyoroti keamanan siber sebagai isu yang serius saat pandemi ini karena telah menjadi pemicu berbagai jenis serangan siber dan penyebaran informasi yang tidak benar (disinformasi).

1.1.1. Penetrasi Internet dan Revolusi Industri 4.0

Berdasarkan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2019 hingga kuartal II tahun 2020, Indonesia memiliki pengguna internet aktif sebanyak 196,7 (seratus sembilan puluh enam koma tujuh) juta jiwa atau setara 73,7% (tujuh puluh tiga koma tujuh per seratus) dari total populasi Indonesia. Persentase penetrasi internet dijelaskan pada Gambar 1.1.

Sumber: Laporan Survei APJII Tahun 2019-Q2 2020

Gambar 1.1 Kontribusi Pengguna Internet per Wilayah

Perkembangan Teknologi Informasi dan Komunikasi (TIK) telah mendorong lahirnya Revolusi Industri 4.0 yang ditandai dengan berkembangnya teknologi-teknologi seperti kecerdasan buatan, *Internet of Things* (IoT), robotika canggih, dan 3D *printing* yang dimanfaatkan di

berbagai bidang. Penetapan roadmap "Making Indonesia 4.0" menjadi salah satu inisiatif lintas sektornya yaitu pembangunan infrastruktur digital nasional, memaksa Indonesia untuk siap dalam memasuki era industri 4.0 dan implementasinya.

Pada sektor pemerintahan, transformasi digital merupakan upaya dalam mengoptimalkan pelayanan publik. Transformasi digital dalam penyelenggaraan pemerintahan juga mencakup bagaimana mengintegrasikan seluruh area layanan sehingga mampu menciptakan suatu nilai tambah yang memberikan kepuasan kepada masyarakat sebagai pengguna layanan melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Keamanan SPBE merupakan salah satu dari lima domain dalam penyelenggaraan SPBE yang mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, kenirsangkalan sumber daya terikat data dan informasi, infrastruktur SPBE, dan aplikasi SPBE.

Pada sektor infrastruktur vital, revolusi industri 4.0 telah memberikan banyak manfaat dalam hal menjalankan operasional layanannya khususnya dalam hal pengoperasian sistem kontrol, misalnya teknologi operasional seperti *Industrial Control System (ICS)* yang di dalamnya mencakup *Supervisory Control Data Acquisition (SCADA)*. Keterhubungan sistem operasional teknologi dengan internet telah membantu memperluas operasi, meningkatkan operabilitas antar *platform*, dan memudahkan akses namun kemudahan ini juga inheren dengan kerentanan apabila praktik keamanan siber tidak diterapkan dengan baik.

Dalam aktivitas perekonomian, meningkatnya digitalisasi, otomatisasi, dan penggunaan kecerdasan buatan akan mendorong produktivitas dan efisiensi sehingga berdampak pada peningkatan pertumbuhan ekonomi nasional dan daya saing global. Perkembangan ekonomi digital di Indonesia diproyeksikan tumbuh pesat dan eksponensial. Berdasarkan laporan *e-Conomy SEA* pada tahun 2020 yang dipublikasikan *Google, Temasek dan Bain&Company*, nilai transaksi ekonomi digital Indonesia diperkirakan mencapai US$ 124 (seratus dua puluh empat) miliar atau sekitar Rp. 1.740 (seribu tujuh ratus empat puluh) triliun pada tahun 2025. Hal ini tidak terlepas dari pesatnya pertumbuhan perusahaan rintisan (*start-up*) di Indonesia yang menempati urutan kelima di dunia dengan jumlah *startup* mencapai 2.239 (dua ribu dua ratus tiga puluh sembilan) pada bulan Juni 2021.

Dalam hal penyelenggaraan ekonomi digital, salah satu fondasi yang penting adalah penjaminan keamanan informasi suatu sistem elektronik yang aman dan andal sesuai dengan standar keamanan yang berlaku.

Peningkatan penetrasi internet serta perkembangan revolusi industri 4.0 yang begitu pesat ini menimbulkan tantangan baru sekaligus risiko yang harus diantisipasi dan dikelola dengan baik, diantaranya adalah terkait dengan pentingnya penanganan dan penyelesaian kejahatan siber, penyimpanan data pribadi, pengamanan sistem elektronik yang handal, pengelolaan keamanan aplikasi, serta yang tidak kalah penting adalah kesadaran akan keamanan informasi (*security awareness*), dimana pemangku kepentingan perlu mengetahui adanya ancaman keamanan siber dan urgensinya untuk memperhatikan aspek keamanan siber baik melalui perangkat yang dimiliki maupun sistem elektronik yang terhubung.

1.1.2. Ancaman di Ruang Siber

Ruang siber merupakan sebuah domain global yang terhubung melalui interaksi antar elemen-elemen pada infrastruktur TIK. Ruang siber terbentuk karena adanya sistem elektronik yang terhubung dengan internet, yang memiliki beragam kepentingan di ruang siber meliputi : 1) sektor pemerintahan yang terdiri atas 34 (tiga puluh empat) kementerian, 53 (lima puluh tiga) lembaga, 97 (sembilan puluh tujuh) lembaga non struktural, 8 (delapan) lembaga negara, 5 (lima) lembaga lainnya setingkat Menteri, 34 (tiga puluh) provinsi, dan 514 (lima ratus empat belas) kabupaten/kota, 115 (seratus lima belas) Badan Usaha Milik Negara (BUMN) dengan lebih dari 600 (enam ratus) anak perusahaan BUMN; 2) Infrastruktur Informasi Vital yang selanjutnya disebut IIV terdiri atas 11 sektor yaitu Administrasi Pemerintahan, Energi dan Sumber Daya Mineral, Transportasi, Keuangan, Kesehatan, Teknologi Informasi dan Komunikasi, Pangan, Pertahanan; dan 3) 196,7 (seratus sembilan puluh enam koma tujuh) juta para pengguna internet.

Alur komunikasi internet antar entitas dapat dilayani oleh jalur *Internet Exchange* lokal yang disebut *Indonesia Internet Exchange* (IIX). Untuk hubungan antara entitas ke jaringan internet internasional, alur datanya adalah entitas ke *Internet Service Provider* (ISP) kemudian ke *Network Access Provider* (NAP) dan diteruskan ke jaringan internasional, sebagian besar menggunakan *Internet Exchange* (IX), namun sebagian lain dapat dialirkan langsung dari NAP ke jaringan internet

internasional. Indonesia memiliki 605 (enam ratus lima) ISP, 76 (tujuh puluh enam) NAP dan 14 (empat belas) Indonesia IX. Seluruh sektor di Indonesia terhubung melalui internet menggunakan jasa dari ISP. ISP menyediakan layanan internet berdasarkan jaringan yang dimiliki NAP.

Internet di Indonesia dihubungkan oleh kabel serat optik 342.239 (tiga ratus empat puluh dua ribu dua ratus tiga puluh sembilan) Km dan jumlah BTS kurang lebih 374.520 (tiga ratus tujuh puluh empat ribu lima ratus dua puluh) tower. Trafik internasional sejumlah 25 (dua puluh lima) TBps dan trafik lokal sejumlah 6 (enam) TBps. Perbedaan jumlah yang besar tersebut dikarenakan trafik internasional memiliki beragam jenis data yang diakses dengan ukuran yang besar pula seperti *file video*.

Ruang siber juga dapat dilihat sebagai penggabungan dari individu, organisasi, dan sistem yang mengumpulkan, memproses, menyebarkan, dan bertindak atas informasi terkait, serta bergantung pada domain fisik lainnya seperti darat, udara, laut, dan ruang angkasa. Ruang siber Indonesia diilustrasikan pada Gambar 1.3.

Gambar 1.2 Ruang Siber Indonesia

Ketergantungan antara komponen dalam struktur ruang siber terdiri atas tiga lapisan: lapisan fisik, lapisan jaringan logika, dan lapisan sosial.

Gambar 1.3 Lapisan Ruang Siber

Lapisan pertama adalah lapisan fisik yang terdiri atas dua komponen utama, yaitu komponen geografis dan komponen jaringan fisik (perangkat keras dan infrastruktur). Lapisan ini perlu dilindungi agar tidak terjadi kerusakan fisik pada perangkat dan infrastruktur terkait, dan juga tidak terjadi pelanggaran akses secara ilegal ke perangkat dan infrastruktur terkait yang dapat mengakibatkan kegagalan operasional pada perangkat dan infrastruktur tersebut. Lapisan kedua adalah lapisan jaringan logika yang terdiri atas serangkaian hubungan logika yang saling berkaitan. Lapisan ini umumnya disebut sebagai perangkat lunak (*software*) yang terkoneksi dengan perangkat keras (*hardware*). Lapisan ketiga adalah lapisan sosial yang pada hakikatnya adalah lapisan tentang manusia dan aspek-aspek kognitifnya (hati dan pikiran). Lapisan ini terdiri atas dua komponen utama yaitu komponen persona dan komponen siber-persona. Adapun komponen persona merupakan subyek manusia atau aktor sesungguhnya yang berada di dalam sistem jaringan di ruang siber, sementara komponen siber-persona merupakan perpanjangan dari lapisan logika yang menjadi perwakilan digital atau identitas pengguna dari subyek manusia/aktor yang berada di dalam sistem jaringan ruang siber tersebut.

Ancaman di ruang siber atau biasa disebut ancaman siber merupakan keinginan dan kemampuan pihak tertentu, baik aktor negara maupun aktor non-negara, yang mempunyai potensi dan kemungkinan untuk bermanifestasi dalam bentuk serangan di ruang siber yang terdiri atas tiga lapisan. Sementara itu, serangan siber atau serangan di dalam ruang siber atau serangan melalui ruang siber dapat didefinisikan sebagai upaya aktif pihak tertentu dengan keinginan, tujuan, dan kemampuan untuk merusak dan menimbulkan kerugian pada pihak yang diserang.

Serangan siber dapat bermanifestasi menjadi serangan bersifat teknis dan sosial. Serangan siber bersifat teknis merupakan serangan yang ditujukan untuk menyerang lapisan kedua ruang siber, yaitu jaringan logika, melalui metode-metode teknis yang intrusif dengan tujuan mendapatkan akses ilegal ke dalam jaringan dan sistem ruang siber pihak sasaran guna menghancurkan, mengubah, mencuri atau memasukkan informasi, yang mana akhirnya berdampak pada lapisan pertama dan lapisan ketiga di ruang siber. Sedangkan serangan siber yang bersifat sosial merupakan upaya mempengaruhi manusia di ruang siber erat kaitannya dengan peperangan politik, peperangan informasi, peperangan psikologi, dan propaganda. Target utama serangan siber yang bersifat sosial adalah lapisan ketiga ruang siber, yaitu cara pikir, sistem kepercayaan, dan sikap tindak dari manusia yang berinteraksi dengan ruang siber. Senjata utama serangan siber yang bersifat sosial adalah rekayasa informasi guna mendukung dan memperbesar dampak dari aktivitas lainnya yang dilakukan oleh pihak penyerang.

Berubahnya tren peperangan dari fisik menjadi non fisik atau dari konvensional menjadi modern, menjadikan ruang siber sebagai ancaman baru bagi negara terlebih pada Infrastruktur Vital Nasional, yang memiliki fungsi menunjang hajat hidup orang banyak. Gangguan, kerusakan, dan/atau kehancuran pada infrastruktur vital ini dapat berdampak pada pertahanan dan keamanan nasional, ekonomi nasional, kesehatan, keselamatan publik, penyelenggaraan negara, pelayanan publik, merusak reputasi negara dan hilangnya kepercayaan publik, maupun dampak lain yang berupa kombinasi dari hal-hal tersebut.

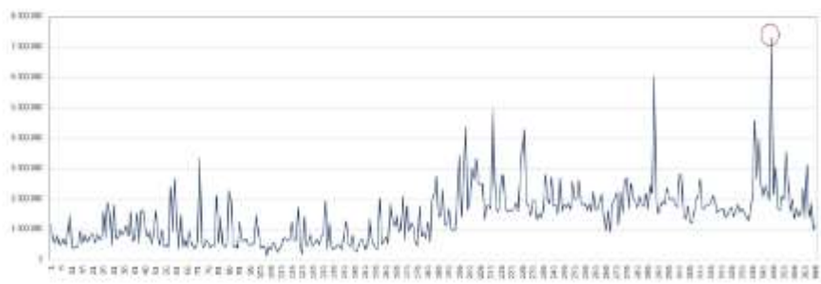
Serangan siber terhadap infrastruktur vital terus mengalami peningkatan, diantaranya adalah kejadian di Estonia pada Tahun 2007 dan Georgia pada Tahun 2008 yang menyebabkan perekonomian negara tersebut lumpuh beberapa waktu. Serangan siber lainnya terjadi pada infrastruktur nuklir di Iran oleh *Stuxnet* pada tahun 2010 dengan menginfeksi lebih dari 60.000 (enam puluh ribu) komputer yang merupakan setengah jumlah komputer yang ada di Iran yang dampaknya menyebar sampai ke Indonesia. Seperti dilansir oleh *Symantec*, Indonesia berada pada urutan kedua setelah Iran di antara 10 (sepuluh) besar negara yang mengalami serangan *Stuxnet*.

Pada tahun 2017, Indonesia mengalami insiden berupa serangan *ransomware wannacry* yang menyerang Rumah Sakit Harapan Kita dan

Dharmais Jakarta. *Malware* ini menyerang ratusan *server* dan komputer dengan mengunci sistem dan data pasien serta meminta sejumlah uang sebagai tebusan sehingga mengakibatkan terganggunya operasional dan pelayanan pengobatan rumah sakit. Melihat dari beberapa kasus insiden siber pada infrastruktur vital yang berdampak tidak hanya pada operasional tetapi juga memiliki efek domino terhadap layanan elektronik lainnya, maka bentuk perlindungan terhadap infrastruktur vital saat ini bukan hanya terbatas pada perlindungan infrastruktur fisik tetapi juga meliputi perlindungan infrastruktur informasi.

Indonesia merupakan salah satu negara yang menjadi sasaran serangan siber, seperti laporan dari Interpol yang mengutip data dari *Kaspersky* tahun 2020 bahwa terdapat sekitar 2,7 (dua koma tujuh) juta hitungan deteksi *ransomware* di ASEAN selama tiga kuartal pertama sepanjang tahun 2020 pada kondisi pandemi *covid-19*, dan Indonesia menjadi salah satu negara paling parah terkena dampak yaitu dengan 1,3 (satu koma tiga) juta hitungan. Nilai tersebut terhitung hampir setengah dari seluruh deteksi *ransomware* di wilayah di ASEAN pada tahun 2020.

Berdasarkan data hasil *monitoring* serangan siber oleh Pusat Operasi Keamanan Siber Nasional selama 7 x 24 jam yang dilakukan mulai tanggal 1 Januari 2020 pukul 00:00:00 hingga tanggal 31 Desember 2020 pukul 23:59:59, total serangan siber di tahun 2020 diketahui sebanyak 495.337.202 (empat ratus sembilan puluh lima juta tiga ratus tiga puluh tujuh ribu dua ratus dua), dengan serangan siber tertinggi terjadi pada tanggal 10 Desember 2020 dengan jumlah mencapai 7.311.606 (tujuh juta tiga ratus sebelas ribu enam ratus enam) serangan yang ditunjukkan pada Gambar 1.4.



Gambar 1.4 Grafik Serangan Siber Sepanjang Tahun 2020

Pada masa pandemi *covid-19*, meningkatnya keresahan masyarakat atas penyebaran virus *covid-19* mengakibatkan para

pelaku ancaman siber untuk memanfaatkan hal tersebut untuk menyebarkan aplikasi ataupun situs terkait informasi *covid-19* namun telah ditambahkan fungsi berbahaya bagi penggunanya. *Malware* ini memanfaatkan potensi keingintahuan atau kepanikan masyarakat dalam situasi pandemi sebagai pembuka jalan untuk melakukan intrusi yang tidak sah pada suatu infrastruktur TI melalui penyebaran *malware*, virus, *ransomware* serta spam email sehingga upaya pencurian data sensitif atau insiden siber lainnya bisa lebih mudah dilakukan. Pada tahun 2020, insiden *data breach* menjadi topik besar di Indonesia sejak bocornya data berupa identitas pengguna salah satu *e-commerce* Indonesia. Menindaklanjuti isu-isu tersebut BSSN secara aktif melakukan kampanye literasi keamanan siber melalui berbagai media serta mengonsolidasikan langkah mitigasi kepada pihak-pihak yang mengalami insiden siber.

Pada sektor perekonomian, serangan atau kejahatan siber memberikan dampak berupa kerugian finansial yang cukup besar kepada suatu negara. Sebuah Studi *Frost & Sullivan* yang diprakarsai oleh *Microsoft* pada tahun 2017 mengungkapkan bahwa potensi kerugian ekonomi yang diakibatkan insiden siber di Asia Pasifik diperkirakan mencapai 7% (tujuh per seratus) dari total GDP atau setara US$ 1.745 (seribu tujuh ratus empat puluh lima) triliun. Indonesia sendiri diperkirakan mengalami kerugian ekonomi akibat insiden siber sebesar US$ 34,2 (tiga puluh empat koma dua) miliar atau 3,7% (tiga koma tujuh per seratus) dari PDB Indonesia. Namun, nilai tersebut diyakini hanya sebagian dari total kerugian yang terjadi atau umum disebut fenomena gunung es karena selain kerugian ekonomi, organisasi yang mengalami insiden siber juga harus menghadapi kerugian secara tidak langsung seperti kehilangan reputasi, pelanggan, kehilangan peluang pengembangan perusahaan, kehilangan pekerja serta dampak sistemik lainnya. Di sisi lain, penelitian yang dilakukan oleh *Palo Alto*, selama periode 2019-2020 menunjukkan bahwa sekitar 84% (delapan puluh empat per seratus) dari perusahaan di Indonesia telah meningkatkan pengalokasian anggaran di bidang keamanan siber.

Adanya Peraturan Pemerintah (PP) Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE) mengamanatkan bahwa penyelenggara jasa sistem pembayaran wajib mematuhi standar level keamanan Sistem Elektronik sesuai dengan ketentuan peraturan

perundang-undangan yang ditetapkan oleh BSSN, Gubernur BI, dan/ atau Ketua Otoritas Jasa Keuangan. PP Nomor 80 Tahun 2019 memberikan kepastian hukum bagi kegiatan industri *e-commerce* di Indonesia dan berorientasi pada perlindungan konsumen, dengan demikian BSSN harus hadir dan berkontribusi melalui penguatan regulasi keamanan siber terkait penyelenggaraan PMSE.

Sementara itu, dari sisi serangan siber bersifat sosial, pemerintah Indonesia juga mencatat tingginya kuantitas dan kualitas serangan siber sebagaimana terlihat pada dinamika aktivitas masyarakat Indonesia dalam hal membuat, menyimpan, dan menyebarkan informasi melalui ruang siber, dan juga implikasinya ke dalam perilaku masyarakat di tingkat nasional yang berdampak kepada kepentingan keamanan nasional. Serangan siber bersifat sosial dengan target *social networking* seperti *social cognitive hacking*, *social hacking*, *pseudo-social hacking*, disinformasi, pemalsuan dan pembocoran, *villages of evidence*, identitas palsu, *trolling* and *filming*, serta *humor* and *memes*. Ancaman ini membahayakan persatuan Indonesia yang ada pada Pancasila sebagai ideologi dan falsafah serta pusat kekuatan Bangsa Indonesia (*Center of Gravity*). Berdasarkan laporan Kementerian Komunikasi dan Informatika (Kemenkominfo) terdapat kasus berita bohong atau hoaks sebanyak 5.156 (lima ribu seratus lima puluh enam) kasus (mulai Agustus 2018 hingga Maret 2020). Selain itu sejak Januari hingga Oktober 2020 terdapat 2020 (dua ribu dua puluh) permintaan untuk penutupan/penurunan konten hoaks terkait *covid-19* kepada Kemenkominfo. Sedangkan berdasarkan Patroli Siber Kepolisian Negara Republik Indonesia sejak bulan Januari hingga Desember 2020 menunjukkan bahwa penyebaran konten provokatif berjumlah 1.048 (seribu empat puluh delapan) laporan, diikuti dengan laporan penipuan *online* sebanyak 649 laporan, akses ilegal sebanyak 138 (seratus tiga puluh delapan) laporan, pencurian data 39 (tiga puluh sembilan) laporan, manipulasi data sebanyak 71 (tujuh puluh satu) laporan, intersepsi ilegal 24 (dua puluh empat) laporan, dan peretasan sistem elektronik 18 (delapan belas) laporan.

Secara keseluruhan pemerintah Indonesia memprediksi bahwa tren serangan siber baik yang bersifat teknis maupun sosial kedepannya akan terus mengalami peningkatan yang signifikan. Untuk itu, guna memajukan kepentingan nasional di tingkat global, ruang siber tidak

cukup hanya dibangun saja, melainkan harus diikuti tiga hal lainnya, yaitu bagaimana mengamankan, menggunakan ruang siber secara maksimal, dan bagaimana memiliki kuantitas serta kualitas yang kompetitif di tingkat dunia pada seluruh lapisan ruang siber.

Selain aspek teknis, aspek kesiapan sumber daya manusia keamanan siber adalah aspek kritikal dalam membangun ketahanan keamanan siber untuk memajukan dan menumbuhkan ekonomi digital yang berperan dalam meningkatkan daya saing dan inovasi siber. Permasalahan sumber daya manusia secara umum adalah bahwa saat ini Indonesia dihadapkan pada 58.76% (lima puluh delapan koma tujuh enam per seratus) sumber daya manusia angkatan kerja merupakan lulusan SD-SMP, serta *problem mismatch* yang mencapai 63% (enam puluh tiga per seratus). Untuk itu, diperlukan suatu intervensi dalam pembangunan sumber daya manusia agar keterampilan dan kompetensi angkatan kerja Indonesia mampu bersaing. Salah satu peran strategis BSSN adalah meningkatkan kapabilitas sumber daya manusia di bidang keamanan siber dan sandi yang perlu diselaraskan dengan upaya perluasan lapangan kerja dan *skill upgrading*.

Sebuah studi yang dilakukan *International Information System Security Certification Consortium* (ISC2) menyatakan bahwa pekerja di bidang siber di seluruh dunia harus tumbuh 89% (delapan puluh sembilan per seratus) untuk memenuhi kebutuhan pekerja keamanan siber. BSSN sendiri memperkirakan total kebutuhan sumber daya manusia keamanan siber adalah 18.054 (delapan belas ribu lima puluh empat) orang untuk mengisi 9.804 (sembilan ribu delapan ratus empat) kesempatan kerja yang mencakup kebutuhan industri, pemerintah, BUMN, dan sektor lainnya. Hal tersebut menjadi tantangan bagi BSSN untuk menyiapkan sumber daya manusia Keamanan siber melalui upaya peningkatan kapabilitas sumber daya manusia serta menumbuhkan ekosistem sertifikasi sumber daya manusia melalui lembaga sertifikasi profesi keamanan siber. Salah satu upaya yang telah dilakukan BSSN pada tahun 2019 telah adalah menetapkan Peta Okupasi Nasional Keamanan Siber yang memuat 30 (tiga puluh) okupasi sebagai rujukan strategis pembangunan sumber daya manusia keamanan siber Indonesia, pembentukan sertifikasi sumber daya manusia di bidang keamanan siber, hingga bagian strategi penanggulangan insiden keamanan siber nasional.

Dalam hal peningkatan daya saing teknologi keamanan siber dan sandi, isu strategis perdagangan bebas barang dan jasa keamanan siber mengemuka pada tahun 2021 ini. Amerika melalui forum *Technical Barrier to Trade* (TbT) *World Trade Organization* (WTO) pernah mengajukan proposal kepada Indonesia untuk membahas peluang perdagangan bebas barang dan jasa keamanan siber. Sejauh ini, Indonesia (BSSN) belum memiliki regulasi yang mengatur perdagangan barang dan jasa keamanan siber. Belum ada regulasi yang mengatur kewajiban perangkat TIK harus mendapatkan sertifikasi keamanan produk sebelum diperdagangkan di Indonesia. Di samping, belum ada regulasi yang mengatur kewajiban penerapan atau penggunaan kriptografi (enkripsi) pada level kriptografi tertentu dan kewajiban sertifikasi modul sandi pada perangkat TIK sebelum diperdagangkan atau digunakan di Indonesia. Isu tersebut juga sempat mengemuka di forum *United Nation - Economic and Social Commission for Asia and the Pacific* (UN-ESCAP). Pada forum tersebut ESCAP melakukan penilaian terhadap negara Asia Pasific dalam menerapkan perdagangan bebas di negaranya masing-masing yang didalamnya juga mempertanyakan kebijakan perdagangan barang dan jasa terkait keamanan siber.

Saat ini dasar hukum yang mengatur perlindungan terhadap ruang siber di Indonesia yaitu Undang-Undang Nomor 10 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam UU ITE, Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi. Undang-undang ini memberikan perlindungan hukum untuk konten sistem elektronik dan transaksi elektronik, diantaranya mencakup aturan seperti perlindungan data pribadi, akses tidak sah terhadap sistem komputer, dan penyadapan ilegal terhadap sistem komputer. Kemudian sebagai peraturan turunan dari UU ITE, Pemerintah mengeluarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) yang memuat pengaturan aspek keamanan pada PSTE diantaranya bahwa setiap Penyelenggara Sistem Elektronik (PSE) wajib memiliki dan menjalankan prosedur dan sarana untuk pengamanan sistem elektronik dalam menghindari gangguan, kegagalan dan kerugian.

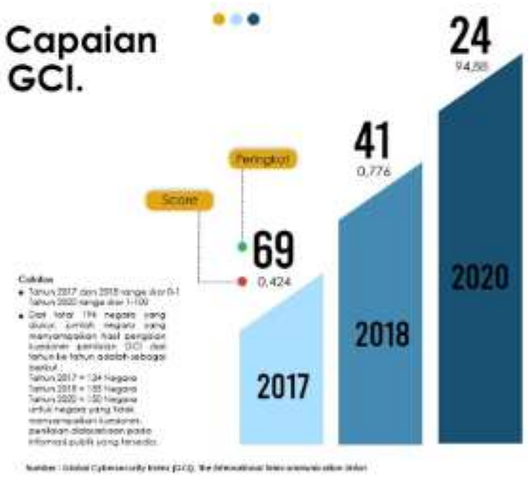
Pengaturan yang berkaitan dengan keamanan siber belum secara khusus diatur dan masih tersebar pada beberapa peraturan perundang-undangan yang bersifat parsial dan sektoral. Sedangkan, UU ITE dan PP PSTE belum secara komprehensif mengatur upaya keamanan siber yang mengaitkan antara pihak-pihak yang bertanggungjawab dalam upaya penyelenggaraan keamanan siber. Belum adanya payung hukum secara keseluruhan terkait keamanan siber menyebabkan kerangka regulasi keamanan siber saat ini masih tersebar di beberapa kementerian dan lembaga. Pada tahun 2020, Dewan Perwakilan Rakyat (DPR) menginisiasi penyusunan Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber yang termasuk dalam Program Legislasi Nasional (prolegnas) jangka menengah 2020-2024 namun pelaksanaannya ditunda untuk mendapatkan masukan terlebih dahulu dari badan legislatif, instansi pemerintah dan pemangku kepentingan lainnya. Dalam rangka penguatan regulasi perlindungan ruang siber, BSSN saat ini telah merampungkan Rancangan Peraturan Presiden Strategi Keamanan Siber Nasional (SKSN) dan Rancangan Peraturan Presiden tentang Pelindungan Infrastruktur Informasi Vital.

1.2.3. Pencapaian Kinerja BSSN Tahun 2020

Rencana Strategis BSSN Tahun 2020-2024 telah menetapkan dua tujuan BSSN, yang pertama adalah terwujudnya kedaulatan keamanan siber Indonesia dengan indikator keberhasilan berupa peningkatan skor *Global Cybersecurity Index* (GCI) dan yang kedua adalah terwujudnya tata kelola pemerintahan yang baik di BSSN dengan indikator keberhasilan berupa peningkatan Indeks Reformasi Birokrasi (Indeks RB).

GCI adalah indeks komposit yang disusun berdasarkan survei yang diselenggarakan oleh *The International Telecommunication Union* (ITU) untuk mengukur komitmen negara dalam mewujudkan keamanan siber secara nasional yang berdampak global sesuai dengan lima pilar GCI, yaitu *legal, technical, organizational, capacity development,* dan *cooperation* dengan penilaian melalui survei *online* berbasis pertanyaan. GCI bersifat *multistakeholder*, yang berarti pemenuhan inisiatif keamanan siber yang menjadi kriteria penilaian bukan hanya dari sisi pemerintah saja melainkan melibatkan banyak pihak. Sebagaimana

tercantum pada sasaran pembangunan nasional bidang keamanan siber melalui RPJMN 2020-2024, BSSN menargetkan peningkatan skor GCI dari dari 0,792 (nol koma tujuh sembilan dua) pada tahun 2020 menjadi 0,838 (nol koma delapan tiga delapan) pada tahun 2024. Pada bulan Juni tahun 2021, ITU telah mempublikasikan hasil penilaian GCI Tahun 2020 dengan hasil bahwa negara Indonesia menempati posisi ke-24 (dua puluh empat) dari 194 (seratus sembilan puluh empat) negara dengan perolehan skor sebesar 0,949 (nol koma sembilan empat sembilan) atau meningkat sebesar 0,173 (nol koma satu tujuh tiga) dari perolehan 2018. Di wilayah Asia Pasifik, Indonesia menempati ranking 6 (enam) dari 19 (sembilan belas) negara. Prestasi tersebut merupakan wujud dari semakin tingginya komitmen Indonesia dalam perannya turut menjaga keamanan siber baik secara nasional maupun global, namun dengan kenaikan yang cukup signifikan tersebut masih memerlukan serangkaian upaya dan strategi secara masif dalam mewujudkan keamanan siber di Indonesia dari ancaman siber yang semakin meningkat.



Gambar 1.5 Capaian Skor GCI Indonesia Tahun 2017 sampai dengan 2020

Merujuk pada hasil *profiling* yang dilakukan ITU, Indonesia memiliki catatan peningkatan yang semakin baik dan kuat khususnya pada area *Cooperative, Technical* dan *Capacity Development*. Sedangkan pada area *Legal* dan *Organizational* masih dibutuhkan upaya yang berkelanjutan dalam mewujudkan keamanan siber secara proporsional dan tepat guna, diantaranya melalui inisiatif perumusan peraturan dan kebijakan mengenai pencurian identitas serta data secara *online*,

penyusunan peraturan dan kebijakan mengenai pelecehan, disamping peraturan yang sudah ada terkait kekerasan dan pencemaran nama baik, serta pengesahan dan penerapan peraturan tentang Strategi Keamanan Siber Nasional (SKSN). SKSN meliputi pengaturan tentang pengamanan Infrastruktur Informasi Vital dan pemenuhan *cybersecurity resilience*, peningkatan dukungan pemerintah pada program pendidikan keamanan siber pada kurikulum sekolah dasar, sekolah menengah, dan pendidikan tinggi, dan pemenuhan sertifikasi untuk *Computer Security Incident Response Team* (CSIRT) nasional dan CSIRT sektoral yang diakui secara internasional.

Pencapaian indikator tujuan BSSN tersebut di atas, didukung oleh sasaran strategis BSSN dan indikatornya dengan hasil capaian kinerja sebagaimana pada Tabel 1.1

Tabel 1.1 Capaian Kinerja BSSN 2020

Sasaran Strategis		Indikator Sasaran Strategis		2020	
				Target	Realisasi
1	Meningkatnya Maturitas Keamanan Siber di Indonesia	1.1	Tingkat Maturitas Objek Keamanan Siber	Level II	Level IV
2	Terwujudnya Penyelenggaraan Keamanan Siber dan Sandi yang Prima	2.1	Persentase Pemenuhan Layanan Keamanan Siber dan Sandi yang Prima	90%	95,04%
3	Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien dan Berorientasi pada Pelayanan Publik	3.1	Indeks Reformasi Birokrasi	70,01	76,27

Sumber: Laporan Kinerja BSSN Tahun 2020

Pencapaian sasaran strategis Meningkatnya Maturitas Keamanan Siber di Indonesia dengan indikator Tingkat Maturitas Objek Keamanan Siber Tahun 2020 mencapai Level IV yang dapat diartikan bahwa

penerapan keamanan siber pada sektor pemerintah, IIV dan ekonomi digital secara umum telah terorganisir dengan baik. Perbaikan yang perlu dilakukan dalam meningkatkan sasaran strategis adalah dengan segera menyelesaikan payung hukum sebagai landasan pelaksanaan implementasinya serta membangun instrumen pengukuran. Pelaksanaan penilaiannya perlu dilakukan secara berulang sehingga terlihat peningkatan pengelolaan keamanan siber yang dilakukan oleh pemangku kepentingan, dan perlu adanya proses reviu secara berkala, serta implementasi perbaikan yang dilakukan secara berkelanjutan.

Pemenuhan layanan keamanan siber dan sandi yang prima pada tahun 2020 mencapai 95% (sembilan puluh lima per seratus) dari target 90% (sembilan puluh per seratus). Pemenuhan layanan keamanan siber dan sandi dimaksud merupakan upaya pemenuhan kebutuhan pengguna layanan keamanan siber dan sandi meliputi layanan bidang identifikasi, deteksi, proteksi, penanggulangan pemulihan, pemantauan dan pengendalian, dan operasi keamanan siber yang sesuai standar layanan BSSN yang didefinisikan. Untuk peningkatan capaian kinerja secara berkelanjutan, BSSN perlu melakukan monitoring dan evaluasi layanan secara berkala guna perbaikan dan peningkatan kualitas layanan selanjutnya, serta memperhatikan aspek pemenuhan dan penetapan standar layanan.

Dalam hal penyelenggaraan reformasi birokrasi, BSSN berhasil meningkatkan kualitas penyelenggaraan tata kelola pemerintahan yang baik dengan nilai Indeks RB sebesar 76,27 (tujuh puluh enam koma dua tujuh) atau kategori "BB", dimana dalam perumusan nilai tersebut terdapat penyesuaian metode evaluasi reformasi birokrasi yang merujuk pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 26 Tahun 2020 Pedoman Evaluasi Pelaksanaan Reformasi Birokrasi. Langkah strategi yang dilakukan BSSN selanjutnya dalam rangka meningkatkan kualitas reformasi birokrasi adalah melakukan reviu dan penyesuaian target indeks RB tahun 2020-2024 dengan tetap memperhatikan hal-hal yang telah dicapai pada pelaksanaan reformasi birokrasi tahun sebelumnya. Pencapaian indeks RB yang melebihi dari target ini tidak terlepas dari berbagai inisiatif penataan pada delapan area perubahan reformasi birokrasi sebagaimana tertuang dalam *Roadmap* Reformasi Birokrasi BSSN Tahun 2020-2024 yang diimplementasikan dan dimonitoring secara periodik. Inisiatif

lainnya dalam hal tata kelola pemerintahan adalah BSSN melakukan upaya peningkatan kualitas pelaporan keuangan, hal ini ditunjukan dengan perolehan Opini Wajar Tanpa Pengecualian (WTP) dari Badan Pemeriksa Keuangan (BPK) atas Laporan Keuangan BSSN Tahun 2020.

Pencapaian BSSN lainnya dalam hal peningkatan tata kelola pemerintahan adalah BSSN berhasil memperoleh penghargaan predikat Zona Integritas Wilayah Bebas Korupsi (WBK) dan Wilayah Birokrasi Bersih dan Melayani dari Kemenpan RB melalui unit kerja Balai Sertifikasi Elektronik (BSrE). Dalam hal pengelolaan sumber daya manusia, BSSN pada BKN *Award* Tahun 2021 berhasil meraih peringkat pertama untuk lembaga negara/ lembaga tinggi negara/ lembaga pemerintah non kementerian Tipe B pada kategori perencanaan kebutuhan, pelayanan pengadaan, kepangkatan dan pensiun.

Dalam RPJMN Tahun 2020-2024 agenda pembangunan penguatan stabilitas politik, hukum, pertahanan dan keamanan 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. Pelaksanaan agenda pembangunan nasional tersebut diperkuat dengan adanya *major project* bidang keamanan siber adalah Penguatan NSOC-SOC dan Pembentukan 121 (seratus dua puluh satu) CSIRT Kementerian/ Lembaga/ Daerah (K/L/D) yang kemudian dijabarkan ke dalam *output* prioritas nasional sebagaimana matriks RPJMN 2020-2024 dan diimplementasikan setiap tahunnya dalam kerangka Rencana Kerja Pemerintah (RKP). Berikut adalah pencapaian RKP dan kegiatan prioritas BSSN lainnya Tahun 2020:

a. Penguatan Infrastruktur Keamanan Siber

Dalam rangka mengantisipasi dan mengatasi terjadinya serangan siber, BSSN melakukan upaya penguatan NSOC dan SOC untuk memperluas cakupan area monitoring terhadap lalu lintas dan konektivitas internet yang berasal atau menuju Indonesia dalam upaya untuk turut mengamankan penyelenggaraan layanan berbasis protokol internet di Indonesia. Adapun dukungan kegiatan monitoring BSSN yang telah dicapai antara lain perlindungan dan monitoring keamanan siber pada sistem elektronik Komisi Pemilihan Umum (KPU) yang digunakan pada Pemilihan Umum Kepala Daerah secara serentak Tahun 2020, memberikan notifikasi terkait

permasalahan kebocoran data yang terjadi pada kementerian/ lembaga atau Instansi di Indonesia, memberikan asistensi terkait dengan tanggap insiden kasus peretasan *website*, berkolaborasi dengan pemangku kepentingan dalam hal penelusuran pelaku peretasan, pencarian kerentanan keamanan secara aktif pada *platform* aplikasi generik yang umum digunakan di Indonesia, berkolaborasi dengan Tim Tanggap Insiden Keamanan Siber baik pada lingkup bilateral, regional, maupun internasional, serta membangun kewaspadaan situasional keamanan siber.

Pada tahun 2020, BSSN telah melakukan perluasan cakupan NSOC pada empat titik NAP/ISP dan Pembangunan Kapabilitas *National Computer Security Incident Response Team* (Nat-CSIRT). Perluasan cakupan NSOC dilakukan untuk meningkatkan kapasitas monitoring ancaman keamanan siber. Data hasil monitoring berupa kerawanan dan serangan siber yang terjadi pada infrastruktur telekomunikasi ditindaklanjuti oleh unit kerja terkait di BSSN dalam upaya proteksi ataupun penanganan dan penanggulangan terhadap kerusakan maupun kelumpuhan sistem siber pemangku kepentingan. Perluasan cakupan NSOC ditargetkan selesai pada tahun 2024 yang mencakup 34 (tiga puluh empat) titik di seluruh Indonesia.

b. Pembangunan dan penguatan CSIRT

Pembentukan tim respon insiden/ CSIRT di Instansi Pemerintah dilaksanakan dalam rangka peningkatan maturitas keamanan siber di bidang penanggulangan dan pemulihan. Pada tahun 2020, Target pembentukan CSIRT ditetapkan berdasarkan Surat Kepala BSSN Nomor 4328/KBSSN/D3/PP.01.07/11/2019 tanggal 29 November 2019 tentang Penunjukkan 5 (lima) Instansi Pemerintah Pusat dan 10 Instansi Pemerintah Daerah sebagai *pilot project* Pembentukan CSIRT Tahun 2020. Dengan terbentuknya CSIRT ini diharapkan dapat meningkatkan penilaian GCI pada indikator *National/Government Computer Emergency Response Team* (CERT)/ *Computer Incident Response Team* (CIRT)/ CSIRT di dalam pilar *Technical Measures*. Pembentukan CSIRT dilakukan secara bertahap mulai tahun 2020 sampai tahun 2024 dimana pada tahun 2024 ditargetkan telah terbentuk pada seluruh Kementerian/Lembaga dan Daerah.

Selain CSIRT organisasi, pada tahun 2020 BSSN berhasil mendorong dan mengasistensi terbentuknya 2 (dua) CSIRT Sektoral yang terdiri atas 1 (satu) CSIRT di sektor Perbankan dan 1 (satu) CSIRT di sektor akademik.

c. Penguatan Regulasi Strategis Keamanan Siber dan Sandi

Pada tahun 2020, BSSN menyusun dua regulasi strategis berupa Rancangan Peraturan Presiden Strategi Keamanan Siber Nasional yang memuat visi, misi, landasan pelaksanaan, peran pemangku kepentingan, dan fokus area kerja dalam rangka membentuk ekosistem lingkungan strategis yang menguntungkan guna mempertahankan dan memajukan kepentingan nasional di tingkat global melalui perwujudan keamanan siber nasional. Saat ini permohonan izin prakarsa dalam telaahan Sekretariat Kabinet. Regulasi strategis lainnya adalah Rancangan Peraturan Presiden Tentang Pelindungan Infrastruktur Informasi Vital yang saat ini dalam tahap pembahasan Rapat Panitia Antar Kementerian. Selain dua regulasi strategis di atas, BSSN melakukan penyusunan Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik sebagai tindak lanjut dari PP PSTE. BSSN mendorong penerapan Standar Manajemen Pengamanan Informasi melalui bimbingan teknis Indeks Keamanan Informasi (KAMI) kepada lebih dari 1000 (seribu) PSE dan asistensi *assessment* sebanyak 61 (enam puluh satu) PSE.

d. Penguatan Kerja Sama Internasional dan Diplomasi Siber

Ranah kerja sama di bidang keamanan siber umumnya mencakup pelindungan sektor pemerintah, infrastruktur informasi vital, ekonomi digital, penanganan insiden, pembangunan kapasitas, penanganan kejahatan siber dan terorisme siber, termasuk didalamnya penerapan norma siber tentang perilaku negara yang bertanggung jawab. Kerja sama ini memberikan manfaat dalam peningkatan Kapasitas Siber Indonesia melalui beragam kegiatan *visit*, dialog, *workshop*, *training*, *information sharing*, *best practice and expert sharing*, dan lain-lain. Kerja sama yang telah dilakukan Pemerintah Indonesia dengan Pemerintah Negara lain diantaranya sebagai berikut Inggris Raya, Australia, Amerika Serikat , Belanda, dan RRT. Pada lingkup regional BSSN juga terlibat aktif dalam beberapa forum diantaranya: 1. ASEAN melalui forum *ARF on ICT*,

ANSAC, ASEAN Cyber CSS, dan lain-lain; 2. APEC melalui forum *APECTEL WG-Security Prosperity Steering Group*; dan 3. AALCO (*Asia Africa Law Consultative Organization*).

e. Penguatan Sumber Daya Manusia Bidang Keamanan Siber

Dalam hal peningkatan kapabilitas sumber daya manusia Keamanan Siber yang selaras dengan proyek Penguatan NSOC-SOC, BSSN telah menyusun peta okupasi nasional keamanan siber sebagai rujukan nasional dalam penetapan standar kompetensi yang harus dipenuhi bagi personel yang akan bekerja di bidang keamanan siber. Selain itu, BSSN telah melakukan Kerjasama dengan Kementerian Tenaga Kerja dengan hasil berupa penetapan Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang *Security Operation Center* (SOC) melalui Keputusan Menteri Tenaga Kerja (Kepmenaker) RI Nomor 391 Tahun 2020. SKKNI ini disusun berdasarkan kebutuhan industri guna memenuhi aspek '*people*' pada komponen inti pembangunan SOC yang efektif dan optimal.

Setiap tahunnya BSSN mencetak bibit unggul sumber daya manusia ahli Keamanan Siber dan Sandi melalui Politeknik Siber dan Sandi Negara (PSSN) sejumlah 75 (tujuh puluh lima) sampai dengan 100 (seratus) orang, serta melalui pelatihan teknis dan fungsional keamanan siber yang dilaksanakan di Pusat Pengembangan Sumber Daya Manusia (Pusbang SDM) BSSN, yang telah mendidik sebanyak 1.984 (seribu sembilan ratus delapan puluh empat) orang.

Dalam hal peningkatan kesiapsiagaan penanganan insiden siber pada sektor pemerintahan, IIV dan Ekonomi Digital, pada Tahun 2020 BSSN menyelenggarakan *National Cyber Exercise Drill Test* yang diikuti oleh 485 (empat ratus delapan puluh lima) orang. Kegiatan ini diharapkan meningkatkan kecepatan dan ketepatan dalam melakukan mitigasi apabila terjadi insiden siber pada masing-masing instansi/organisasi. BSSN juga secara aktif melakukan kampanye Budaya Keamanan siber serta Literasi Keamanan Siber pada tahun 2020 kepada semua pemangku kepentingan di sektor pemerintah, pelaku usaha, akademisi dan masyarakat di 24 (dua puluh empat) kota yang diikuti oleh 23.666 (dua puluh tiga ribu enam ratus enam puluh enam) peserta. BSSN juga melakukan kampanye digital Pengendalian Informasi dengan jumlah jangkauan

masyarakat yang teredukasi literasi pengendalian informasi adalah sebesar 39.853 (tiga puluh sembilan ribu delapan ratus lima puluh tiga) orang. Agar pelaksanaan kampanye Budaya Keamanan siber serta Literasi Keamanan Siber lebih terarah sesuai dengan yang diharapkan, BSSN telah menetapkan Peraturan Badan Siber dan Sandi Negara Nomor 3 Tahun 2021 tentang Penyelenggaraan Literasi Media dan Literasi Keamanan Siber. Kegiatan ini ditujukan untuk mengedukasi masyarakat dalam beraktivitas di ruang siber secara aman serta dapat memanfaatkan media sosial dengan bijak.

Dalam rangka literasi keamanan siber yang mendukung kesetaraan *gender* sesuai pengarusutamaan dalam RPJMN 2020-2024, pada tahun 2021 BSSN telah mendeklarasikan *Indonesia Women in Cybersecurity* (IWCS) yang bertujuan untuk mendorong wanita dan anak-anak perempuan untuk berperan dalam membangun keamanan siber di Indonesia melalui pilar kesadaran, pendidikan, dan *empowerment* sehingga akan menumbuhkan ekosistem dimana wanita dan laki-laki memiliki profesionalitas yang sama dalam bidang keamanan siber.

f. Penyelenggaraan Sertifikat Elektronik/ Tanda Tangan Elektronik

BSSN adalah salah satu penyelenggara sertifikat elektronik/ tanda tangan elektronik untuk mendukung penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) atau *E-Government* melalui Balai Sertifikasi Elektronik (BSrE) BSSN. Hasil implementasi Sertifikat Elektronik/Tanda Tangan Elektronik pada K/L/D telah berdampak positif dan signifikan dalam peningkatan kinerja K/L/D, antara lain: meningkatkan efektifitas dan efisiensi proses administrasi tata naskah dinas elektronik pemerintahan dan mempercepat proses perizinan pada Pelayanan Terpadu Satu Pintu (PTSP).

Hingga saat ini, BSSN telah bekerja sama dengan 328 (tiga ratus dua puluh delapan) instansi terkait layanan sertifikat elektronik dengan rincian sebagai berikut: 93 (sembilan puluh tiga) Pemerintah Pusat dan BUMN. 236 (dua ratus tiga puluh enam) Instansi Daerah dan Universitas. Hingga bulan Juni 2021 sertifikat elektronik yang telah diterbitkan sebanyak 132.650 (seratus tiga puluh dua ribu enam ratus lima puluh) sertifikat.

Pada sektor ekonomi digital, tahun 2020 BSSN melakukan Penerapan Standar Kriptografi pada Sektor Ekonomi Digital yang bersifat interoperabilitas kepada 12 (dua belas) PSE. Kegiatan ini bertujuan melengkapi sistem elektronik PSE pelaku ekonomi digital dengan standar kriptografi berupa sertifikat elektronik yang dapat melindungi dan menghindari sistem elektronik dari ancaman kejahatan siber yang mungkin timbul.

g. Peningkatan Daya Saing Teknologi dan Produk Keamanan Siber

BSSN melalui unit kerja Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi (Puskajibang) berupaya meningkatkan inovasi dan layanan teknologi dalam mendukung pengembangan industri dalam negeri di bidang teknologi keamanan siber dan sandi. Salah satu produk hasil pengkajian dan pengembangan diantaranya adalah *Secure File Encryption* (SELECTION) versi 3.0 yang telah dilakukan *pilot project* di lingkungan Sistem Komunikasi dan Informasi Ekstranet (SKIE) Kemenlu dengan 25 (dua puluh lima) Instansi Pemerintah Pusat. Puskajibang Tekamsisan juga berkontribusi dalam mendukung Prioritas Riset Nasional 2020-2024 dan Rencana Induk Riset Nasional 2020-2024 dalam tema riset Keamanan Siber dan Penanganan Disinformasi serta Rekayasa Keteknikan dengan topik/tema *Big Data* Nasional.

Selain melakukan pengkajian dan pengembangan, BSSN juga membangun kemandirian industri Teknologi Keamanan Siber melalui Program *Homegrown Cybersecurity Industry, Program Research and Development* Keamanan Siber serta *Cybersecurity Startup*. Salah satunya melalui peluncuran *CyberHub* yang telah resmi dilaksanakan pada 18 Januari 2021. *Cyberhub* bertujuan menghubungkan antara pencari kerja dan pencari tenaga kerja untuk bisa berkarir di tempat yang sesuai, membangun semangat kerjasama dan gotong royong untuk maju dan berkembang bersama untuk membangun ekosistem keamanan siber nasional, dan sebagai inkubator perusahaan rintisan atau layanan keamanan siber untuk mewujudkan kemandirian bangsa dan memperkuat ekosistem keamanan siber nasional.

Selain inisiatif di atas, BSSN juga melakukan penjaminan keamanan produk teknologi melalui Kerangka *Common Criteria* SNI

ISO/IEC 15408 *Evaluation Assurance Level* dengan sertifikasi (penerbitan sertifikat kesesuaian hasil uji) fitur keamanan produk TIK, pada tahun 2020 terdapat 1 (satu) produk tersertifikasi.

1.2.4. Pemenuhan Aspirasi Pemangku Kepentingan

Sebagai koordinator dan konsolidator berbagai pemangku kepentingan di bidang keamanan 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.

Selain itu, BSSN berperan aktif dalam memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik dari segala jenis gangguan. Sesuai PP PSTE, BSSN melalui Balai Sertifikasi Elektronik menyelenggarakan sertifikasi elektronik di sektor pemerintah, IIV dan ekonomi digital. Selain upaya tersebut, dalam rangka pengendalian informasi, BSSN juga memperhatikan tuntutan masyarakat untuk memberikan edukasi dan literasi bidang keamanan siber dan sandi, sehingga masyarakat memahami tentang urgensi suatu informasi yang dapat dipertanggungjawabkan kebenarannya dan disampaikan sesuai waktu yang dibutuhkan.

1.2. POTENSI DAN PERMASALAHAN

Identifikasi potensi dan permasalahan BSSN dilakukan dengan menganalisis kekuatan, tantangan, peluang, kelemahan dan potensi yang dihadapi BSSN dalam rangka melaksanakan amanat RPJMN 2020-2024. Berkenaan dengan hal tersebut, BSSN berupaya untuk mewujudkan 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.

Sedangkan 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.

Untuk mewujudkan kedaulatan dan kemandirian tersebut, BSSN terus berupaya untuk meningkatkan kapabilitas SDM BSSN. Saat ini, sumber daya manusia BSSN keseluruhan sejumlah 1.196 (seribu seratus sembilan puluh enam) orang personel yang terdiri atas laki-laki sebanyak 832 (delapan ratus tiga puluh dua) dan perempuan sebanyak 364 (tiga ratus enam puluh empat) orang. Jumlah tersebut belum termasuk mahasiswa sejumlah 392 (tiga ratus sembilan puluh dua) orang yang masih dalam proses mengikuti perkuliahan di Politeknik Siber dan Sandi Negara. Total jumlah sumber daya manusia BSSN terdiri atas beberapa latar belakang pendidikan yang mendukung tugas dan peran dalam perkuatan kompetensi sandiman sesuai tugas pokok dan fungsinya. Peningkatan kapabilitas akademisi sumber daya manusia BSSN terus ditingkatkan, salah satunya adalah dengan penambahan alokasi beasiswa S2 dan S3 ke beberapa universitas baik dalam maupun luar negeri. Rincian potensi sumber daya manusia BSSN dapat dilihat pada rekapitulasi dislokasi pegawai sebagai berikut:

Tabel 1.2 Dislokasi Pegawai Berdasarkan Latar Belakang Pendidikan dan Golongan

Organisasi	Golongan						Jenjang Pendidikan								Total
	IV	III	II	I	CPNS	TNI/ Polri	S3	S2	S1	D3	D1	SMA	SMP	SD	
Jumlah	81	838	179	-	84	14	6	233	642	98	4	205	5	3	1196
Persentase (%)	7	70	15	-	7	1	0,50	19,48	53,68	8,19	0,33	17,14	0,42	0,25	

Sumber : Data Kepegawaian 1 Januari 2021

Selain kemampuan yang mumpuni di bidang keamanan siber dan sandi, personel BSSN diharapkan memiliki 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 yang ditetapkan melalui Peraturan BSSN Nomor 3 Tahun 2018 tentang Sistem Nilai BSSN, sebagai berikut:

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 atas 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.

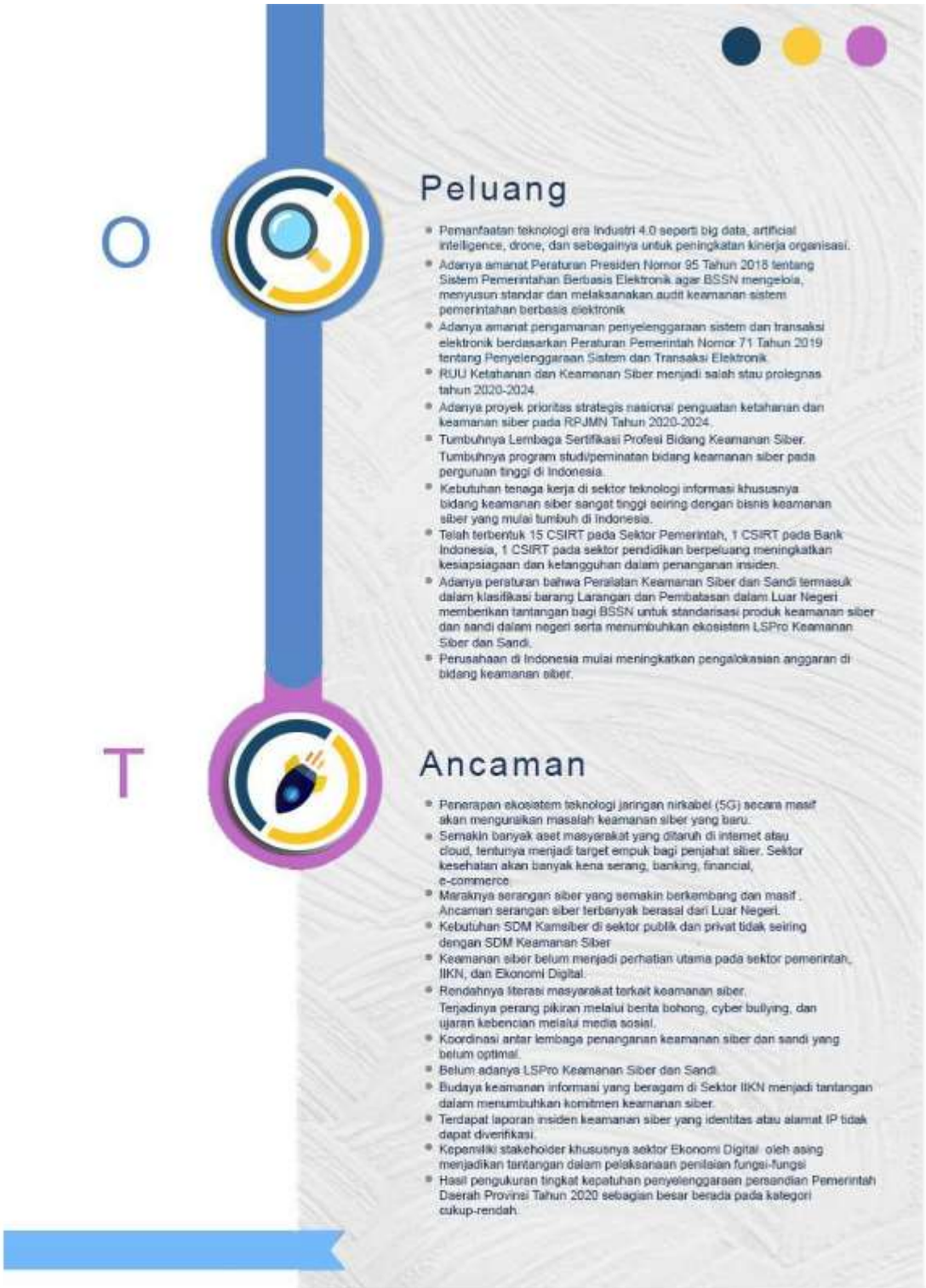
4. Tepercaya

   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, disosialisasikan, diartikulasikan, dihayati, sehingga secara keseluruhan menjadi lebih mudah pada implementasinya. Selain menjadi tata cara atau perilaku organisasi atau individu, sistem nilai juga menggambarkan kinerja dan pelayanan yang menjadi arah pengembangan kapabilitas organisasi, mencerminkan

hubungan antar unsur BSSN serta memberikan jaminan dalam pemenuhan kebutuhan dan harapan pemangku kepentingan BSSN.

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 secara ringkas ditunjukkan pada Gambar 1.6 berikut:



Gambar 1.5 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 2021–2024 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;
3. Di sisi lain, dalam rangka mendukung penyelenggaraan tugas dan fungsi BSSN tantangan yang masih dihadapi di sisi internal organisasi adalah tantangan penyelenggaraan tata kelola pemerintahan yang baik, diantaranya pada aspek perubahan *mindset* dan budaya kinerja, penataan kebijakan, kelembagaan, tatalaksana, sumber daya manusia, akuntabilitas, pengawasan demi menghasilkan peningkatan kualitas pelayanan publik BSSN kepada masyarakat dan para pemangku kepentingan.

BAB II
VISI, MISI, TUJUAN DAN SASARAN STRATEGIS BSSN

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 tepercaya;
7. perlindungan bagi segenap bangsa dan memberikan rasa aman pada seluruh warga;
8. pengelolaan pemerintahan yang bersih, efektif, dan tepercaya;
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:

   a. menyusun dan menerapkan kebijakan keamanan siber dan persandian nasional yang berkualitas;

b. 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;
c. berperan aktif dalam meningkatkan kompetensi sumber daya manusia nasional di bidang keamanan siber dan sandi serta kompetensi pendukung yang diakui secara global;
d. membangun kondisi yang aman di ruang siber;
e. menjamin perangkat teknologi yang aman;
f. 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 serta masyarakat dalam meningkatkan pertumbuhan ekonomi nasional.

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 turut aktif dalam mengamankan ruang siber di Indonesia. Tujuan Strategis ini memastikan bahwa melalui tugas dan fungsi yang dijalankan BSSN akan mengantarkannya menjadi institusi yang diakui dan menjadi referensi pada tingkat internasional. Implementasi ukuran keberhasilan BSSN dalam mewujudkan tujuan strategis pada periode pertama peta jalan sesuai dengan dokumen RPJMN 2020-2024.

Pencapaian tujuan strategis ini ditandai dengan indikator keberhasilan yaitu meningkatnya skor GCI. Berdasarkan penetapan target pada dokumen Renstra sebelumnya sebagaimana telah tertuang dalam dokumen RPJMN 2020-2024, target skor GCI pada Tahun 2020 adalah 0,792 (nol koma tujuh sembilan dua) dan diharapkan terdapat peningkatan menjadi 0,838 (nol koma delapan tiga delapan) pada tahun 2024. Namun berdasarkan hasil rilis penilaian GCI terhadap negara-negara secara global tahun 2020 yang dilakukan oleh ITU dan telah dipublikasikan pada tahun 2021, Indonesia memperoleh skor GCI 94,88 (sembilan puluh empat koma delapan delapan) atau mengalami peningkatan dari penilaian sebelumnya yaitu peringkat 41 (empat puluh satu) naik menjadi peringkat 24 (dua puluh empat) dari 194 (seratus sembilan puluh empat) negara.

Dengan melihat adanya peningkatan penilaian GCI terhadap negara Indonesia yang telah dilakukan tahun 2020, maka perlu dilakukan penyesuaian target skor GCI pada dokumenRenstra BSSN

2021-2024. Dengan mempertimbangkan komponen penilaian GCI yang bersifat dinamis dalam setiap periode pengukurannya dan dengan melihat inisiatif serta rencana aksi yang telah dan akan dilakukan BSSN serta pemangku kepentingan lainnya dalam hal upaya meningkatkan keamanan siber di Indonesia, maka pada dokumen Perubahan Renstra BSSN 2020-2024 berikut, terdapat penyesuain target skor GCI Indonesia yang tahun 2024 menjadi 90,04 (sembilan puluh koma nol empat) dengan skala yang digunakan adalah 1-100 (satu sampai seratus).

2. terwujudnya tata kelola pemerintahan yang baik di BSSN.

Modal penting dalam keberhasilan suatu organisasi meliputi tiga hal yaitu manusia, informasi, dan organisasi itu sendiri. Melalui Renstra BSSN ini, telah ditetapkan satu tujuan yang menggambarkan kekuatan organisasi berupa penguatan 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 sampai dengan saat ini yang ditunjukkan melalui adanya peningkatan indeks reformasi birokrasi dan hasil evaluasi akuntabilitas kinerja instansi pemerintah serta kematangan sistem pengawasan internal pemerintah BSSN. Melalui capaian prestasi penilaian reformasi birokrasi, BSSN terus berupaya melakukan perbaikan secara berkesinambungan dengan salah satunya adalah melakukan penyiapan pelaksanaan audit keamanan SPBE yang bertujuan dalam mendorong terwujudnya perlindungan aset teknologi, informasi dan komunikasi sehingga akan mengefisienkan birokrasi tata kelola pemerintahan dan meningkatkan kualitas pelayanan serta kepercayaan publik pada implementasi SPBE.

Implementasi ukuran keberhasilan BSSN dalam mewujudkan tujuan strategis "Terwujudnya Tata Kelola Pemerintahan yang baik di BSSN" ditandai dengan indikator tujuan adalah meningkatnya

Indeks Reformasi Birokrasi BSSN dengan penetapan target 79,04 (tujuh puluh sembilan koma nol empat) pada tahun 2021. Melalui pertimbangan serangkaian upaya dan rencana aksi yang telah dituangkan dalam roadmap reformasi birokrasi BSSN tahun 2020-2024, maka target Reformasi Birokrasi BSSN tahun 2024 adalah 86,85 (delapan puluh enam koma delapan lima).

2.4. SASARAN STRATEGIS BSSN

Dalam rangka mendukung pencapaian 2 (dua) tujuan sebagaimana disebutkan di atas, BSSN telah menetapkan 3 (tiga) sasaran strategis yang merupakan kondisi yang ingin dicapai oleh BSSN dalam kurun waktu 2021-2024. Adapun Sasaran Strategis BSSN Tahun 2021-2024 sebagai berikut:

1. Sasaran 1: Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas

Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, BSSN memiliki fungsi perumusan dan penetapan kebijakan teknis di bidang keamanan siber. kebijakan keamanan siber dan sandi adalah sikap dan langkah yang diambil BSSN dalam melakukan strategi, upaya, dan cara yang dituangkan dalam suatu kerangka regulasi dengan tujuan untuk memperkuat keamanan siber dan sandi dalam rangka mencapai tujuan nasional pada ruang lingkup keamanan negara yaitu mewujudkan keamanan siber di Indonesia secara berdaulat. Kebijakan Keamanan Siber dan Sandi merupakan seperangkat aturan dalam melindungi seluruh lapisan ruang siber termasuk data/aset informasi yang ada di dalamnya dari ancaman dan serangan siber baik bersifat teknis maupun non teknis dalam hal ini juga melalui penerapan konsep, teori, seni, dan ilmu kriptografi beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.

Penetapan sasaran strategis ini selaras dengan hasil penilaian GCI Indonesia, dimana salah satu area yang perlu dioptimalkan adalah pada area *legal measure* atau kebijakan keamanan siber. Untuk itu, BSSN sesuai tugas dan fungsinya berupaya untuk mewujudkan tersedianya kebijakan keamanan siber yang berkualitas melalui penyediaan aturan yang menjadi panduan dan rujukan bagi

pemangku kepentingan dalam menerapkan pengelolaan keamanan siber pada lingkup organisasi maupun sektor di Indonesia.

Ukuran keberhasilan BSSN dalam mewujudkan kebijakan keamanan siber dan sandi yang berkualitas ditandai dengan indikator berupa Indeks Penyelesaian Kebijakan Keamanan Siber dan Sandi. Tingkat Penyelesaian Kebijakan/Regulasi Prioritas selanjutnya diharapkan akan mendukung dan memperkuat program pemerintah melalui penyusunan kebijakan/regulasi yang andal dan sejalan dengan kebijakan simplifikasi regulasi nasional, serta dalam rangka memastikan adanya peningkatan kinerja BSSN dalam hal penyelesaian kebijakan/regulasi prioritas khususnya pada ruang lingkup keamanan siber dan sandi.

Tingkat penyelesaian kebijakan prioritas merupakan salah satu upaya dalam mendorong dan memperkuat regulasi keamanan siber dan sandi dalam bentuk penyusunan rancangan Undang-Undang, rancangan Peraturan Pemerintah, rancangan Peraturan Presiden, rancangan Peraturan Badan dan/atau rancangan peraturan internal lainnya. BSSN menetapkan target peningkatan Tingkat Penyelesaian Kebijakan Prioritas Keamanan Siber dan Sandi dari nilai 70% (tujuh puluh per seratus) pada tahun 2021 dan meningkat menjadi nilai 80% (delapan puluh per seratus) pada tahun 2024.

2. Sasaran 2: Meningkatnya Kapasitas Keamanan Siber dan Sandi

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, terdapat dua kondisi dimana diperlukan peran BSSN dalam meningkatkan pengelolaan keamanan siber baik pada skala nasional maupun lingkup sektoral. Kondisi yang pertama adalah bagaimana BSSN hadir dalam memberikan jaminan terhadap berfungsinya kerangka kerja keamanan siber di Indonesia dalam melindungi seluruh warga negara dari adanya ancaman siber yang semakin masif sehingga akan terbentuk ekosistem keamanan siber secara andal di Indonesia. Kondisi yang kedua, dalam rangka mewujudkan kondisi yang pertama tidak terlepas dari perlunya penguatan kerjasama dan kolaborasi antar pemangku kepentingan

(*quad helix*) baik pemerintah, pelaku usaha, akademisi, dan komunitas. Melalui penguatan sinergi bersama yang dilakukan antar pemangku kepentingan keamanan siber di Indonesia akan mampu mengembangkan kemampuan dalam menerapkan keamanan siber untuk menjaga dan mengelola serta melindungi aset yang dimiliki dari adanya ancaman/insiden siber. Bentuk kerjasama dan kolaborasi selanjutnya diimplementasikan melalui upaya BSSN dalam mendorong terbentuknya kematangan entitas agar dapat melakukan proses identifikasi, proteksi, deteksi, penanggulangan dan pemulihan insiden siber secara sistematis dan terstruktur. Melalui konsep peningkatan kematangan keamanan siber oleh semua pemangku kepentingan akan mewujudkan ekosistem siber yang terintegrasi, efektif, dan solid di wilayah Indonesia.

Ukuran keberhasilan BSSN dalam mewujudkan sasaran strategi meningkatnya kapasitas keamanan siber dan sandi diukur melalui 2 (dua) indikator berikut:

a. Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan

Sebagai bentuk implementasi hasil dari terselenggaranya operasi keamanan siber, keamanan dan pengendalian informasi dan sandi secara tepat guna dan sesuai dengan kebutuhan pemangku kepentingan maka terdapat parameter keberhasilan yang ditunjukkan melalui rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang dimanfaatkan yang selanjutnya hasil rekomendasi akan menjadi panduan dalam rangka perbaikan pengelolaan keamanan siber sesuai lingkup penanganannya. operasi keamanan siber dan sandi meliputi operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi.

Rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi merupakan hasil tindak lanjut berupa analisis yang disajikan kepada pemangku kepentingan berupa usulan/masukan dalam merespons suatu permasalahan tertentu sesuai dengan ruang lingkup pelaksanaan penyelenggaraan siber dan sandi dimana penyampaian usulan tersebut harus dapat memberikan bobot

atau mengandung asas kemanfaatan kepada pemangku kepentingan dalam rangka perbaikan operasional keamanan sesuai sektor atau organisasi terkait.

Berdasarkan hal tersebut, Perubahan Renstra BSSN Tahun 2020- 2024 BSSN menargetkan adanya peningkatan pemanfaatan hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi sebesar 57,71% (lima puluh tujuh koma tujuh satu per seratus) pada Tahun 2021, dan meningkat menjadi 76,01% (tujuh puluh enam koma nol satu per seratus) pada tahun 2024.

b. Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59

Kematangan Keamanan Siber diartikan sebagai kemampuan pemangku kepentingan dalam rangka penyelenggaraan keamanan siber berdasarkan proses bisnis, yaitu identifikasi kerentanan, proteksi dan penanganan insiden yang dilaksanakan secara berkesinambungan. Tingkat Maturitas Keamanan Siber menunjukkan kematangan dalam pengelolaan keamanan siber meliputi proses identifikasi, proteksi, deteksi, dan penanggulangan dan pemulihan. Tingkat Kematangan Keamanan Siber diperoleh melalui proses Evaluasi Kematangan Keamanan Siber untuk mengetahui *gap* antara kondisi pengelolaan keamanan siber saat ini dengan peraturan, standar dan panduan keamanan yang telah ditetapkan sehingga dapat dilakukan rencana tindakan untuk mendapatkan tingkat pengelolaan keamanan siber yang lebih baik.

Berdasarkan Laporan Kinerja BSSN Tahun 2020, capaian indikator kinerja Tingkat Maturitas Keamanan Siber pada sektor Pemerintah, IIV Ekonomi Digital mencapai Level IV. Pada tahun 2020, capaian indikator kinerja tingkat maturitas keamanan siber mencapai Level IV yang dapat diartikan bahwa penerapan keamanan siber pada sektor Pemerintah, IIV, dan Ekonomi Digital secara umum telah terorganisir dengan baik namun masih perlu dilakukan penerapan otomasi dalam pengukurannya, penguatan kerangka regulasi dan perlunya reviu secara berkala, serta implementasi rekomendasi perbaikan secara berkelanjutan. Penilaian tahun 2020 mencakup 17 (tujuh belas) pemangku kepentingan pada sektor Pemerintah, Infrastruktur Informasi Vital

Nasional, dan Ekonomi Digital. Jumlah ini akan terus ditingkatkan guna memperoleh gambaran kondisi keamanan siber secara menyeluruh sehingga dapat diambil langkah tepat dalam upaya peningkatan kapasitas pemangku kepentingan tiap sektor.

Pada Perubahan Renstra BSSN 2020-2024, BSSN melakukan penajaman atas indikator sehingga berubah menjadi Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59 (dua koma lima sembilan). Hal ini bertujuan untuk memberikan gambaran kondisi PSE dalam penerapan keamanan siber yang dilakukan sudah terorganisir dengan baik, bersifat formal dan dilakukan reviu secara berkala serta konsisten dalam penerapan hasil rekomendasi yang telah disampaikan verifikator. Melalui Perubahan Renstra BSSN Tahun 2020-2024, maka target yang ditetapkan BSSN pada indikator Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59 (dua koma lima sembilan) pada tahun 2021 adalah 9,6% (sembilan koma enam per seratus) dan diharapkan meningkat menjadi 100% (seratus per seratus) pada tahun 2024.

3. Sasaran 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 secara prima didukung melalui proses birokrasi yang bersih, akuntabel, berkinerja tinggi, efektif dan efisien yang bertujuan untuk mewujudkan tata kelola pemerintahan yang dinamis. Proses penerapan pada lingkup organisasi dimulai melalui menumbuhkan budaya birokrasi dalam menerjemahkan permasalahan dan kendala yang ada pada periode sebelumnya dan menjadi representasi pembelajaran bersama secara adaptif dalam mewujudkan kedaulatan siber Indonesia berkelas dunia. Keberhasilan sasaran strategis ini diukur dengan indikator reformasi birokrasi, dimana pada Perubahan Renstra BSSN Tahun 2020-2024 ditargetkan peningkatan indeks reformasi birokrasi dari 79,04 (tujuh puluh sembilan koma nol empat) pada tahun 2021, meningkat menjadi 86,85 (delapan puluh enam koma delapan lima) pada tahun 2024.

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

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

No	Tujuan	Sasaran Strategis		Indikator Kinerja	
1	Terwujudnya Kedaulatan Keamanan Siber Indonesia Indikator: (skor GCI) 2021: 79,02 2022: 87,04 2023: 88,54 2024: 90,04	1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas	1.1	Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi
		2	Meningkatnya Kapasitas Keamanan Siber dan Sandi	2.1	Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan
				2.2	Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59
2	Terwujudnya Tata Kelola Pemerintahan yang baik di BSSN Indikator: (Indeks RB) 2021: 79,04 2022: 81,81	3	Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien dan Berorientasi pada Pelayanan	3.1	Indeks Reformasi Birokrasi

	2023: 84,32 2024: 86,85		Publik		

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

3.1. ARAH KEBIJAKAN DAN STRATEGI NASIONAL

Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024, telah menjabarkan visi, misi, serta arahan Presiden ke dalam 7 (tujuh) agenda pembangunan Rencana Pembangunan Jangka Menengah Nasional (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 dan Sandi

Pada RPJMN 2020-2024, Agenda pembangunan penguatan stabilitas politik, hukum, pertahanan dan keamanan pada periode 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. Dalam mewujudkan keberhasilan pencapaian agenda pembangunan nasional tersebut, telah ditetapkan sasaran pembangunan nasional yang akan dicapai dalam periode 2020-2024 yaitu Menjaga Stabilitas Keamanan Nasional dengan salah satu

indikatornya adalah skor *GCI* Indonesia dengan target 0,838 (nol koma delapan tiga delapan) pada tahun 2024.

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

1. Penguatan infrastruktur, sumber daya manusia, dan regulasi keamanan siber;
2. Pembangunan dan penguatan Tim Cepat Tanggap Keamanan siber;
3. Pencegahan kejahatan siber dan peningkatan kerja sama internasional bidang siber; dan
4. Penyelesaian kejahatan siber.

Arah kebijakan di atas diperkuat dengan adanya *major project* penguatan ketahanan dan keamanan siber. *Major project* 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.

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

Pada RPJMN Tahun 2020-2024, BSSN menjadi pelaksana utama *Major project* Penguatan NSOC-SOC dan Pembentukan 121 (seratus dua puluh satu) CSIRT. 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 *multipemangku kepentingan* keamanan siber dalam melakukan deteksi dini serangan atau ancaman siber;
3. meningkatnya pelayanan multi pemangku *kepentingan* 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 yang dilaksanakan oleh BSSN bersama dengan Pemerintah Daerah, Polri, dan Badan Intelijen Negara. BSSN terlibat dalam 3 (tiga) proyek prioritas nasional sebagai berikut:

1. Penguatan Infrastruktur, sumber daya manusia, dan Regulasi Keamanan Siber pembangunan, dengan output prioritas yang di *tag* kepada proyek prioritas strategis nasional yaitu:

a. Perluasan Cakupan Area *National Cybersecurity Operation Center,* dengan target 34 (tiga puluh empat) titik;
b. Pembangunan Kapabilitas *National Computer Security Incident Response Team (Nat-CSIRT)* dengan target 1 (satu) sistem;
c. Pembangunan Sistem Monitoring Pengendalian Informasi, dengan target 1 (satu) sistem;
d. Penguatan *National Data Center* dengan target 1 (satu) *Data Center* berstandar internasional;
e. Pembangunan Infrastruktur *Voluntary Vulnerability Disclosure Program* (VVDP) dengan target sejumlah 1 (satu) sistem VVDP;
f. Pembangunan *Information Sharing and Analysis Center* (ISAC) dengan target 1 (satu) sistem ISAC;
g. Peningkatan kompetensi sumber daya manusia pengelola keamanan Sistem Pemerintahan Berbasis Elektronik (SPBE) pada K/L/D dengan target 600 (enam ratus) lulusan;
h. Pengembangan sumber daya manusia di Bidang Keamanan Siber K/L/D dengan target 500 (lima ratus) lulusan;
i. Penyelenggaraan Program *Born to Defence* untuk sumber daya manusia Pengelola Keamanan Siber Sektor IIV dengan target 2.500 (dua ribu lima ratus) orang;
j. *National Cyber Exercise Drill Test* [RPJMN 2020-2024] dengan target 6.630 (enam ribu enam ratus tiga puluh) orang.

2. Pembangunan dan penguatan Tim Cepat Tanggap Keamanan Siber. dengan output prioritas yang di *tag* kepada proyek prioritas strategis nasional adalah pembentukan CSIRT pada Sektor Pemerintah dengan target 34 (tiga puluh empat) CSIRT pada 121 (seratus dua puluh satu) K/L/D;
3. Pencegahan kejahatan siber dan peningkatan kerja sama internasional bidang siber, dengan output prioritas yang di *tag* kepada proyek prioritas strategis nasional adalah kerja sama regional, bilateral, dan multilateral bidang keamanan siber [RPJMN 2020-2024] dengan target sejumlah 4 (empat) kegiatan.

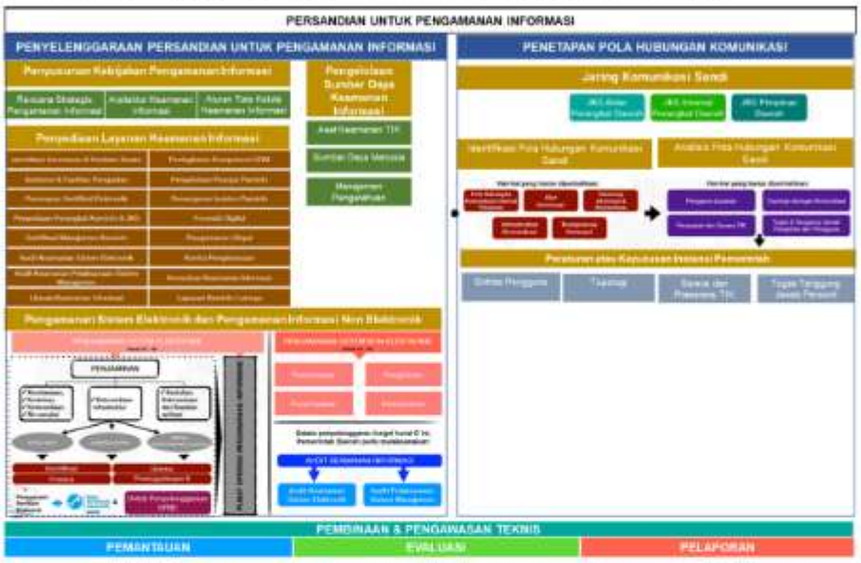
Dengan ditetapkannya BSSN sebagai pelaksana utama *major project* di atas, BSSN dituntut untuk dapat menjalin kolaborasi dengan semua pemangku kepentingan dalam membangun sistem dan tata kelola pelaksanaan penguatan keamanan siber yang terintegrasi. Fungsi BSSN yaitu menjadi pusat yang mengoordinasikan 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, Infrastruktur Informasi Vital Nasional, 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.

Major project dan indikasi pendanaannya dapat dimutakhirkan melalui Rencana Kerja Pemerintah setiap tahunnya 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. Pada tahun 2020 pelaksanaan *major project* Penguatan NSOC-SOC dan Pembentukan 121 (seratus dua puluh satu) CSIRT belum dapat memenuhi target sesuai RPJMN tahun pertama, dikarenakan adanya dampak Instruksi Presiden No 4 Tahun 2020 tentang *Refocusing* Kegiatan, Realokasi Anggaran, serta Pengadaan Barang dan Jasa dalam Rangka Percepatan Penanganan *Covid-19*, dimana BSSN mengalami *refocusing* anggaran lebih dari 50% (lima puluh per seratus). Hal ini menyebabkan beberapa output prioritas nasional perlu di *arrange* kembali target penyelesaiannya dalam periode hingga 2024 dengan tetap memperhatikan pencapaian target pada akhir RPJMN 2020-2024.

Selain mewujudkan *Major project* diatas, BSSN juga berperan mendukung *major project* prioritas nasional kelima yaitu Infrastruktur TIK untuk mendukung Transformasi Digital dengan *highlight* proyeknya adalah Penyediaan Infrastruktur SPBE yaitu dalam hal penguatan keamanan dalam Pusat Data Nasional bersama dengan Kementerian Komunikasi dan Informatika, dan Badan Pengkajian dan Penerapan Teknologi. Dalam mewujudkan dukungan stabilitas keamanan nasional, diperlukan keterlibatan aktif peran Pemerintah Daerah. Melalui

Undang-Undang Nomor 23 Tahun 2014, menjadikan persandian sebagai urusan pemerintahan konkuren yang bertujuan menyelenggarakan pengamanan informasi dan mewujudkan tata kelola secara terpadu dalam proses manajemen SPBE secara efektif, efisien, berkesinambungan, dan berkualitas. BSSN telah menyusun peraturan pelaksanaan urusan pemerintahan bidang persandian di daerah melalui Peraturan BSSN Nomor 10 Tahun 2019 seperti Gambar 3.2.



Gambar 3.2 Persandian untuk Pengamanan Informasi Pada Pemerintah Daerah

Peraturan dimaksud memuat norma, standar, prosedur, dan kriteria pelaksanaan urusan persandian. Berdasarkan Peraturan BSSN Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah menyebutkan bahwa penyelenggaraan persandian untuk pengamanan informasi dilaksanakan melalui 4 (empat) aspek yaitu :

1. penyusunan kebijakan pengamanan informasi;
2. pengelolaan sumber daya 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 hal 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 diubah 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 292 (dua ratus sembilan puluh dua) instansi dengan rincian 87 (delapan puluh tujuh) instansi pusat dan 205 (dua ratus lima) instansi daerah. Adapun jumlah sistem elektronik yang telah terintegrasi adalah sebanyak 346 (tiga ratus empat puluh enam) aplikasi. Data implementasi sertifikat elektronik pada K/L/D 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

Sistem Pemerintahan Berbasis Elektronik (SPBE) ditujukan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya. Tata kelola dan manajemen sistem pemerintahan berbasis elektronik secara nasional juga diperlukan untuk meningkatkan keterpaduan dan efisiensi sistem pemerintahan berbasis elektronik. Dalam pengelolaan SPBE, untuk meningkatkan keterpaduan pelaksanaan Tata Kelola SPBE yang didalamnya mencakup unsur Rencana Induk Nasional, Arsitektur, Peta Rencana, Rencana dan Anggaran, Proses Bisnis, Data dan Informasi, Infrastruktur TIK, Aplikasi, Keamanan Informasi, dan layanan SPBE, maka dibentuk Tim Koordinasi SPBE Nasional. BSSN tergabung dalam Tim Koordinasi SPBE Nasional dengan pada domain keamanan informasi. Sesuai dengan amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE, BSSN mempunyai 3 (tiga) tugas utama dalam mendukung program realisasi SPBE, yaitu: melaksanakan keamanan SPBE, menyusun standar keamanan SPBE Nasional, dan menetapkan manajemen dan audit keamanan SPBE. Dalam implementasinya, ruang lingkup peran BSSN dalam SPBE yaitu sebagai berikut:

1. Penyusunan Arsitektur SPBE Nasional Domain Keamanan SPBE;
2. Memberikan pertimbangan kelaikan keamanan Pusat Data Nasional, jaringan intra pemerintah, sistem penghubung layanan pemerintah dan aplikasi umum;

3. Penyusunan Peraturan tentang standar teknis dan prosedur keamanan SPBE;
4. Penyusunan Peraturan tentang Pedoman Manajemen Keamanan SPBE;
5. Koordinasi dan penyediaan layanan konsultasi penerapan keamanan dan manajemen keamanan SPBE Instansi Pusat dan Daerah;
6. Melakukan penyusunan Peraturan Kepala BSSN tentang standar tata cara pelaksanaan audit keamanan SPBE;
7. Melaksanakan audit keamanan aplikasi umum dan infrastruktur SPBE Nasional; dan
8. Melakukan koordinasi pelaksanaan audit Keamanan Aplikasi Khusus dan Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah.

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 pada RPJMN 2020-2024

a. Pengarusutamaan *Gender*

Pengarusutamaan *gender* (PUG) bertujuan untuk mewujudkan kesetaraan gender sehingga mampu mewujudkan pembangunan yang lebih adil dan merata bagi seluruh penduduk Indonesia. Kesetaraan gender dapat dicapai dengan mengurangi kesenjangan antara laki-laki dan perempuan dalam mengakses dan mengontrol sumber daya, berpartisipasi di seluruh proses pembangunan dan pengambilan keputusan, serta memperoleh manfaat dari pembangunan.

Untuk mengatasi isu keterwakilan wanita dalam bidang pekerjaan keamanan siber, tahun 2021 BSSN telah mendeklarasikan *Indonesia Women in Cybersecurity* (IWCS) bertepatan dengan peringatan dengan Hari Kartini. IWCS ini bertujuan untuk mendorong wanita dan anak-anak perempuan untuk berperan dalam membangun keamanan siber di Indonesia melalui pilar kesadaran, pendidikan, dan *empowerment* sehingga akan

menumbuhkan ekosistem dimana wanita dan laki-laki memiliki profesionalitas yang sama dalam bidang keamanan siber.

Terdapat empat program yang diusung IWCS, yakni untuk meningkatkan kesadaran (*awareness*), menyediakan edukasi, lalu *mentorship* bagi wanita yang ingin berkarier di bidang keamanan siber, dan *apprenticeship* di tempat kerja. 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 pada kondisi saat ini.

Selain program IWCS, kebijakan PUG BSSN pada periode 2021-2024 dilaksanakan dengan melanjutkan program-program yang telah dilakukan secara konsisten pada periode sebelumnya, diantaranya kesetaraan gender dalam proporsi penerimaan mahasiswa politeknik siber dan sandi negara dan pegawai BSSN. Selain itu, dalam bidang keterwakilan wanita 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.

b. Pengarusutamaan Transformasi Digital

Pengarusutamaan transformasi digital merupakan upaya untuk mengoptimalkan peranan teknologi digital dalam meningkatkan daya saing bangsa dan sebagai salah satu sumber pertumbuhan ekonomi Indonesia ke depan. Untuk itu, BSSN akan melakukan upaya peningkatan dan penerapan penyelenggaraan pemerintahan berbasis elektronik baik dalam layanan publik maupun layanan internal BSSN.

Selain itu, dalam rangka mendukung transformasi digital bagi para pelaku Usaha Mikro Kecil Menengah (UMKM), BSSN berupaya untuk menggerakan sektor UMKM melalui pemberian edukasi dan literasi serta penilaian mandiri melalui instrumen Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) yang dilakukan baik secara daring maupun luring ke seluruh wilayah Indonesia. Salah satu tujuan penilaian selanjutnya adalah agar UMKM dapat segera melakukan transformasi dalam melakukan aktifitasnya dari manual menjadi digital dengan tetap menjaga dan memperhatikan unsur

keamanannya, sehingga secara signifikan diharapkan dapat menambah dan memperkuat area pangsa pasar serta pendapatan.

Hal tersebut selaras dengan salah satu program pemerintah yaitu Bangga Buatan Indonesia, dimana PAMAN KAMI merupakan solusi bagi pelaku UMKM sebagai langkah awal memeriksa status keamanan informasi yang dimiliki. PAMAN KAMI menjadi landasan UMKM dalam menyusun strategi dan upaya pencegahan, meminimalisir maupun penanggulangan terjadinya serangan siber. Pada masa pandemi yang menyebabkan sebagian besar UMKM gulung tikar dikarenakan lemahnya daya beli masyarakat yang mengunjungi lokasi toko-toko atau industri, melalui dorongan penerapan teknologi digital dan peduli akan sisi keamanan penggunaan teknologi tersebut diharapkan UMKM mampu bertahan dan tetap berkembang meskipun dalam kondisi pandemi saat ini.

c. Pengarusutamaan Sosial Budaya

Pengarusutamaan modal sosial budaya merupakan internalisasi nilai dan pendayagunaan kekayaan budaya untuk mendukung seluruh proses pembangunan. Pengetahuan tradisional, kearifan lokal, pranata sosial harus menjadi pertimbangan proses perencanaan pembangunan nasional. Pesatnya perkembangan dan pemanfaatan Teknologi Informasi dan Komunikasi (TIK) telah menjadikan masyarakat Indonesia menjadi masyarakat informasi, masyarakat dimana kualitas hidup, dan juga prospek perubahan sosial dan pembangunan ekonomi, tergantung pada peningkatan dan manfaat informasi.

Namun di sisi lain, terdapat efek negatif pada semakin pesatnya pemanfaatan TIK yang terhubung dengan penggunaan internet seperti kurang bijaknya pemanfaatan informasi dalam ruang siber sebagai contoh semakin merebaknya kasus pornografi, berita bohong (hoaks), ujaran kebencian, diskriminatif dan isu SARA dapat mengikis nilai-nilai budaya luhur Indonesia dan kearifan lokal Indonesia. Sesuai tugas dan fungsi BSSN dalam pengendalian informasi maka BSSN akan konsisten melakukan upaya upaya pembangunan budaya keamanan siber melalui edukasi kesadaran keamanan informasi data pribadi kepada masyarakat umum dan literasi pengendalian informasi sehingga masyarakat memahami tentang urgensi suatu informasi memiliki nilai yang dapat

dipertanggungjawabkan kebenarannya dan disampaikan sesuai waktu yang dibutuhkan.

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 2021-2024

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 pelaksanaanya.

Arah Kebijakan dan Strategi pada Perubahan Renstra BSSN Tahun 2020-2024 ini masih merujuk pada Arah Kebijakan dan Strategi pada Renstra BSSN Tahun 2020-2024 karena dinilai masih relevan dengan lingkungan strategis BSSN saat ini. Arah Kebijakan dan Strategis BSSN dalam rangka mendukung pencapaian tujuan BSSN sebagai berikut:

1. Arah kebijakan dalam mencapai tujuan terwujudnya kedaulatan keamanan siber Indonesia sebagai berikut:

a. meningkatkan operasional secara lincah/*agile* 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.

3.2.1. Peningkatan operasional secara *agile* 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 serta tata kelola 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 pengkajian 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 *recovery*.
3. meningkatkan reputasi layanan keamanan siber dan sandi BSSN.

Berdasarkan agenda pembangunan nasional yang terdapat di dalam 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 pengkajian 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.

3.2.3. 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 pengkajian 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 6 Tahun 2020, 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. Berdasarkan arahan Presiden pada RPJMN 2020-2024, bahwa penyusunan regulasi dilakukan dengan berpedoman pada prinsip regulasi yang berorientasi tujuan, mengurangi

tumpang tindih, dan regulasi yang mengutamakan kualitas dibandingkan kuantitas.

Dalam rangka mendukung strategi pembangunan di bidang keamanan siber dan sandi untuk mengatasi isu strategis keamanan siber, BSSN mendorong dan mendukung penyusunan kerangka regulasi sebagai berikut :

1. Kebijakan terkait Strategi Keamanan Siber dan Sandi yang terdiri atas:
   a. Peraturan Presiden terkait Strategi Keamanan Siber Nasional;
   b. Peraturan Presiden Pelindungan Infrastruktur Informasi Vital; dan
   c. Peraturan BSSN tentang Metrik Keamanan Siber Indonesia.
2. Kebijakan terkait Tata Kelola Keamanan Siber dan Sandi yang terdiri atas:
   a. Peraturan BSSN tentang Manajemen Krisis Keamanan Siber Nasional;
   b. Peraturan BSSN terkait Audit Keamanan Informasi;
   c. Peraturan BSSN terkait Standar Audit SPBE;
   d. Peraturan BSSN terkait manajemen keamanan SPBE;
   e. Peraturan BSSN terkait Monitoring Keamanan Siber Nasional;
   f. Peraturan BSSN terkait *Voluntary Vulnerability Disclosure Program* (VVDP);
   g. Penyusunan peraturan CSIRT Sektoral (CII SIRT); dan
   h. Peraturan BSSN terkait Penyelenggaraan Sertifikat Elektronik.
3. Kebijakan Terkait sumber daya manusia Keamanan Siber dan Sandi yaitu, Peraturan BSSN tentang Roadmap Pembinaan Sumber Daya Manusia Bidang Keamanan Siber.

Penjelasan terkait urgensi pembentukan, unit kerja penanggung jawab dan target penyelesaian kebijakan tersebut dijabarkan dalam Matriks Kerangka Regulasi BSSN Tahun 2021-2024 sebagaimana tercantum pada Anak Lampiran 2 Perubahan Renstra BSSN Tahun 2020-2024.

3.4. KERANGKA KELEMBAGAAN

Perubahan lingkungan strategis yang dinamis, menuntut BSSN sebagai perangkat pemerintah perlu menyesuaikan kelembagaannya dengan situasi dan tuntutan perubahan. Selang berjalan 3 (tiga) tahun

sejak pembentukan BSSN, telah dilakukan evaluasi terhadap kelembagaan BSSN. Hasil evaluasi struktur organisasi BSSN sesuai Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara, dimana unit Kedeputian dikelompokkan berdasarkan fungsi yaitu identifikasi dan deteksi, proteksi, dan penanggulangan pemulihan, sementara di tingkat Eselon II dikelompokkan berdasarkan sektor yaitu Pemerintah, IIV dan Ekonomi Digital, menunjukkan kurang efektifnya pola koordinasi dan kolaborasi dalam proses kerja serta sulitnya membentuk maturitas keamanan siber secara penuh pada setiap pemangku kepentingan karena setiap Deputi hanya bertanggung jawab pada satu fungsi saja. Selain pertimbangan tersebut, juga dikenali kebutuhan penajaman fungsi-fungsi BSSN sebelumnya.

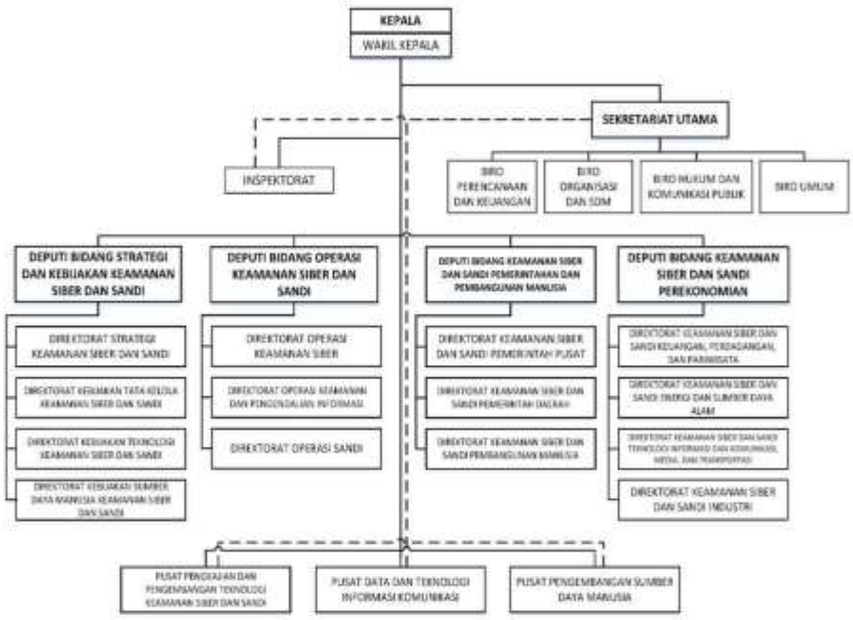
Penyempurnaan organisasi Badan Siber dan Sandi Negara dilakukan dengan memperhatikan mandat, kebijakan pembangunan, serta berpedoman pada prinsip "*structure follow process follow strategy*" yang artinya strategi menjadi acuan dilakukannya penataan proses bisnis dan penyesuaian struktur organisasi. Penataan organisasi BSSN juga memperhatikan fungsi-fungsi yang sebelumnya telah dijalankan BSSN untuk menjamin keberlangsungan proses yang telah ada. Fungsi-fungsi BSSN dalam Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara telah terpetakan dalam penataan organisasi dan tata kerja BSSN yang dilakukan saat ini dan dikelompokkan berdasarkan kesamaan, kedekatan, dan tujuan yang akan dicapai untuk menghindari terjadinya duplikasi fungsi.

Hasil evaluasi organisasi tersebut selanjutnya mendasari perubahan organisasi dan tata kerja BSSN pada tahun 2021 yang ditandai dengan diterbitkannya Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. BSSN melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan. Dalam melaksanakan tugas tersebut, BSSN melaksanakan fungsi sebagai berikut:

a. perumusan dan penetapan kebijakan teknis di bidang keamanan siber dan sandi;
b. pelaksanaan kebijakan teknis di bidang keamanan siber dan sandi;
c. penyusunan norma, standar, prosedur, dan kriteria di bidang persandian;
d. pelaksanaan bimbingan teknis dan supervisi di bidang persandian;

e. koordinasi pelaksanaan tugas, pembinaan, dan dukungan administrasi kepada seluruh unsur organisasi di lingkungan BSSN;
f. pengelolaan barang milik negara yang menjadi tanggung jawab BSSN;
g. pelaksanaan dukungan yang bersifat substantif kepada seluruh unsur organisasi di lingkungan BSSN; dan
h. pengawasan atas pelaksanaan tugas di lingkungan BSSN.

Organisasi dan Tata Kerja BSSN, Struktur Organisasi BSSN ditunjukkan pada Gambar 3.6



Gambar 3.6 Struktur Organisasi BSSN

BSSN terdiri atas :

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

BSSN juga didukung dengan unsur-unsur pendukung yaitu:

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

Dalam pelaksanaan pengendalian internal, BSSN juga didukung unit kerja Inspektorat sebagai unsur pengawas.

Dengan adanya penataan organisasi ini diharapkan BSSN dapat mewujudkan organisasi yang *agile* dengan memperhatikan aspek strategi, struktur, proses, sumber daya manusia, sarana dan prasarana serta aspek teknologi. Proses dalam organisasi merupakan aspek yang sangat penting guna berlangsungnya seluruh aktivitas organisasi untuk menciptakan dan memelihara rantai nilai dalam rangka mencapai tujuan utama secara dinamis. Perubahan Organisasi dan Tata Kerja BSSN ini juga harus memastikan bahwa penyelarasan proses bisnis lintas unit kerja dalam suatu arsitektur proses bisnis yang tuntas dapat terwujud. 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.

Penyusunan proses bisnis oleh instansi pemerintah merupakan kewajiban yang harus dikerjakan sesuai dengan ketentuan pasal 7 Ayat (2) UU Nomor 30 Tahun 2014 tentang Administrasi Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Menpan dan RB Nomor 19 Tahun 2018 tentang Penyusunan Peta Proses Bisnis Instansi Pemerintah. Peta Proses Bisnis BSSN merupakan acuan bagi BSSN dan unit organisasi untuk menggambarkan hubungan kerja yang efektif dan efisien antar unit organisasi untuk menghasilkan kinerja sesuai dengan tujuan pendirian organisasi. 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. Proses bisnis BSSN ditunjukkan pada gambar berikut :

Gambar 3.7 Proses Bisnis Badan Siber dan Sandi Negara

Proses bisnis terdiri atas tiga proses : 1) proses utama; 2) proses pendukung; dan 3) proses manajerial. Proses utama, yaitu proses bisnis yang berpengaruh langsung terhadap keberhasilan dalam mencapai visi, misi, dan strategi Badan Siber dan Sandi Negara serta berperan langsung dalam memenuhi kebutuhan pengguna eksternal dan internal BSSN. Proses Utama terdiri atas Penyusunan Kebijakan dan Strategi, Peningkatan Kapasitas Kamsibersan, dan Penyelenggaraan Kamsibersan. Proses Pendukung yaitu proses untuk mengelola operasional dari suatu sistem dan memastikan proses utama berjalan dengan baik. Proses pendukung BSSN terdiri atas Pengelolaan Teknologi Informasi, Pengelolaan Layanan Hukum, Pengkajian dan Pengembangan Kamsibersan, dan Pengelolaan Komunikasi dan Layanan Informasi. Proses Manajerial yaitu proses yang memungkinkan aktivitas pada proses utama dan pendukung berjalan lebih optimal terdiri atas Penataan Organisasi dan Tata Laksana, Pengelolaan sumber daya manusia BSSN, Pengelolaan Administrasi dan Umum, Pengelolaan Perencanaan dan Anggaran, dan Peningkatan Sistem Pengawasan.

Kelembagaan BSSN harus bersifat dinamis sebagai bentuk adaptasi terhadap perkembangan lingkungan strategis BSSN dengan tetap mengacu pada visi misi Organisasi. Untuk itu, kelembagaan dan tata laksana BSSN perlu dievaluasi secara berkala untuk mendapatkan organisasi yang tepat fungsi, tepat ukuran dan tepat proses agar mendukung tercapainya kinerja organisasi yang optimal.

Penguatan kelembagaan BSSN juga dilakukan melalui Penyederhanaan birokrasi melalui optimalisasi jabatan fungsional Jabatan Fungsional memiliki peran penting dalam mewujudkan tujuan organisasi, karena jabatan fungsional merupakan ujung tombak

dari implementasi tugas Kementerian/Lembaga dalam mencapai target dan rencana strategis. Penyederhanaan birokrasi melalui optimalisasi jabatan fungsional sebagai tindak lanjut Arahan Presiden Republik Indonesia, serta sebagai bentuk pelaksanaan Peraturan Pendayagunaan Aparatur Negara dan Reformasi Birokrasi 28 tahun 2019 tentang Penyetaraan Jabatan Administrasi Ke Dalam Jabatan Fungsional. Pada Tahun 2020, BSSN telah melakukan penyederhanaan birokrasi dengan pengalihan jabatan administrator dan pengawas ke dalam jabatan fungsional kepada sejumlah 98 (sembilan puluh delapan) orang yang terdiri atas 51 (lima puluh satu) jabatan fungsional madya dan 47 (empat puluh tujuh) jabatan fungsional muda.

Penyederhanaan birokrasi BSSN ini diharapkan akan mengoptimalkan *talent* organisasi BSSN yang berdaya saing, mewujudkan organisasi yang *agile*, dan peningkatan profesionalisme Aparatur Sipil Negara yang berujung pada peningkatan kualitas pelayanan publik kepada para pemangku kepentingan. Penyederhanaan birokrasi akan dilakukan secara bertahap dan dievaluasi secara berkala untuk menilai jabatan fungsional yang memerlukan penyempurnaan atau fungsi-fungsi organisasi yang memerlukan jabatan fungsional baru.

Pesatnya perkembangan teknologi ditambah dengan pandemi *covid-19* dinilai telah mempercepat proses transformasi digital tak terkecuali pada lini pemerintahan. Penguatan tatalaksana dengan memanfaatkan transformasi digital merupakan tuntutan bagi setiap penyelenggara pemerintahan. Hal ini selaras dengan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik yang bertujuan untuk mewujudkan sistem pemerintahan berbasis elektronik yang terpadu baik di instansi Pusat maupun Pemerintah Daerah. Untuk itu, BSSN akan melakukan peningkatan penerapan tatalaksana berbasis elektronik baik dalam layanan publik maupun layanan internal BSSN.

BAB IV

TARGET KINERJA DAN KERANGKA PENDANAAN

4.1. TARGET KINERJA

Keberhasilan pencapaian Renstra BSSN Tahun 2021 – 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 90,94 (sembilan puluh koma sembilan empat) pada tahun 2024.

4.1.1. Sasaran Strategis, Indikator Kinerja Sasaran Strategis dan Target

Indikator Kinerja Sasaran Strategis BSSN Tahun 2021–2024 beserta target kinerja per tahun tercantum pada Tabel 4.1.

Tabel 4.1 Sasaran Strategis, Indikator Kinerja Sasaran Strategis dan Target BSSN Tahun 2021-2024

No	Sasaran Strategis	Indikator Kinerja Sasaran Strategis	Target			
			2021	2022	2023	2024
1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas	1.1. Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi	70%	70%	75%	80%
2	Meningkatnya Kapasitas Keamanan Siber dan Sandi	2.1. Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan	58,87 %	64,14 %	69,40 %	75,42 %
		2.2. Persentase Penyelenggara	9,6%	38,5%	69,1%	100%

		Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59				
3	Terwujudnya Birokrasi BSSN yang Bersih, Akuntabel, Berkinerja Tinggi, Efektif, Efisien dan Berorientasi pada Pelayanan Publik	3.1. Indeks Reformasi Birokrasi	79,04	81,81	84,32	86,85

4.1.2. Sasaran Program, Indikator Kinerja Sasaran Program dan Target

BSSN mengampu 2 (dua) program yaitu Program 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 4.1.

Tabel 4.1 Sasaran Program, Indikator Kinerja Sasaran Program dan Target Program Keamanan dan Ketahanan Siber dan Sandi Negara Tahun 2021-2024

No	Sasaran Program	Indikator Kinerja Sasaran Program	Target			
			2021	2022	2023	2024
1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas	1.1. Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi	70%	70%	75%	80%

2	Meningkatnya Kapasitas Keamanan Siber dan Sandi	1.1. Persentase rekomendasi hasil operasi keamanan siber, operasi pengendalian informasi dan sandi yang termanfaatkan	58,87%	64,14%	69,40%	75,42%
		1.2. Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59	9,6%	38,5%	69,1%	100,0%

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 4.2.

Tabel 4.2 Sasaran Program, Indikator Kinerja Sasaran Program dan Target Program Dukungan Manajemen Tahun 2021-2024

No	Sasaran Program	Indikator Kinerja Sasaran Program	Target			
			2021	2022	2023	2024
1	Meningkatnya Pengelolaan Sumber Daya BSSN yang Andal dan Profesional	1.1. Indeks Reformasi Birokrasi	79,04	81,81	84,32	86,85
		1.2. Opini Badan Pemeriksa Keuangan (BPK)	WTP	WTP	WTP	WTP
		1.3. Nilai AKIP BSSN	64,17	65,92	67,72	68,72
2	Meningkatnya Tata Kelola TIK yang Aman dan Andal	2.1. Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)	3,3	3,5	3,8	4

3	Meningkatnya Pemanfaatan Hasil Pengkajian dan Pengembangan Bidang Siber dan Sandi	3.1 Persentase Hasil Pengkajian dan Pengembangan yang dimanfaatkan oleh pengguna	69%	70%	71%	72%

4.1.3. Sasaran Kegiatan, Indikator Kinerja Sasaran Kegiatan dan Target

Program keamanan dan ketahanan siber dan sandi negara terdiri atas 7 (tujuh) kegiatan yang diampu oleh 16 (enam belas) unit kerja setingkat Eselon II dan 1 (satu) unit kerja BSrE. Penyusunan Sasaran Kegiatan, Indikator Kinerja Kegiatan telah mempertimbangkan Redesain Sistem Perencanaan Penganggaran. Sasaran kegiatan, indikator kinerja sasaran kegiatan beserta targetnya pada program keamanan dan ketahanan siber dan sandi negara dapat dilihat pada Tabel 4.3

Tabel 4.3 Sasaran Kegiatan, Indikator Kinerja Sasaran Kegiatan dan Target Program Keamanan dan Ketahanan Siber dan Sandi Negara Tahun 2021-2024

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target			
			2021	2022	2023	2024
6653	Perumusan Kebijakan Keamanan Siber dan Sandi Unit Kerja: 1. Direktorat Strategi Keamanan Siber Dan Sandi 2. Direktorat Kebijakan Tata Kelola Keamanan Siber Dan Sandi 3. Direktorat Kebijakan Teknologi Keamanan Siber Dan Sandi 4. Direktorat Kebijakan Sumber Daya Manusia Keamanan Siber Dan Sandi					
1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas	1.1. Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi	70%	70%	75%	80%
6654	Penyelenggaraan Operasi Keamanan Siber dan Sandi Unit Kerja: 1. Direktorat Operasi Keamanan Siber 2. Direktorat Operasi Keamanan dan Pengendalian Informasi 3. Direktorat Operasi Sandi					

1	Meningkatnya Kapasitas Operasi Keamanan Siber dan Sandi	1.1. Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan	58,87 %	64,14 %	69,40 %	75,42 %
6655	Pengembangan Kapasitas Keamanan dan Sandi Siber Sektor Pemerintahan dan Pembangunan Manusia Unit Kerja: 1. Direktorat Keamanan Siber dan Sandi Pemerintah Pusat 2. Direktorat Keamanan Siber dan Sandi Pemerintah Daerah 3. Direktorat Keamanan Siber dan Sandi Pembangunan Manusia					
1	Meningkatnya Kapasitas Keamanan Siber dan Sandi Sektor Pemerintahan dan Pembangunan Manusia	1.1. Persentase Penyelenggara Sistem Elektronik (PSE) pada Sektor Pemerintahan dan Pembangunan Manusia dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59	8,2%	38,8%	69,4%	100%
6656	Pengembangan Kapasitas Keamanan Siber dan Sandi Sektor Perekonomian Unit Kerja: 1. Direktorat Keamanan Siber dan Sandi Keuangan dan Perdagangan 2. Direktorat Keamanan Siber dan Sandi Energi dan Sumber Daya Alam 3. Direktorat Keamanan Siber dan Sandi Teknologi Informasi dan Komunikasi, Media dan Transportasi 4. Direktorat Keamanan Siber dan Sandi Industri					
1	Meningkatnya Kapasitas Keamanan Siber dan Sandi Sektor Perekonomian	1.1. Persentase Penyelenggara Sistem Elektronik (PSE) pada Sektor Perekonomian dengan Tingkat Kematangan	11,1%	38,3%	68,8%	100%

		keamanan siber pada skor minimal 2,59				
3121	Pengembangan Sumber Daya Manusia Keamanan Siber dan Sandi Unit Kerja: Pusat Pengembangan Sumber Daya Manusia					
1	Terwujudnya SDM Kamsiber dan Sandi yang Profesional dan Berintegritas	1.1. Persentase Lulusan SDM Keamanan Siber dan Sandi berstandarkan nilai minimal baik	83%	84%	85%	85%
		1.2. Persentase Kepuasan (Instansi) Pengguna Lulusan Diklat	83%	85%	87%	89%
		1.3. Persentase Lulusan Uji Kompetensi Pemangku Kepentingan	88%	89%	89%	91%
3123	Pendidikan Profesional di Bidang Siber dan Sandi Unit Kerja: Politeknik Siber dan Sandi Negara					
1	Tersedianya Mahasiswa Poltek SSN yang Profesional dan Berintegritas	1.1. Tingkat Kepuasan Pengguna Terhadap Kompetensi Lulusan	95%	95%	95%	95%
		1.2. Persentase Lulusan dari Mahasiswa yang Naik Tingkat	90%	91%	91%	92%
3124	Penyelenggaraan Sertifikasi Elektronik Unit Kerja: Balai Sertifikasi Elektronik					
1	Terwujudnya Pengelolaan Sertifikat Elektronik yang Andal dan Profesional	1.1. Tingkat Efektifitas Implementasi Sertifikat Elektronik	75%	80%	85%	90%

Program dukungan manajemen terdiri atas 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 4.4.

Tabel 4.4 Sasaran Kegiatan, Indikator Kinerja Sasaran Kegiatan dan Target Program Dukungan Manajemen Tahun 2021-2024

No	Sasaran Kegiatan	Indikator Kinerja Sasaran Kegiatan	Target			
			2021	2022	2023	2024
3075	Penyelenggaraan Perencanaan dan Keuangan Unit Kerja: Biro Perencanaan dan Keuangan					
1	Meningkatnya Perencanaan, Pengelolaan Kinerja, dan Keuangan yang Andal dan Profesional	1.1. Nilai Kinerja Anggaran BSSN	88	90	93	93
		1.2. Nilai Indikator Kinerja Pelaksanaan Anggaran BSSN	88,82	90,15	91,51	92,80
		1.3. Nilai AKIP BSSN	64,17	65,92	67,72	68,72
3076	Penyelenggaraan Organisasi dan Sumber Daya Manusia Unit Kerja: Biro Organisasi dan Sumber Daya Manusia					
1	Meningkatnya Pengelolaan Organisasi dan Tata Laksana yang Andal	1.1. Tingkat Pemenuhan Proses Bisnis	75%	80%	85%	90%
		1.2. Tingkat Pemenuhan Pola Pikir dan Budaya Kerja	75%	80%	85%	90%
2	Meningkatnya Manajemen Aparatur Sipil Negara yang Profesional	2.1. Indeks Profesionalitas Aparatur Sipil Negara	81,25	81,50	81,75	82,00
		2.2. Indeks Penerapan Sistem Merit	0,69	0,73	0,74	0,75
3077	Penyelenggaraan Hukum dan Komunikasi Publik Unit Kerja: Biro Hukum dan Komunikasi Publik					
1	Meningkatnya Hukum dan Komunikasi Publik yang Andal dan	1.1. Persentase penyelesaian pemberian tanggapan hukum atas	100%	100%	100%	100%

	Profesional	rancangan peraturan atau peraturan				
		1.2. Indeks Keterbukaan Informasi Publik BSSN	83,05	85,55	87,77	90,65
2	Meningkatnya Ketatausahaan, Kearsipan dan Dukungan Strategis Pimpinan yang Andal dan Profesional	2.1. Hasil Pengawasan Arsip	89,08	90,01	90,01	90,01
		2.2. Persentase pemenuhan layanan dukungan strategis pimpinan	100%	100%	100%	100%
3078	Penyelenggaraan Layanan Umum Unit Kerja: Biro Umum					
1	Meningkatnya Dukungan Administratif Bidang, Kerumahtanggaan , Pengelolaan BMN, dan Layanan Pengadaan yang andal dan profesional	1.1. Tingkat Kematangan UKPBJ BSSN	72,00	75,75	83,25	87,00
		1.2. Tingkat Akuntabilitas Pengelolaan BMN	91%	92%	93%	94%
		1.3. Pemenuhan dan Pemeliharaan Sarana dan Prasarana	85%	90%	90%	95%
3079	Pengawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara Unit Kerja: Inspektorat					
1	Meningkatnya Pengawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara yang andal dan profesional	1.1. Opini BPK	WTP	WTP	WTP	WTP
		1.2. Tingkat Kapabilitas APIP	Level 3 DC	Level 3 DC	Level 3 DC	Level 3
3138	Pengelolaan Data dan Teknologi Informasi Komunikasi Unit Kerja: Pusat Data dan Teknologi Informasi Komunikasi					

1	Meningkatnya Tata Kelola TIK yang aman dan andal	1.1. Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)	3,3	3,5	3,8	4
3139	Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi Unit Kerja: Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi					
1	Meningkatnya Pemanfaatan Hasil Pengkajian dan Pengembangan Bidang Siber dan Sandi	1.1. Persentase Hasil Pengkajian dan Pengembangan yang dimanfaatkan oleh pengguna	69%	70%	71%	72%

4.2. KERANGKA PENDANAAN

Indikasi kebutuhan pendanaan untuk mencapai tujuan dan sasaran strategis BSSN dalam kurun 2021-2024 sebagaimana telah dijabarkan pada Subbab 4.1 disampaikan pada Tabel 4.5. Adapun pendanaan pada tahun 2021 yang tertulis merupakan sesuai Daftar Isian Pelaksanaan Anggaran (DIPA) BSSN, sedangkan indikasi kebutuhan pendanaan 2022-2024 memuat indikasi kebutuhan pendanaan rangka mencapai tujuan dan sasaran strategis BSSN.

Tabel 4.5 Kerangka Pendanaan BSSN Tahun 2021-2024

Program	Indikasi Kebutuhan Pendanaan (dalam ribuan rupiah)			
	2021	2022	2023	2024
Dukungan Manajemen	753.491.985	1.078.842.063	1.366.377.974	1.853.877.561
Keamanan dan Ketahanan Siber dan Sandi Negara	852.108.396	1.397.317.627	3.161.796.645	4.285.112.838
Total	1.605.600.381	2.476.159.690	4.528.174.619	6.138.990.399

Penyusunan kerangka pendanaan BSSN tahun 2021-2024 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 2021-2024 sebagaimana diamanatkan dalam matriks pembangunan jangka menengah BSSN pada RPJMN Tahun 2021-2024.
2. pendanaan inisiatif strategis BSSN Tahun 2021-2024 dalam rangka pencapaian tujuan dan sasaran strategis BSSN.
3. pendanaan pemenuhan kebutuhan dasar penyelenggaraan perkantoran BSSN Tahun 2021-2024.

Rincian target kinerja dan indikasi kebutuhan anggaran masing-masing program dan kegiatan BSSN Tahun 2021 sampai dengan 2024 tertuang dalam matriks kinerja dan kerangka pendanaan sebagaimana tercantum pada Anak Lampiran 1 Perubahan Renstra BSSN Tahun 2020-2024.

BAB V
PENUTUP

Perubahan 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, Perubahan Renstra BSSN Tahun 2020-2024 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 pada akhir periode RPJMN Tahun 2020-2024. Untuk menjamin akuntabilitas dan konsistensi arah pembangunan BSSN, Perubahan 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 Perubahan Renstra BSSN 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.

ANAK LAMPIRAN 1

MATRIKS KINERJA DAN PENDANAAN

Program / Kegiatan	Sasaran Program (Outcome)/ Sasaran Kegiatan (Output)/Indikator	Lokasi	TARGET KINERJA				KERANGKA PENDANAAN				Unit Organisasi Pelaksana
			2021	2022	2023	2024	2021	2022	2023	2024	
BADAN SIBER DAN SANDI NEGARA							1,605,600,381,000	2,476,159,691,000	4,528,174,619,000	6,138,990,399,000	
SS 1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas										
IKS 1.1	*Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi*		70%	70%	75%	80%					
SS 2	Meningkatnya Kapasitas Keamanan Siber dan Sandi										

IKS 2.1	*Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan*		58.87%	64.14%	69.40%	75.42%			
IKS 2.2	*Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59*		9.6%	38.5%	69.1%	100.0%			
SS. 3	Terwujudnya Birokrasi BSSN yang Efektif, Profesional dan berorientasi pada pelayanan publik								
IKS 3.1	*Indeks Reformasi Birokrasi*		79.04	81.81	84.32	86.85			

PROGRAM KEAMANAN DAN KETAHANAN SIBER DAN SANDI NEGARA							852,108,396,000	1,397,317,628,000	3,161,796,645,000	4,285,112,838,000	DEPUTI I, DEPUTI II, DEPUTI III, DEPUTI IV, PUSBANG SDM, PSSN, BSrE
SP. 1 Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas											
IKP 1.1 Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi		70%	70%	75%	80%						
SP. 2 Meningkatnya Kapasitas Keamanan Siber dan Sandi											
IKP 2.1 Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan		58.8 7%	64.1 4%	69.4 0%	75.4 2%						

IKP 2.2	*Persentase Penyelenggara Sistem Elektronik (PSE) dengan Tingkat Kematangan keamanan siber pada skor 2,59*		9.6%	38.5%	69.1%	100.0%			
Kode xxxx : Perumusan Kebijakan Keamanan Siber dan Sandi		Pusat							
SK.1	Terwujudnya Kebijakan Keamanan Siber dan Sandi yang berkualitas						12,573,503,000	21,385,662,000	182,391,877,000	281,042,516,000	DIREKTORAT STRATEGI KEAMANAN SIBER DAN SANDI, DIREKTORAT KEBIJAKAN TATA KELOLA KEAMANAN SIBER DAN SANDI, DIREKTORAT KEBIJAKAN TEKNOLOGI KEAMANAN SIBER DAN SANDI, DIREKTORAT KEBIJAKAN SUMBER DAYA MANUSIA KEAMANAN SIBER DAN SANDI
IKK 1.1	*Tingkat Penyelesaian Kebijakan Prioritas Bidang Keamanan Siber dan Sandi*		70%	70%	75%	80%					

Kode xxxx : Penyelenggaraan Operasi Keamanan Siber dan Sandi		Pusat							
	SK.1	Meningkatnya Kapasitas Operasi Keamanan Siber dan Sandi							
	IKK 1.1	*Persentase rekomendasi hasil operasi keamanan siber, operasi keamanan dan pengendalian informasi, dan operasi sandi yang termanfaatkan*		58.87%	64.14%	69.40%	75.42%		
			Pusat					662,146,098,000	1,091,806,339,000	2,187,040,438,000	2,829,319,125,000	DIREKTORAT OPERASI KEAMANAN SIBER, DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI, DIREKTORAT OPERASI SANDI.
Kode xxxx : Pengembangan Kapasitas Keamanan Siber dan Sandi Sektor Pemerintahan dan Pembangunan Manusia								20,383,858,000	46,240,345,000	163,663,850,000	253,708,908,000	DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAH PUSAT, DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAH DAERAH, DIREKTORAT KEAMANAN SIBER DAN SANDI PEMBANGUNAN MANUSIA.

SK.1	Meningkatnya Kapasitas Keamanan Siber dan Sandi Sektor Pemerintahan dan Pembangunan Manusia							
IKK1.1	*Persentase Penyelenggara Sistem Elektronik (PSE) pada Sektor Pemerintahan dan Pembangunan Manusia dengan Tingkat Kematangan keamanan siber pada skor minimal 2,59*	8,2%	38,8 %	69,4 %	100, 0%			

Kode xxxx : Pengembangan Kapasitas Keamanan Siber dan Sandi Sektor Perekonomian	Pusat					20,187,509,000	30,772,058,000	306,396,045,000	454,305,272,000	DIREKTORAT KEAMANAN SIBER DAN SANDI KEUANGAN DAN PERDAGANGAN, DIREKTORAT KEAMANAN SIBER DAN SANDI ENERGI DAN SUMBER DAYA ALAM,DIREKTORAT KEAMANAN SIBER DAN SANDI TEKNOLOGI INFORMASI DAN KOMUNIKASI, MEDIA DAN TRANSPORTASI,DIREKTORAT KEAMANAN SIBER DAN SANDI INDUSTRI	
SK.1 Meningkatnya Kapasitas Keamanan Siber dan Sandi Sektor Perekonomian											
IKK1.1 Persentase Penyelenggara Sistem Elektronik (PSE) pada Sektor Perekonomian dengan Tingkat Kematangan keamanan siber pada skor 2,59		11.1%	38.3%	68.8%	100.0%	21,509,391,00	64,407,989,00	122,335,232,0	152,239,878,0	PUSBANG SDM	
xxxx: Pengembangan SDM Keamanan Siber	Pusat										

dan Sandi					0	0	00	00	
SK.1 Terwujudnya SDM Kamsiber dan Sandi yang Profesional dan Berintegritas									
IKK 1.1 Persentase Lulusan SDM Keamanan Siber dan Sandi berstandarkan nilai minimal baik		83%	84%	85%	85%				
IKK 1.2 Persentase Kepuasan (Instansi) Pengguna Lulusan Diklat		83%	85%	87%	89%				
IKK 1.3 Persentase Lulusan Uji Kompetensi Pemangku Kepentingan		88%	89%	89%	91%				
3123: Pendidikan Profesional di Bidang Siber dan Sandi	Pusat					36,699,215,000	53,539,095,000	82,171,079,000	139,435,047,000
SK.1 Tersedianya Mahasiswa Politek SSN yang Profesional dan Berintegritas									PSSN

IKK 1.1	*Tingkat Kepuasan Pengguna Terhadap Kompetensi Lulusan*		95%	95%	95%	95%				
IKK 1.2	*Persentase Lulusan dari Mahasiswa yang Naik Tingkat*		90%	91%	91%	92%				
3124: Penyelenggaraan Sertifikasi Elektronik		Pusat					78,608,822,000	89,166,140,000	117,798,124,000	175,062,092,000	BSrE
Sk.1	Terwujudnya Pengelolaan sertifikat elektronik yang andal dan profesional										
IKK.1	*Tingkat Efektifitas Implementasi Sertifikat Elektronik*		75%	80%	85%	90%					
PROGRAM DUKUNGAN MANAJEMEN							753,491,985,000	1,078,842,063,000	1,366,377,974,000	1,853,877,561,000	SEKRETARIAT UTAMA, INSPEKTORAT , PUSDATIK, PUSKAJIBANG
SP.1	Meningkatnya Pengelolaan Sumber Daya BSSN yang andal dan profesional										
IKP 1.1	*Indeks Reformasi*		79.04	81.81	84.32	86.85					

	Birokrasi									
IKP 1.2	*Opini BPK*		WTP	WTP	WTP	WTP				
IKP 1.3	*Nilai Akuntabilitas Kinerja Instansi Pemerintah (AKIP)*		64.17	65.92	67.72	68.72				
SP.2	Meningkatnya Tata Kelola TIK yang aman dan andal									
IKP 2.1	*Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)*		3.3	3.5	3.8	4				
SP . 3	Meningkatnya Pemanfaatan Hasil Pengkajian dan Pengembanga n Bidang Siber dan Sandi									
IKP 3.1	*Persentase Hasil Pengkajian dan Pengembanga n yang dimanfaatkan oleh pengguna*		69%	70%	71%	72%				
3075 : Penyelenggaraan Perencanaan dan Keuangan		Pusat					182,646,239,000	192,007,751,000	201,608,139,000	211,688,546,000	BIRO RENKEU

SK.1	Meningkatnya Perencanaan, Pengelolaan Kinerja, dan Keuangan yang Andal dan Profesional										
IKK 1.1	*Nilai Kinerja Anggaran*		88	90	93	93					
IKK 1.2	*Nilai Indikator Kinerja Pelaksanaan Anggaran BSSN*		88.82	90.15	91.51	92.8					
IKK 1.3	*Nilai Akuntabilitas Kinerja Instansi Pemerintah (AKIP)*		64.17	65.92	67.72	68.72					
3076 : Penyelenggaraan Organisasi dan SDM		Pusat					9,986,501,000	37,288,234,00 0	39,152,646,00 0	41,110,278,00 0	BIRO OSDM
SK.1	Meningkatnya Pengelolaan Organisasi dan Tata Laksana yang Andal										
IKK 1.1	*Tingkat Pemenuhan Proses Bisnis*		75%	80%	85%	90%					
IKK 1.2	*Tingkat Pemenuhan Pola Pikir dan Budaya Kerja*		75%	80%	85%	90%					

SK.2	Meningkatnya Manajemen Aparatur Sipil Negara yang Profesional									
IKK 2.1	*Indeks Profesionalitas Aparatur Sipil Negara (ASN)*		81.25	81.50	81.75	82.00				
IKK 2.2	*Indeks Penerapan Sistem Merit (ASN)*		0.69	0.73	0.74	0.75				
xxxx : Penyelenggaraan Hukum dan Komunikasi Publik		Pusat					13,897,675,000	15,425,717,000	16,139,168,000	16,886,554,000	BIRO HUKUM DAN KOMUNIKASI PUBLIK
SK.1	Meningkatnya Hukum dan Komunikasi Publik yang Andal dan Profesional									
IKK 1.1	*Persentase penyelesaian pemberian tanggapan hukum atas rancangan peraturan atau peraturan*		100 %	100 %	100 %	100 %				
IKK 1.2	*Indeks Keterbukaan Informasi Publik BSSN*		83.05	85.55	87.77	90.65				

SK.2	Meningkatnya Ketatausahaan, Kearsipan dan Dukungan Strategis Pimpinan yang Andal dan Profesional									
IKK 2.1	*Hasil Pengawasan Arsip*		89.08	90.01	90.01	90.01				
IKK 2.2	*Persentase pemenuhan layanan dukungan strategis pimpinan*		100 %	100 %	100 %	100 %				
3078 : Penyelenggaraan Dukungan Administratif Bidang Kerumahtanggaan, Pengelolaan BMN, dan Layanan Pengadaan		Pusat					209,916,193,000	197,065,429,000	196,978,674,000	196,889,318,000
SK.1	Meningkatnya Dukungan Administratif Bidang Kerumahtanggaan, Pengelolaan BMN, dan Layanan Pengadaan yang Andal dan Profesional									BIRO UMUM
IKK	*Tingkat*		72.0	75.7	83.2	87.0				

1.1	*Kematangan UKPBJ BSSN*		0	5	5	0				
IKK 1.2	*Tingkat Akuntabilitas Pengelolaan BMN*		91%	92%	93%	94%				
IKK 1.3	*Pemenuhan dan Pemeliharaan Sarana dan Prasarana*		85%	90%	90%	95%				
3079 : Pengawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara		Pusat					3,924,618,000	4,028,582,000	4,230,011,000	4,441,512,000
SK.1	Meningkatnya Pengawasan dan Peningkatan Akuntabilitas Aparatur Badan Siber dan Sandi Negara yang Andal dan Profesional									INSPEKTORAT
IKK 1.1	*Opini BPK*		WTP	WTP	WTP	WTP				
IKK 1.2	*Tingkat Kapabilitas APIP*		Level 3 DC	Level 3 DC	Level 3 DC	Level 3				
3038 : Pengelolaan Data dan Teknologi Informasi Komunikasi		Pusat					255,225,708,000	517,015,919,000	773,170,916,000	1,228,674,943,000
SK.1	Meningkatnya Tata Kelola TIK yang									PUSDATIK

	aman dan andal										
IKK 1.1	*Indeks Sistem Pemerintah Berbasis Elektronik (SPBE)*		3.3	3.5	3.8	4					
3039 : Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi		Pusat					77,895,051,000	116,010,431,000	135,098,420,000	154,186,410,000	PUSKAJIBANG TEKAMSISAN
SK.1	Meningkatnya Pemanfaatan Hasil Pengkajian dan Pengembangan Bidang Siber dan Sandi										
IKK 1.1	*Persentase Hasil Pengkajian dan Pengembangan yang dimanfaatkan oleh penggna*		69%	70%	71%	72%					

ANAK LAMPIRAN 2

MATRIKS KERANGKA REGULASI BSSN TAHUN 2021-2024

No	Arah Kerangka Regulasi/ Kebutuhan Regulasi	Urgensi Pembentukan	Unit Kerja Penanggung Jawab	Unit Kerja Terkait	Target (Tahun)
1	Peraturan Presiden terkait Strategi Keamanan Siber Nasional	Merupakan tindak lanjut Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara, 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 Strategi Keamanan Siber dan Sandi	1 Deputi Operasi Keamanan Siber dan Sandi	2022
				2 Deputi Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia	
				3 Deputi Keamanan Siber dan Sandi Perekonomian	
2	Peraturan Presiden Pelindungan Infrastruktur Informasi Vital	Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang menganggu ketertiban umum. Gangguan terhadap	Direktorat Kebijakan Tata Kelola Keamanan Siber dan	1 Deputi Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia	2021

		infrastruktur informasi vital nasional dapat menimbulkan kerugian dan dampak yang serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, serta perekonomian nasional. Untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik, perlu pengaturan mengenai Pelindungan Infrastruktur Informasi Vital.	Sandi	2 Deputi Keamanan Siber dan Sandi Perekonomian	
3	Peraturan BSSN tentang Metrik Keamanan Siber Indonesia	Tindak lanjut Agenda Pembangunan RPJMN IV Tahun 2020 - 2024 yaitu Memperkuat Stabilitas Polhukhankam dan Transformasi Pelayanan Publik yaitu Memperbaiki sistem peradilan, penataan regulasi dan tata kelola. Peraturan ini mengatur tentang Indeks Keamanan Siber Nasional merupakan alat evaluasi untuk mengukur Metrik Keamanan Siber di Tingkat Nasional terkait pengembangan keamanan siber, risk-assessment strategy, dan audit keamanan siber.	Direktorat Strategi Keamanan Siber dan Sandi	-	2023
4	Peraturan tentang Manajemen Krisis Keamanan Siber Nasional	Merupakan tindak lanjut Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara yang menganamatkan BSSN menjadi pusat manajemen krisis siber sehingga perlu diatur organisasi dan tata kelola manajemen krisis siber di Indonesia.	Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi	-	2022
5	Peraturan terkait Audit Keamanan Informasi	Dalam rangka mendukung strategi pembangunan ekosistem di bidang keamanan siber dan sandi serta sebagai landasan BSSN dalam melaksanakan tugas dan fungsinya selain atas dasar kewenangan yang telah tercantum	Direktorat Kebijakan dan Tata Kelola Keamanan Siber dan	1 Deputi Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia	2022

	dalam Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.	Sandi	2	Deputi Keamanan Siber dan Sandi Perekonomian		
6	Peraturan BSSN tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan SPBE	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 Kebijakan Tata Kelola Keamanan Siber dan Sandi	1	Direktorat Keamanan Siber Pemerintah Pusat	2022
				2	Direktorat Keamanan Siber Pemerintah Daerah	
7	Peraturan BSSN terkait Manajemen Keamanan SPBE	Tindak lanjut dari Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE dimana BSSN menjadi *leading sector* dalam menangani masalah manajemen keamanan Sistem Pemerintahan Berbasis Elektronik.	Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi	1	Direktorat Keamanan Siber Pemerintah Pusat	2021
				2	Direktorat Keamanan Siber Pemerintah Daerah	
8	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.	Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi	1	Direktorat Operasi Keamanan Siber	2022
9	Peraturan BSSN terkait *Voluntary*	Tindak lanjut dasar hukum dan panduan penyelenggaraan Program serta untuk	Direktorat Kebijakan Tata	1	Deputi Bidang Operasi Keamanan	2023

	Vulnerability Disclosure Program (VVDP)	memberikan kepastian hukum kepada pencari kerentanan yang berpartisipasi di dalam Program dalam rangka finalisasi Rancangan Peraturan BSSN tentang Penyelenggaraan Program VVDP.	Kelola Keamanan Siber dan Sandi	2 Deputi Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia 3 Deputi Keamanan Siber dan Sandi Perekonomian	
10	Penyusunan peraturan CSIRT Sektoral (CII SIRT)	Tindak lanjut Naskah Akademik tentang Keamanan dan Ketahanan Siber dalam mengoordinasikan kejadian yang berkaitan dengan keamanan siber. 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.	Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi	1 Deputi Bidang Operasi Keamanan Siber dan Sandi 2 Deputi Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia 3 Deputi Keamanan Siber dan Sandi Perekonomian	2023

11	Peraturan BSSN tentang *Roadmap* 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 semakin nyata, sehingga perlu dipersiapkan pendekatan dan strategi yang tepat untuk menjembatani antara kualitas lulusan pendidikan dengan kebutuhan sumber daya manusia di dunia kerja, sehing 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 agar tercipta *link and match* diantara keduanya.	Direktorat Kebijakan Sumber Daya Manusia Keamanan Siber dan Sandi	-	2023	

12	Peraturan BSSN terkait Penyelenggaraan Sertifikat Elektronik	Peraturan Kepala Badan Siber dan Sandi Negara tentang Penyelenggaraan Sertifikat Elektronik merupakan Perubahan atas Peraturan Kepala Lemsaneg Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik. Peraturan tersebut sebagai turunan dari peraturan di atasnya (UU ITE, PP PSTE, Peraturan Presiden SPBE). Sehubungan dengan hal tersebut perlu pengaturan tentang tata kelola penyelenggaraan sertifikat elektronik dalam rangka dukungan keamanan informasi dalam pelaksanaan *e-government*.	Balai Sertifikasi Elektronik	-	2022

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd

HINSA SIBURIAN