[logo]

DRAFT LAW
NUMBER … OF …
CONCERNING
CYBER SECURITY AND RESILIENCE

LEGISLATION COMMITTEE
HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA
JAKARTA, MAY 2019

DRAFT

LAW OF THE REPUBLIC OF INDONESIA

NUMBER ... OF ...

CONCERNING

CYBER SECURITY AND RESILIENCE

BY THE GRACE OF GOD ALMIGHTY

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that in order to achieve the objective of forming a Government of Indonesia that protects all Indonesian people and the entire land of Indonesia, promotes the welfare of the people, enriches the life of the nation, and participates in the creation of world order, as mandated in the preamble of the 1945 Constitution of the Republic of Indonesia, the Republic of Indonesia implements cyber security and resilience;

b. that the implementation of cyber security and resilience is faced with the risk of cyber threats that jeopardize the national interest, as well as it is necessary to strengthen the cyber resources management in a synergic, collaborative, competitive, and professional manner;

c. that the implementation of cyber security and resilience needs to be regulated in a law to accommodate the legal developments and needs of the people;

d. that based on the considerations as referred to in letter a, letter b, and letter c, it is necessary to stipulate a Law concerning Cyber Security and Resilience;

In view of: Article 4 paragraph (1), Article 20, Article 21, Article 28F, Article 28G paragraph (1), Article 28J, and Article 33 paragraph (2) of the 1945 Constitution of the Republic of Indonesia;

Upon Joint Approval of
THE HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA
and
THE PRESIDENT OF THE REPUBLIC OF INDONESIA

HAS DECIDED:

To stipulate: LAW CONCERNING CYBER SECURITY AND RESILIENCE.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Law:

1. Cyber means the global space accommodating the various interests shaped by the interaction between human and information technology, computerization, computer network, cryptography, and/or artificial intelligence.
2. Cyber Security and Resilience mean the dynamic Cyber condition encompassing all aspects of the national life that is integrated, secure, and resilient, as well as able to develop Indonesia’s Cyber strength in facing all Cyber threats against Indonesia’s Cyber interest and resources controlled by the Republic of Indonesia.

3. Indonesia's Cyber Interest means the safety of the nation, security, sovereignty, integrity of the territory of the Republic of Indonesia, and national interest in various aspects, whether ideology, politics, economy, socio-culture, or defense and security, in the Cyber space.
4. Cyber Threat means all attempts, activities, and/or actions, whether domestic or foreign, considered and/or proven to possibly weaken, harm, and/or impair Indonesia's Cyber Interest.
5. Cyber Incident means the Cyber Threat causing a Cyber electronic system to malfunction.
6. Cyber Attack means the Cyber Threat causing an object of Cyber security to be inoperable, in part or in whole, and/or temporarily or permanently.
7. Object of Cyber Security means the data, information, facilities and infrastructures, as well as human resources receiving protection from the Cyber Security and Resilience provider.
8. Security Perimeter means the area in the Cyber and non-Cyber space accessible only to a person with Cyber Security and Resilience clearance.
9. Detection means the effort to detect the presence, scale, and distance of a Cyber Threat from the Security Perimeter.
10. Identification means the effort to identify and analyze the level of hazard, cause, and effect of a detected Cyber Threat.
11. Protection means the effort to protect an Object of Cyber Security from Cyber Threat to maintain the functionality of the Object of Cyber Security against damage or loss, in part or in whole.
12. Countermeasure means the effort to alleviate, eliminate, minimize the impact, and/or prevent the exacerbation of impact of an existing Cyber Incident or Cyber Attack.
13. Recovery means the effort to remedy the adverse impact or recover the loss caused by a Cyber Incident or Cyber Attack and restore the functionality of the Object of Cyber Security.

14. Monitoring means the effort to learn about the dynamics and trends relating to Cyber Incident or Cyber Attack in order to formulate an effective and efficient strategy and tactic within the scope of Cyber Security and Resilience.
15. Control means the effort to maintain and strengthen the ecosystem of Cyber Security and Resilience.
16. Accreditation means the acknowledgement of meeting specific standards in the education, training, and examination of human resources competency sector within the scope of Cyber Security and Resilience.
17. Electronic Certificate means the cryptographic algorithm-based certificate issued as a digital marker or identity of a person, computer, electronic system, data, electronic document, and/or Cyber network.
18. National Cyber and Encryption Agency (*Badan Siber dan Sandi Negara*), hereinafter abbreviated as BSSN, means the agency overseeing government affairs in the Cyber Security and Resilience sector under this Law.
19. Central Government means the President of the Republic of Indonesia holding the power of the government of the Republic of Indonesia, assisted by the Vice President and ministers as referred to in the 1945 Constitution of the Republic of Indonesia.
20. Regional Government means the head of regional government as the element of the Regional Government overseeing government affairs that fall under the authority of an autonomous region.
21. Person means a private person or a legal person.

CHAPTER II
PRINCIPLES AND OBJECTIVES

Article 2

Cyber Security and Resilience shall be based on the principles of:

a. sovereignty;
b. trustworthiness;
c. professionalism;
d. readiness;
e. competitiveness;
f. legal certainty; and
g. collaboration.

Article 3

Cyber Security and Resilience shall have the objectives of:

a. protecting the integrity and sovereignty of the state from Cyber Threat;
b. improving Cyber competitiveness and innovation through free, open, and responsible Cyber utilization;
c. supporting the development and advancement of digital economy in the aspects of Cyber industry governance, facility and infrastructure security, and national Cyber resources; and
d. consolidating in a synergic and collaborative manner all elements involved in the implementation of Cyber Security and Resilience to achieve the national objective and have free and active participation in anticipating Cyber Threat for the purpose of world peace.

CHAPTER III
IMPLEMENTATION OF CYBER SECURITY AND RESILIENCE

Part One
General

Article 4

(1) The State shall be responsible for implementing Cyber Security and Resilience.

(2) The Cyber Security and Resilience as referred to in paragraph (1) shall be implemented by state agencies, Central Government, Regional Governments, and/or the public.

(3) The Central Government shall assign BSSN to coordinate and collaborate on the implementation of Cyber Security and Resilience to be in line with Indonesia's Cyber Interest.

Article 5

The implementation of Cyber Security and Resilience must prioritize the:

a. advancement of Indonesia's Cyber Interest;

b. respect for human rights;

c. independence in science and technology innovation; and

d. advancement of the national economy.

Part Two

Cyber Security and Resilience Provider

Article 6

The Cyber Security and Resilience provider shall consist of:

a. state agencies;

b. Central Government; and

c. Regional Governments.

Article 7

(1) The Cyber Security and Resilience provider in a state agency as referred to in Article 6 letter a shall be the responsibility of the leadership of the state agency carried out by the secretariat of the state agency.

(2) The Cyber Security and Resilience provider in the Central Government as referred to in Article 6 letter b shall consist of:

a. BSSN;

b. Cyber division at the Indonesian National Armed Forces;

c. Cyber division at the Indonesian National Police;

d. Cyber division at the Attorney General's Office of the Republic of Indonesia;

e. Cyber division at the Indonesian State Intelligence Agency; and

f. Cyber division at ministries/non-ministerial institutions other than as referred to in letter a, letter b, letter c, letter d, and letter e.

(3) The Cyber Security and Resilience provider in a Regional Government as referred to in Article 6 letter c shall consist of:

a. Cyber division at Provincial Governments; and

b. Cyber division at district/city Governments.

(4) The Cyber Security and Resilience as referred to in paragraph (2) letter a to letter e shall be implemented according to the respective scope of duties and functions based on the laws and regulations.

(5) The Cyber Security and Resilience as referred to in paragraph (1), paragraph (2) letter f, and paragraph (3) shall be implemented on a limited basis for the purpose of Cyber Security and Resilience within the scope of their internal organization.

Article 8

(1) Cyber Security and Resilience other than as referred to in Article 6 can be implemented by the public.

(2) The Cyber Security and Resilience implemented by the public as referred to in paragraph (1) shall be limited to the following activities:

a. protection of electronic system within the scope of internal organization; and/or

b. provision of services in the Cyber Security and Resilience sector.

Part Three

Coordination and Collaboration of Cyber Security and Resilience Provider

Article 9

(1) The coordination and collaboration as referred to in Article 4 paragraph (3) shall be carried out through:
   a. regular meetings;
   b. institutional and human resources capacity building;
   c. countermeasure and recovery training;
   d. joint tactical activities; and/or
   e. technical and non-technical support for facility and infrastructure capacity building, human resources competency building; and/or
   f. cooperation network expansion.

(2) The coordination and collaboration as referred to in paragraph (1) shall be consolidated by BSSN.

(3) Further provisions on the coordination and collaboration as referred to in paragraph (1) and paragraph (2) shall be stipulated in a Government Regulation.

CHAPTER IV

CYBER SECURITY AND RESILIENCE GOVERNANCE

Part One

General

Article 10

(1) Cyber Security and Resilience shall be implemented for the Object of Cyber Security on the national Cyber infrastructures.

(2) The national Cyber infrastructures as referred to in paragraph (1) shall consist of:

a. national critical information infrastructures, including public key infrastructures;

b. electronic-based government administration infrastructures;

c. national digital economic infrastructures; and

d. other electronic system infrastructures in accordance with the laws and regulations.

(3) The national Cyber infrastructures as referred to in paragraph (2) shall be compiled into a list.

(4) The list as referred to in paragraph (3) shall be stipulated in a BSSN Regulation.

Article 11

(1) Cyber Security and Resilience shall be implemented to mitigate risk and respond to Cyber Threat.

(2) The Cyber Threat as referred to in paragraph (1) shall consist of:

a. Cyber Incident within the Security Perimeter;

b. Cyber Attack on the Object of Cyber Security;

c. malicious software;

d. destructive and/or negative content;

e. product, product prototype, product design, or invention that can be used as a Cyber weapon;

f. deliberate attempt intended to weaken, harm, and/or impair Indonesia's Cyber Interest; and/or

g. other forms of Cyber Threat.

Part Two

Cyber Threat Risk Mitigation

Article 12

(1) Any Cyber Security and Resilience provider must mitigate Cyber Threat risk to protect the Object of Cyber Security under their purview.

(2) The risk as referred to in paragraph (1) shall be mitigated by:

a. making a copy of every software required to operate the electronic system;

b. making a regular copy of data in the electronic system to be used as backup;

c. saving the copies as referred to in letter a and letter b in a different electronic system than the source of the copies;

d. operating a Cyber Security and Resilience operations center;

e. managing access to the Security Perimeter under their purview;

f. regularly changing the access code to the electronic system;

g. preparing a standard operating procedure for Cyber Threat risk mitigation, and regularly running a simulation of the procedure for human resources within the scope of internal organization; and

h. making other risk mitigation efforts in accordance with this Law.

Article 13

(1) The Cyber Threat risk as referred to in Article 12 shall be mitigated according to the specific standards set by BSSN.

(2) BSSN shall govern and assess the conformity of the Cyber Threat risk mitigation as referred to in paragraph (1).

Part Three

Cyber Threat Response

Article 14

(1) Every Cyber Security and Resilience provider must respond to Cyber Threat to protect the Object of Cyber Security under their purview.

(2) The response as referred to in paragraph (1) shall be made by:

a. inspecting the integrity, availability, and functionality of the Object of Cyber Security under their purview at the time the Cyber Incident or Cyber Attack becomes known;

b. recording and reporting every Cyber Incident or Cyber Attack against the Object of Cyber Security under their purview to BSSN;

c. analyzing the level of hazard of the Cyber Incident or Cyber Attack against the Object of Cyber Security under their purview;

d. deleting any malicious software from their electronic system;

e. temporarily stop using the electronic system infected by the Cyber Threat;

f. disconnecting data connection from the electronic system to any other electronic system suspected of being the source of the Cyber Threat;

g. taking actions recommended by BSSN to stop the Cyber Incident or Cyber Attack against the Object of Cyber Security under their purview from spreading or causing harm;

h. notifying electronic system users or customers of the Cyber Threat response made to protect the Object of Cyber Security under their purview; and/or

i. taking other actions as a Cyber Threat response in accordance with this Law.

Article 15

(1) The level of hazard of Cyber Threat as referred to in Article 14 paragraph (2) letter c shall consist of:

a. no hazard;

b. low hazard;

c. medium hazard; and

d. high hazard.

(2) Provisions on the criteria of each level of hazard as referred to in paragraph (1) shall be stipulated in a Government Regulation.

Article 16

(1) The Cyber Threat response as referred to in Article 14 and Article 15 must refer to the specific standards set by BSSN.

(2) BSSN shall govern and assess the conformity of the Cyber Threat response as referred to in paragraph (1).

Part Four

Cyber Device

Article 17

(1) Any Cyber Device used in the implementation of Cyber Security and Resilience on the national Cyber infrastructures must have product certification.

(2) The product certification as referred to in paragraph (1) shall be issued by BSSN.

(3) Provisions on the product certification as referred to in paragraph (1) shall be stipulated in a BSSN Regulation.

Part Five

Service Provider in the Cyber Security and Resilience Sector

Article 18

(1) The service provider in the Cyber Security and Resilience sector as referred to in Article 8 paragraph (2) letter b must have a license.

(2) The license as referred to in paragraph (1) shall be issued for the following business activities:

a. Cyber Security and Resilience system management;

b. electronic system access security penetration testing; and

c. cryptographic algorithm development.

(3) The license as referred to in paragraph (1) shall be issued by BSSN.

(4) Provisions on the license as referred to in paragraph (1) shall be stipulated in a BSSN Regulation.

Part Six
Human Resources Competency

Article 19

(1) Any Cyber Security and Resilience provider must employ human resources with competency in the Cyber Security and Resilience sector.

(2) The competency as referred to in paragraph (1) shall refer to the specific standards set by BSSN.

Article 20

(1) Any Cyber Security and Resilience provider may conduct a business activity in the education or training sector to meet the specific standards as referred to in Article 19 paragraph (2).

(2) The business activity as referred to in paragraph (1) must have accreditation from BSSN.

Article 21

(1) To improve human resources capability and professionalism, any Cyber Security and Resilience providers that are members of the public may form an association and establish a professional organization in the Cyber Security and Resilience sector.

(2) The professional organization as referred to in paragraph (1) may issue certificate of professional competency to human resources meeting the specific standards as referred to in Article 19 paragraph (2).

(3) The certificate of professional competency as referred to in paragraph (2) may only be issued by a professional organization having accreditation as professional certification agency.

(4) The accreditation as referred to in paragraph (3) shall be granted by BSSN on the recommendation of the authorized professional advisory institution in accordance with the laws and regulations.

Part Seven
Governance Enforcement

Article 22

(1) Any Cyber Security and Resilience provider not meeting the specific standards as referred to in Article 13 paragraph (1), Article 16 paragraph (1), and Article 19 paragraph (2) shall be imposed with an administrative sanction.

(2) The administrative sanction as referred to in paragraph (1) shall consist of:
   a. warning;
   b. rejection of Cyber Security and Resilience clearance application;
   c. temporary suspension of Cyber Security and Resilience clearance;
   d. permanent revocation of Cyber Security and Resilience clearance;
   e. temporary suspension of service provider license;
   f. permanent revocation of service provider license;
   g. temporary suspension or blocking of electronic system operations;
   h. permanent termination or blocking of electronic system operations; and/or
   i. imposition of an administrative fine.

Article 23

(1) Any Cyber Security and Resilience provider not using the certified Cyber device as referred to in Article 17 paragraph (2) shall be imposed with an administrative sanction.

(2) The administrative sanction as referred to in paragraph (1) shall consist of:
   a. warning;
   b. temporary suspension or blocking of electronic system operations;
   c. permanent termination or blocking of electronic system operations; and/or
   d. imposition of an administrative fine.

Article 24

(1) Any service provider in the Cyber Security and Resilience sector not having the license in conducting their business activities as referred to in Article 18 paragraph (3) shall be imposed with an administrative sanction.

(2) The administrative sanction as referred to in paragraph (1) shall consist of:
   a. warning;
   b. temporary suspension or blocking of electronic system operations;
   c. permanent termination or blocking of electronic system operations; and/or
   d. imposition of an administrative fine.

Article 25

(1) Any Cyber Security and Resilience provider conducting the business activity in the education and training sector as referred to in Article 20 paragraph (2) without accreditation shall be imposed with an administrative sanction.

(2) The administrative sanction as referred to in paragraph (1) shall consist of:
   a. warning;
   b. temporary suspension or blocking of electronic system operations;

c. permanent termination or blocking of electronic system operations; and/or

d. imposition of an administrative fine.

Article 26

(1) Any professional organization issuing the certificate of professional competency as referred to in Article 21 without accreditation shall be imposed with an administrative sanction.

(2) The administrative sanction as referred to in paragraph (1) shall consist of:

a. warning;

b. temporary suspension or blocking of electronic system operations;

c. permanent termination or blocking of electronic system operations; and/or

d. imposition of an administrative fine.

Article 27

(1) Any Cyber Security and Resilience provider imposed with the administrative sanction as referred to in Article 22 to Article 26 shall have the right to raise a defense.

(2) Further provisions on the administrative sanction and defense as referred to in paragraph (1) shall be stipulated in a Government Regulation.

Part Eight

Risk of Loss and Loss Coverage

Article 28

(1) Any Person sustaining a loss due to the implementation of Cyber Security and Resilience function and/or activity may file an application for rehabilitation, compensation, and/or restitution.

(2) The rehabilitation, compensation, and/or restitution as referred to in paragraph (1) shall be applied for in accordance with the laws and regulations.

Article 29

(1) Any Cyber Security and Resilience provider may procure Cyber insurance services to cover the risk of loss caused by Cyber Incident or Cyber Attack.

(2) The Cyber insurance services as referred to in paragraph (1) shall be provided by an Indonesian insurance provider.

Article 30

(1) The Cyber insurance service provider as referred to in Article 29 paragraph (2) must employ human resources with competency in the Cyber Security and Resilience sector.

(2) The human resources as referred to in paragraph (1) shall at least include:
a. Cyber risk underwriter; and
b. Cyber loss adjuster.

(3) The competency of human resources as referred to in paragraph (1) shall be evidenced by certificate of competency issued by BSSN.

(4) Further provisions on the certificate of competency as referred to in paragraph (2) shall be stipulated in a BSSN Regulation.

CHAPTER V
CYBER SECURITY AND RESILIENCE SERVICES

Part One
Cyber Security and Resilience Operations Center

Article 31

(1) In order to carry out Cyber Security and Resilience activities, every Cyber Security and Resilience provider must establish a Cyber Security and Resilience operations center.

(2) The Cyber Security and Resilience operations center as referred to in paragraph (1) must be connected to the national Cyber Security and Resilience operations center.

(3) Any Cyber Security and Resilience operations center operated by micro, small, and medium enterprises and cooperatives shall be exempted from the provision as referred to in paragraph (2).

(4) The national Cyber Security and Resilience operations center as referred to in paragraph (2) shall be operated by BSSN.

Article 32

The Cyber Security and Resilience operations center as referred to in Article 31 paragraph (1) shall provide services consisting of:

a. operating a point of contact or contact center for reporting any suspected impending or existing Cyber Incident or Cyber Attack;

b. processing the suspected Cyber Incident or Cyber Attack report for a follow-up action; and

c. providing information on the status and progress of the suspected Cyber Incident or Cyber Attack report to the informer.

Article 33

Technical provisions on the operating procedure for the Cyber Security and Resilience operations center as referred to in Article 31 and Article 32 shall be stipulated in a BSSN Regulation.

Part Two

Cyber Security and Resilience Culture Development

Article 34

Every Cyber Security and Resilience provider must make efforts to develop a Cyber Security and Resilience culture to improve the quality of risk management in Cyber utilization.

Article 35

The efforts to develop a Cyber Security and Resilience culture as referred to in Article 34 shall consist of:

a. managing information and documentation related to Cyber Security and Resilience; and
b. organizing promotional activities, technical guidance, and/or scientific activities to improve public literacy and awareness about Cyber Security and Resilience; and
c. rewarding every Person participating in achieving the objectives of Cyber Security and Resilience implementation.

CHAPTER VI

CYBER DIPLOMACY

Article 36

(1) In order to advance Indonesia's Cyber Interest at the international level and participate in maintaining the world peace, it is necessary to implement Cyber diplomacy through a series of efforts using diplomatic methods and means within the scope of Cyber Security and Resilience.
(2) The efforts of Cyber diplomacy as referred to in paragraph (1) shall include:
    a. participating in creating, formulating, promoting proposals or initiatives for international concepts, norms, behaviors, and guidelines in bilateral, regional, or multilateral Cyber Security and Resilience;

b. participating in Cyber Security and Resilience problem solving activities in bilateral, regional, or multilateral forums;
c. participating in administering international regime in the Cyber Security and Resilience sector at the regional or multilateral level;
d. establishing partnerships, cooperation, and mutual relations with various countries and/or international organizations to improve the national Cyber resilience, prevent Cyber abuse, and/or raise awareness about different Cyber concepts and governance in the world;
e. encouraging countries in the region to build Cyber Security and Resilience capacity and maintain a common system to exchange situational information on Cyber Security and Resilience vulnerability, threats, and incidents;
f. organizing activities, meetings, or workshops to disseminate Indonesia's Cyber Security and Resilience concept and/or policy to other countries; and
g. making other efforts in accordance with the laws and regulations and/or international laws.

Article 37

(1) The Cyber diplomacy as referred to in Article 36 shall be implemented by BSSN.
(2) BSSN shall collaborate and coordinate with the ministry overseeing foreign affairs to implement the Cyber diplomacy as referred to in paragraph (1).
(3) In order to ensure effective implementation of the Cyber diplomacy as referred to in paragraph (1) and paragraph (2), the ministry overseeing foreign affairs shall:
a. propose to the President the appointment of ambassadors to specifically handle diplomatic relations in the Cyber Security and Resilience sector; and

b. designate the position of Cyber Security and Resilience attaché to certain diplomatic representatives.

CHAPTER VII
LAW ENFORCEMENT

Part One
Electronic Content and Application Filtering

Article 38

(1) BSSN shall filter any electronic content and application containing malicious software to support the efforts to protect electronic application users.

(2) Provisions on the operating procedure for the electronic content and application filtering as referred to in paragraph (1) shall be stipulated in a BSSN Regulation.

Part Two
Prosecution

Article 39

(1) BSSN shall prosecute any Person proven to have committed a Cyber Security and Resilience violation.

(2) The prosecution as referred to in paragraph (1) shall consist of:

a. imposition of an administrative sanction;

b. submission of investigation results to the competent authority in criminal investigation;

c. filing of a claim for damages; and/or

d. other actions in accordance with the laws and regulations.

(3) Technical provisions on the operating procedure for the prosecution as referred to in paragraph (1) and paragraph (2) shall be stipulated in a BSSN Regulation.

Part Three

Support for Law Enforcement Process

Article 40

(1) For the purpose of law enforcement process, BSSN shall provide support for civil and criminal case examination processes.

(2) The support for civil case examination process as referred to in paragraph (1) shall be provided during the evidentiary stage of the trial.

(3) The support for criminal case examination process as referred to in paragraph (1) shall be provided during the preliminary investigation, investigation, and/or evidentiary stage of the trial.

(4) The support as referred to in paragraph (1) shall be provided by BSSN in accordance with the laws and regulations.

CHAPTER VIII

BSSN

Part One

Position

Article 41

BSSN works under and is responsible to the President.

Part Two

Duties and Functions

Article 42

(1) BSSN shall have the duties to:
   a. oversee government affairs in the Cyber Security and Resilience sector in an effective and efficient manner;
   b. utilize, develop, and consolidate all stakeholder elements related to Cyber Security and Resilience; and
   c. supervise the use of cryptographic products and the implementation of state cryptography.

(2) The performance of the duty as referred to in paragraph (1) letter c shall be stipulated in a separate law.

Article 43

BSSN shall serve the functions of:

a. Cyber Security and Resilience governance;
b. Cyber Security and Resilience services;
c. Cyber diplomacy;
d. support for law enforcement; and
e. advisory in the implementation of Electronic Certification.

Part Three

Authority

Article 44

BSSN shall have the authority to:

a. establish and enforce regulations, specific standards, and/or operating procedures in the Cyber Security and Resilience sector on a national scale;
b. formulate Cyber Security and Resilience strategic frameworks and technical frameworks;

c. make efforts to achieve Cyber Security and Resilience for Indonesia at home and abroad;
d. determine the Security Perimeter;
e. issue, suspend, or revoke licenses, certification, or accreditation within the scope of Cyber Security and Resilience;
f. conduct investigations, prosecutions, and impose administrative sanctions;
g. perform assessment, testing, penetration of electronic system access security, and/or audit of Cyber Security and Resilience; and
h. provide support for criminal and civil law enforcement processes.

Article 45

(1) In order to support the criminal law enforcement process as referred to in Article 44 letter h, BSSN shall:
    a. analyze digital evidence;
    b. provide expert testimony in digital forensics; and/or
    c. provide Cyber Security and Resilience technical support during the preliminary investigation and investigation stages.
(2) The support for criminal law enforcement process as referred to in paragraph (1) shall be provided by BSSN upon a written request from the preliminary investigator, investigator, and/or public prosecutor to BSSN.
(3) The support for civil law enforcement process as referred to in Article 44 letter h shall be provided by BSSN upon a written request from the court.
(4) The support for criminal and civil law enforcement as referred to in paragraph (2) and paragraph (3) shall be provided in accordance with the laws and regulations.

Article 46

In addition to the authority as referred to in Article 44, BSSN shall perform Detection, Identification, Protection, Countermeasure, Recovery, Monitoring, and

Control of the Object of Cyber Security as referred to in Article 10 paragraph (2) at home and abroad.

Article 47

For the purpose of the Detection as referred to in Article 46, BSSN shall carry out the following activities:

a. Detection of Cyber Threat against data traffic;
b. Detection of Cyber Threat related to socio-cultural behavior;
c. Detection of potential Cyber Threat;
d. signal intelligence;
e. assessment, testing, and penetration of electronic system access security to identify vulnerabilities and security gaps related to the National Cyber Infrastructures;
f. granting of authorization for activities of researching and testing the strength of Cyber Security and Resilience; and
g. other Detection activities in accordance with the laws and regulations.

Article 48

For the purpose of the Identification as referred to in Article 44 [*sic*], BSSN shall carry out the following activities:

a. Identification of Cyber Threat against data traffic;
b. Identification of Cyber Threat related to socio-cultural behavior;
c. Identification of potential Cyber Threat;
d. analysis of signal intelligence;
e. analysis of assessment, testing, and penetration of electronic system access security related to the National Cyber Infrastructures;
f. granting of authorization for activities of researching and testing the strength of Cyber Security and Resilience; and
g. other Identification activities in accordance with the laws and regulations.

Article 49

For the purpose of the Protection as referred to in Article 44 [*sic*], BSSN shall carry out the following activities:

a. governance of cryptographic algorithm utilization;
b. issuance of Electronic Certificate on the national Cyber infrastructures;
c. protection of intra Cyber network of Cyber Security and Resilience providers;
d. audit of implementation of security standards;
e. planning of state cryptographic device needs;
f. maintenance of state cryptographic devices;
g. management of password system key used for state cryptography;
h. protection of frequency or signal wave security;
i. counter sensing;
j. grant management; and
k. advising of Cyber Security and Resilience communities.

Article 50

For the purpose of the Countermeasure as referred to in Article 44 [*sic*], BSSN shall carry out the following activities:

a. management of information center to countermeasure Cyber Threat;
b. consolidation of efforts to countermeasure Cyber Threat; and
c. consolidation of various countermeasure efforts to maintain the operational continuity of the national Cyber infrastructures.

Article 51

For the purpose of the Recovery as referred to in Article 44 [*sic*], BSSN shall carry out the following activities:

a. dissemination of information to raise awareness about Cyber Security and Resilience;

b. investigation to attempt to recover losses or lost National Cyber Infrastructures; and
c. follow-up actions to investigation results through administrative efforts and/or other loss recovery efforts in accordance with the laws and regulations.

Article 52

For the purpose of the Monitoring as referred to in Article 44 [*sic*], BSSN shall carry out the following activities:

a. governance of data and information related to the origin of past Cyber Incident or Cyber Attack all over the world;
b. governance of data and information related to the impact of past Cyber Incident or Cyber Attack all over the world;
c. study of data and information related to Cyber Incident or Cyber Attack to formulate the best strategy and tactic to respond to various developments in Cyber Threat against the Republic of Indonesia.

Article 53

For the purpose of the Control as referred to in Article 44 [*sic*], BSSN shall carry out the following activities:

a. licensing of service providers in the Cyber Security and Resilience sector;
b. certification of Cyber devices provided to be used on the national Cyber infrastructures;
c. certification of Cyber risk underwriters and Cyber loss adjusters;
d. accreditation of education and training institutions in the Cyber Security and Resilience sector; and
e. accreditation of professional certification agencies in the Cyber Security and Resilience sector.

Part Four

Organization

Article 54

BSSN consists of:

a. Head;

b. Vice Head;

c. Main Secretariat;

d. Deputies;

e. Main Inspectorates; and

f. centers and/or other work units in accordance with the applicable rules and regulations.

Article 55

(1) BSSN is led by a Head, assisted by a Vice Head.

(2) The appointment and dismissal of the Head of BSSN and the Vice Head of BSSN as referred to in paragraph (1) shall be stipulated in a Presidential Decree.

Article 56

(1) The Head of BSSN shall be granted remuneration rights and facilities of a level equivalent to a minister.

(2) The Vice Head of BSSN shall be granted remuneration rights and facilities of a level equivalent to a vice minister.

Article 57

(1) In order to ensure effectiveness and efficiency in coordination and collaboration with Regional Governments, BSSN shall establish representative offices.

(2) The organizational structure and administration of the representative offices as referred to in paragraph (1) shall be determined by BSSN.

Article 58

(1) In order to meet human resources needs to perform the duties, functions, authority, and activities of BSSN within the scope of Cyber Security and Resilience, BSSN shall provide service-related education.

(2) The organizational structure and administration of the service-related education as referred to in paragraph (1) shall be determined by BSSN.

Article 59

(1) In order to implement Cyber Security in the electronic-based government administration, BSSN shall provide Electronic Certificate issuance services.

(2) The Electronic Certificate issuance services as referred to in paragraph (1) shall include:

a. management of cryptographic algorithm-based Electronic Certificate issuance for creating electronic signature and authenticating identity of a Person;

b. management of cryptographic algorithm-based Electronic Certificate issuance for creating electronic signature and authenticating computer or electronic system;

c. management of cryptographic algorithm-based Electronic Certificate issuance for creating electronic signature and authenticating computer network or cyber network; and

d. management of cryptographic algorithm-based Electronic Certificate issuance for creating electronic signature and authenticating electronic data or document.

(3) The Electronic Certificate issuance services as referred to in paragraph (1) and paragraph (2) can be provided to parties external to the Electronic-Based Government System upon request.

(4) The organizational structure and administration of the Electronic Certificate issuance services as referred to in paragraph (1) shall be determined by BSSN.

Article 60

Further provisions on the organization of BSSN as referred to in Article 54 to Article 59 shall be stipulated in a Presidential Regulation.

Article 61

(1) Cyber Security and Resilience in a state of war shall be implemented under the direct control of the President.

(2) The implementation of Cyber Security and Resilience in a state of war as referred to in paragraph (1) must obtain the approval of the House of Representatives.

CHAPTER IX

FUNDING AND PROCUREMENT

Article 62

(1) The funding for the implementation of Cyber Security and Resilience shall be derived from:
   a. State Budget;
   b. regional budgets;
   c. national Cyber Security and Resilience development funds;
   d. grants; and/or
   e. other legitimate and non-binding sources of funding in accordance with the laws and regulations.

(2) The grants as referred to in paragraph (1) letter d can be in the form of:
   a. money;

b. goods;
c. facilities;
d. equipment; and/or
e. services.

Article 63

(1) The money grants as referred to in Article 62 paragraph (2) letter a shall be deposited to the national Cyber Security and Resilience development funds and managed by BSSN.

(2) The managed national Cyber Security and Resilience development funds as referred to in paragraph (1) shall be used for:
a. human resources development;
b. research;
c. grants and awards; and/or
d. reserve funds to anticipate contingency needs due to Cyber Incident and/or Cyber Attack.

(3) Further provisions on the management of national Cyber Security and Resilience development funds as referred to in paragraph (1) and paragraph (2) shall be stipulated in a Government Regulation.

Article 64

(1) The goods, facilities, equipment, and/or services grants as referred to in Article 62 paragraph (2) letter b, letter c, letter d, and letter e shall be managed by BSSN.

(2) The managed goods, facilities, equipment, and/or services grants as referred to in paragraph (1) shall be used for capacity building in the national Cyber Security and Resilience implementation.

(3) Further provisions on the management of goods, facilities, equipment, and/or services grants as referred to in paragraph (1) and paragraph (2) shall be stipulated in a BSSN Regulation.

Article 65

(1) The Central Government and Regional Governments must allocate Cyber Security and Resilience implementation funds in the State Budget and Regional Budgets.

(2) The Cyber Security and Resilience implementation funds as referred to in paragraph (1) shall be allotted for:

a. human resources development; and

b. development and/or reinforcement of Cyber Security and Resilience devices and infrastructures.

(3) Further provisions on the allocation and allotment of Cyber Security and Resilience implementation funds as referred to in paragraph (1) and paragraph (2) shall be stipulated in a Government Regulation.

Article 66

(1) The development and/or reinforcement of Cyber Security and Resilience devices and infrastructures as referred to in Article 65 paragraph (2) letter b must fulfill the 50% (fifty percent) local content requirement.

(2) The 50% (fifty percent) local content requirement as referred to in paragraph (1) shall apply to each procurement of hardware and/or software.

(3) The 50% (fifty percent) local content requirement as referred to in paragraph (1) shall be implemented by the ministry overseeing government affairs in the industrial sector in coordination with BSSN.

(4) Further provisions on the fulfillment of 50% (fifty percent) local content requirement shall be stipulated in a Government Regulation.

Article 67

(1) The hardware and software as referred to in Article 66 paragraph (2) may be procured in certain conditions by direct appointment or direct procurement.

(2) The direct appointment or direct procurement in certain conditions as referred to in paragraph (1) shall be carried out in the event of:
   a. emergency management for public security and safety;
   b. complex works that can only be carried out by a very limited number of service providers in the Cyber Security and Resilience sector or can only be carried out by right holders;
   c. confidential works related to national security and safety; and/or
   d. small-scale works.

(3) The direct appointment or direct procurement as referred to in paragraph (1) shall be carried out in accordance with the laws and regulations.

CHAPTER X
PROHIBITION

Article 68

Any Person shall be prohibited from deliberately and unrightfully or illegally committing any action that causes interference and/or malfunction of the National Cyber infrastructures.

Article 69

Any Person shall be prohibited from deliberately and unrightfully or illegally manufacturing, distributing, or supplying any device designed or developed specifically to facilitate the action as referred to in Article 68.

CHAPTER XI

CRIMINAL PROVISIONS

Article 70

Any Person committing the action as referred to in Article 68 shall be subject to an imprisonment of a maximum of 10 (ten) years and/or a fine of a maximum of Rp10,000,000,000 (ten billion rupiah) based on the magnitude of damage caused.

Article 71

Any Person committing the action as referred to in Article 69 shall be subject to an imprisonment of a maximum of 10 (ten) years and/or a fine of a maximum of Rp10,000,000,000 (ten billion rupiah) based on the magnitude of damage caused.

Article 72

(1) The criminal provisions as referred to in Article 70 and Article 71 shall not apply to any Person researching and/or testing the strength of Cyber Security and Resilience on the national Cyber infrastructures.
(2) Any Person conducting the research and/or testing as referred to in paragraph (1) must be registered and have a license from BSSN.
(3) Provisions on the procedures for the research, testing, registration, and licensing as referred to in paragraph (2) shall be stipulated in a BSSN Regulation.

CHAPTER XII
TRANSITIONAL PROVISIONS

Article 73

Upon the entry into force of this Law, all laws and regulations concerning Cyber Security and Resilience shall be declared to remain valid insofar as the same is not in contravention of this Law.

Article 74

Any organization or agency that is an existing element of the Cyber Security and Resilience implementation shall survive until the same is modified or replaced with a new organization or agency in accordance with this Law.

Article 75

BSSN must make adjustments according to this Law no later than 2 (two) years as of the entry into force of this Law.

CHAPTER XIII
CLOSING PROVISIONS

Article 76

(1) The implementing regulations of this Law must already be stipulated no later than 1 (one) year as of the promulgation of this Law.
(2) The Central Government must report the implementation of this Law to the House of Representatives no later than 3 (three) years following the entry into force of this Law.

Article 77

This Law shall enter into force on the date of its promulgation.

In order that it is known by the public, it is ordered that this Law is promulgated by its placement on the State Gazette of the Republic of Indonesia.

Ratified in Jakarta
on …
PRESIDENT OF THE REPUBLIC OF INDONESIA,

JOKO WIDODO

Promulgated in Jakarta
on …
MINISTER OF LAW AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,

YASONNA LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER … OF …

DRAFT ELUCIDATION OF
LAW OF THE REPUBLIC OF INDONESIA
NUMBER ... OF ...
CONCERNING
CYBER SECURITY AND RESILIENCE

I. GENERAL

Cyber system has become a vital necessity for the Indonesian people and nation. The clear indication is that today's society relies heavily on internet access and gadgets such as mobile phones, personal computers, laptops, etc. to do their activities. On the one hand, it has made Indonesia a huge market for all types of Cyber system-related products. On the other hand, however, Indonesia's cyber system has also grown more vulnerable to attack or abuse by criminals, terrorists, and other parties hostile to the country. Therefore, to achieve the

national objective as mandated in the Preamble of the 1945 Constitution of the Republic of Indonesia, various multi-sectoral efforts to protect all Indonesian people and the entire land of Indonesia, promote the welfare of the people, enrich the life of the nation, and participate in the creation of world order need to be protected from all types of Cyber Threat arising from the abuse of Cyber facilities and infrastructures or resources.

Indonesia's long history has taught us that threats against the safety, sovereignty, and security of the Indonesian people and nation are real. Some threats are tangible, while some are intangible. Therefore, the current foundation of Cyber Security and Resilience needs to be strengthened, synergized, and optimized to further improve Indonesia's resilience to multidimensional threats, both from inside and outside the country.

In the context of maintaining Cyber Security and Resilience, strengthening the foundation means four things. Firstly, all vulnerabilities that can magnify threat or harm in the Cyber sector must be detected and identified. Secondly, all assets crucial to the lives of many people must be protected or guarded against possible sabotage, attacks, or other attempts to have them destroyed or damaged. Thirdly, all ongoing sabotage, attacks, or other attempts must be immediately redressed, and any damage, losses, or destruction resulting therefrom must be immediately recovered. Fourthly, all components in the implementation of Cyber Security and Resilience, i.e. human resources, technical equipment, and non-technical equipment, must be monitored and controlled to reduce or minimize vulnerabilities.

Based on the foregoing, it is necessary to have a common understanding that Indonesia should not have a narrow view on threats in the cyber sector from the technical aspect only and limited to the scope of attacks aimed at critical information infrastructures only. Indonesia therefore needs to adopt a broader

perspective when looking at threats in the Cyber sector, which include those in the context of individual security, communal security, national security, and international security. Indonesia needs the broader insight for today's world civilization has shifted to the fourth industrial revolution, i.e. artificial intelligence revolution characterized by more massive utilization of hi-tech digital technologies. Therefore, the objects of Indonesia's Cyber Security and Resilience are not limited only to Central Government or Regional Government-owned Cyber systems, but also include all critical information infrastructures and Cyber systems vital to the implementation of electronic transactions and/or digital economy, which are largely owned by the private sector.

Due to the extensive range of stakeholders involved in Cyber Security and Resilience, all efforts to maintain Cyber Security and Resilience have to be based on effective collaboration between all national cyber components. All of the national cyber components, both in government sector and private sector, have to work in synergy and need to be given proportional roles to create a united, integrated, and vigilant national security component. It is also necessary to practice Cyber diplomacy to advance Indonesia's interest in the Cyber Security and Resilience sector at the international level.

Taking into account data on total number of Cyber infrastructure providers, massively-used internet applications owned by domestic companies, significant number of issued credit cards and debit cards, total number of domestic companies expanding to other countries and managing electronic systems from other countries, and total number of attempted or actual Cyber Attacks against or aimed at assets in Indonesia, it can be concluded that currently Indonesia's Cyber risk profile is somewhere between significant to massive. This Cyber risk profile ideally requires Indonesia to have a Cyber Security and Resilience ecosystem that is at least at an intermediate maturity level.

An intermediate maturity-level Cyber Security and Resilience ecosystem has a number of characteristics. First, a detailed and formal rule or procedure-based implementation of Cyber Security and Resilience. Second, a government agency to objectively and consistently supervise the compliance with such formal rule or procedure. Third, national Cyber components with analysis mechanism and inherent risk management in their institutional strategic policies and operational business processes.

Considering that Indonesia's Cyber Security and Resilience risk profile will not be lower in the future, it is a *conditio sine qua non* that the country's Cyber Security and Resilience ecosystem maturity level needs to be increased to even higher than the intermediate level. Suppose that Indonesia is able to create a conducive Cyber Security and Resilience climate, its digital economy market will grow even more exponentially. Such a climate will also boost businesses in cyber utilization-related goods and/or services, or particularly Cyber Security and Resilience-related products. This condition will hopefully open up more job or entrepreneurship opportunities, as well as promote research, development, and innovation that will solidify Indonesia's economy.

Based on such understanding, it is necessary to stipulate a law to regulate the implementation of Cyber Security and Resilience. This is important to accelerate Indonesia's Cyber Security and Resilience ecosystem maturity level and keep the exercise of government power in the Cyber Security and Resilience sector in line with the advancement of Indonesia's Cyber Interest, respect for human rights, independence in science and technology innovation, and advancement of the national economy. In general, this Law contains subject matters arranged in a systematic order as follows: implementation of Cyber Security and Resilience, Cyber Security and Resilience governance, Cyber Security and Resilience services, Cyber diplomacy, law enforcement, BSSN's institutional capacity, funding and procurement, prohibition, and criminal provisions.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

Letter a

"Sovereignty" means that cyber security and resilience must be implemented by prioritizing state integrity, national interest, and advancement of Indonesia's interest in the Cyber Security and Resilience sector at the international level.

Letter b

"Trustworthiness" means that Cyber Security and Resilience is implemented based on the principle of mutual trust between the parties involved in the utilization and management of Cyber Security and Resilience.

Letter c

"Professionalism" means that Cyber Security and Resilience is implemented by developing reliable Cyber ecosystem carrying capacity, good governance, and capable human resources capacity.

Letter d

"Readiness" means that Cyber Security and Resilience is implemented based on the capability and readiness to face any possible Cyber Threat, Cyber Incident, and/or Cyber Attack, or Cyber crisis.

Letter e

"Competitiveness" means that Cyber Security and Resilience is implemented with the objectives of developing and advancing digital economy in the aspects of Cyber industry governance, facility and infrastructure security, and competitive national cyber resources.

Letter f

"Legal certainty" means that Cyber Security and Resilience is implemented within the framework of a nation based on the rule of law (*negara hukum*) that prioritizes the basis of laws and regulations, appropriateness, and fairness in every Cyber Security and Resilience provider's policy.

Letter g

"Collaboration" means that Cyber Security and Resilience is implemented by all national Cyber components, whether in state agencies, Central Government, Regional Governments, or communities and private sector in a synergic manner to maintain Indonesia's Cyber Security and Resilience.

Article 3

Self-explanatory.

Article 4

Self-explanatory.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

Paragraph (1)

State agency means the state agency established under the 1945 Constitution of the Republic of Indonesia.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 8

Self-explanatory.

Article 9

Self-explanatory.

Article 10

Self-explanatory.

Article 11

Self-explanatory.

Article 12

Self-explanatory.

Article 13

Self-explanatory.

Article 14

Self-explanatory.

Article 15

Self-explanatory.

Article 16

Self-explanatory.

Article 17

Self-explanatory.

Article 18

Self-explanatory.

Article 19

Self-explanatory.

Article 20

Self-explanatory.

Article 21

Self-explanatory.

Article 22

Self-explanatory.

Article 23

Self-explanatory.

Article 24

Self-explanatory.

Article 25

Self-explanatory.

Article 26

Self-explanatory.

Article 27

Self-explanatory.

Article 28

Self-explanatory.

Article 29

Self-explanatory.

Article 30

Self-explanatory.

Article 31

Self-explanatory.

Article 32

Self-explanatory.

Article 33

Self-explanatory.

Article 34

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Self-explanatory.

Article 37

Self-explanatory.

Article 38

Self-explanatory.

Article 39

Self-explanatory.

Article 40

Self-explanatory.

Article 41

Self-explanatory.

Article 42

Self-explanatory.

Article 43

Self-explanatory.

Article 44

Self-explanatory.

Article 45

Self-explanatory.

Article 46

Self-explanatory.

Article 47

Self-explanatory.

Article 48

Self-explanatory.

Article 49

Self-explanatory.

Article 50

Self-explanatory.

Article 51

Self-explanatory.

Article 52

Self-explanatory.

Article 53

Self-explanatory.

Article 54

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Centers and/or other work units include but not limited to research and development centers, education and training centers, computer information data centers, technical implementation units, and/or offices.

Article 55

Self-explanatory.

Article 56

Self-explanatory.

Article 57

Self-explanatory.

Article 58

Self-explanatory.

Article 59

Self-explanatory.

Article 60

Self-explanatory.

Article 61

Self-explanatory.

Article 62

Self-explanatory.

Article 63

Self-explanatory.

Article 64

Self-explanatory.

Article 65

Self-explanatory.

Article 66

Self-explanatory.

Article 67

Self-explanatory.

Article 68

Self-explanatory.

Article 69

Self-explanatory.

Article 70

Self-explanatory.

Article 71

Self-explanatory.

Article 72

Self-explanatory.

Article 73

Self-explanatory.

Article 74

Self-explanatory.

Article 75

Self-explanatory.

Article 76

Self-explanatory.

Article 77

Self-explanatory.

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER... OF...