LAW OF THE REPUBLIC OF INDONESIA

NUMBER ... OF ...

ON

CYBERSECURITY AND DEFENSE[1]

BY THE GRACE OF GOD ALMIGHTY

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that in bid to realize the creation purpose of the Government of Indonesia which protects the entire Indonesian nation and the entire Indonesian homeland, advances public welfare, develops nation's intellectual level, and participates in implementing world order as mandated under the preamble of the 1945 Constitution of the Republic of Indonesia, the Unitary State of the Republic of Indonesia organizes cybersecurity and defense;

b. that in organizing cybersecurity and defense, the organization is confronted with cyberthreat risks which interfere national interests, as well as the existence of the needs to strengthen the governance of cyber resources in synergic, collaborative, competitive, and professional manners;

c. that the organization of cybersecurity and defense needs to be formulated under a law to be in accordance with the development and needs of the public law;

d. that based on considerations as referred to in letter a, letter b, and letter c, it needs formulation of Law on Cybersecurity and Defense;

[*] This edition of Law on Cybersecurity and Defense was published in May 2019. This translation is created with the best effort as can be offered and by any means, does not constitute and should not be treated as official translation or sworn translation for legal proceeding purposes. The copyright owner: 1) Should not be held liable for any error which occurs in the source document; 2) Reserves the right to change and modify this translation, with subsequent notifications given to every clients in timely manner; and 3) May seek redress for any unlawful or unauthorized transfer or disclosure of this translation against any party.

In view of:

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

With the Mutual Agreement of

HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA

and

PRESIDENT OF THE REPUBLIC OF INDONESIA

HAVE DECIDED:

To enact:

LAW ON CYBERSECURITY AND DEFENSE.

CHAPTER I

GENERAL PROVISIONS

Article 1

Under this Law, the following definitions are employed:

1. Cyber is a global space and accommodates various types of interests which are formed from interactions between human with information technology, computerization, computer networks, cryptography, and/or artificial intelligence.
2. Cybersecurity and Defense are dynamic conditions of Cyber which encompass every aspects of national life which are integrated, secured, and robust, as well as capable of developing Indonesian Cyber strength in encountering any Cyberthreats against Indonesian Cyber interests and resources as controlled by the Unitary State of the Republic of Indonesia.
3. Indonesian Cyber Interests are the safety of nation, security, sovereignty, integrity of territories of the Unitary State of the Republic of Indonesia, and national interests in

various aspects, including ideology, politic, economy, social culture, as well as defense and security, in Cyberspace.

4. Cyberthreats are any efforts, measures, and/or conducts, either domestically or overseas, which are assessed and/or proven may weaken, harm, and/or destroy Indonesian Cyber Interests.
5. Cyberincidents are Cyberthreats which cause Cyber electronic systems to be fail to function properly.
6. Cyberattacks are Cyberthreats which cause the secured Cyber objects to be malfunction, either partially or entirely, and/or temporary or permanent.
7. Secured Cyber Objects are data, information, infrastructures and facilities, as well as human resources, which receive protection from organizers of Cybersecurity and Defense.
8. Security Perimeter is area within the Cyber and non-Cyber scopes which are only accessible by persons who have Cybersecurity and Defense access permit.
9. Detection is effort to find out the whereabout, size, and distance of Cyberthreats from Security Perimeter.
10. Identification is effort to recognize and analyze threat level, cause, and impact of a detected Cyberthreat.
11. Protection is effort to protect Secured Cyber Objects from Cyberthreats, so that the functions of Secured Cyber Objects are not corrupted or missing, either partially or entirely.
12. Countermeasure is effort to overcome, dismiss, minimize impact, and/or prevent the worse state of impact of a Cyberincident or Cyberattack that has occurred.
13. Restoration is effort to repair the adverse effect or restore losses caused by Cyberincident or Cyberattack and return the functionality of Secured Cyber Objects.
14. Monitoring is effort to understand the dynamics and trends relating to Cyberincidents or Cyberattacks in the event of formulating effective and efficient strategies and tactics within the Cybersecurity and Defense scope.
15. Control is effort to maintain and strengthen Cybersecurity and Defense ecosystem.

16. Accreditation is acknowledgement relating to the fulfillment of special standards within the scope of the organization of education, training, and testing of human resources' competences within Cybersecurity and Defense scope.
17. Digital Certificates are certificates which are issued using cryptographic algorithm basis to become the digital marker or identity of person, computer, electronic system, data, electronic document, and/or Cyber network.
18. National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*), hereinafter referred to as BSSN, is an agency which carries out governmental affairs within the Cybersecurity and Defense scope based on this Law.
19. Central Government is the President of the Republic of Indonesia who holds the governmental power of the state of the Republic of Indonesia, who is assisted with Vice President and ministers as referred to under the 1945 Constitution of the Republic of Indonesia.
20. Regional Government is regional head as the element of the organizer of Regional Government who leads the implementation of governmental affairs which become the authority of autonomous regions.
21. Person is individual or legal entity.

CHAPTER II
PRINCIPLES AND PURPOSES

Article 2

Cybersecurity and Defense are based on the principles of:

a. sovereignty;
b. trustworthiness;
c. professionality;
d. preparedness;
e. competitiveness;
f. legal certainty; and
g. collaborative.

Article 3

Cybersecurity and Defense have the purposes to:

a. protect the integrity and sovereignty of the state from Cyberthreats;
b. increase Cyber competitiveness and innovation through the utilization of Cyber which is unrestricted, open, and accountable;
c. support the development and advancement of digital economy on the aspects of Cyber-industry governance, security of infrastructures and facilities, and national Cyber resources; and
d. consolidate, in synergic and collaborative manners, all elements which are involved in the organization of Cybersecurity and Defense to achieve national purpose and assume freedom and active role in anticipating Cyberthreats for world peace.

CHAPTER III
ORGANIZATION OF CYBERSECURITY AND DEFENSE

Division One
General

Article 4

(1) State is responsible for the organization of Cybersecurity and Defense.
(2) Organization of Cybersecurity and Defense as referred to in paragraph (1) is carried out by state institutions, Central Government, Regional Government, and/or the public.
(3) Central Government assigns BSSN to coordinate and collaborate the organization of Cybersecurity and Defense to be in accordance with Indonesian Cyber Interests.

Article 5

Organization of Cybersecurity and Defense must prioritize:

a. advancement of Indonesian Cyber Interests;
b. respect to human rights;
c. independence in science and technology innovations; and

d. advancement of national economy.

Division Two
Organizers of Cybersecurity and Defense

Article 6

Organizers of Cybersecurity and Defense consist of:

a. state institutions;
b. Central Government; and
c. Regional Government.

Article 7

(1) Organizers of Cybersecurity and Defense at state institutions as referred to under Article 6 paragraph a are under the responsibility of executives of state institutions which is implemented by the secretariat of state institutions.

(2) Organizers of Cybersecurity and Defense at Central Government as referred to under Article 6 letter b consist of:
   a. BSSN;
   b. Cyber at Indonesian National Army;
   c. Cyber at Indonesian National Police;
   d. Cyber at Indonesian Prosecutors' Office;
   e. Cyber at State Intelligence Agency; and
   f. Cyber at ministries/non-ministerial institutions other than as referred to in letter a, letter b, letter c, letter d, and letter e.

(3) Organizers of Cybersecurity and Defense at Regional Government as referred to under Article 6 letter c consist of:
   a. Cyber at provincial Regional Government; and
   b. Cyber at regency/city Regional Government.

(4) Organization of Cybersecurity and Defense as referred to in paragraph (2) letter a up to letter e is implemented in accordance with each scope of duty and function based on provisions under laws and regulations.

(5) Organization of Cybersecurity and Defense as referred to in paragraph (1), paragraph (2) letter f, and paragraph (3) is limitedly implemented for Cybersecurity and Defense within the internal scope of its organization.

Article 8

(1) Organization of Cybersecurity and Defense other than as referred to under Article 6 may be performed by the public.

(2) Organization of Cybersecurity and Defense by the public as referred to in paragraph (1) is limited to the following activities:
   a. protection of electronic system within the internal scope of organization; and/or
   b. procurement of services within the Cybersecurity and Defense.

Division Three

Coordination and Collaboration of Organizers of Cybersecurity and Defense

Article 9

(1) Coordination and collaboration as referred to under Article 4 paragraph (3) is performed through:
   a. routine meetings;
   b. increase in institutional and human resources' capacity;
   c. implementation of countermeasure and restoration;
   d. implementation of joint-tactical activities; [*sic*]
   e. provision of technical and non-technical supports for capacity increase of infrastructures and facilities, improvement of human resources' competence; and/or
   f. increase in the reach of cooperation networks.

(2) Implementation of coordination and collaboration as referred to in paragraph (1) are consolidated by BSSN.

(3) Further provisions on coordination and collaboration as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the Government.

CHAPTER IV
GOVERNANCE OF CYBERSECURITY AND DEFENSE

Division One
General

Article 10

(1) Organization of Cybersecurity and Defense is performed against Secured Cyber Objects at national Cyber infrastructures.
(2) National Cyber infrastructures as referred to in paragraph (1) consist of:
    a. national critical information infrastructures, including public-key infrastructures;
    b. electronic-based governmental organization infrastructures;
    c. national digital-economy infrastructures; and
    d. other electronic-system infrastructures in accordance with provisions under laws and regulations.
(3) National Cyber infrastructures as referred to in paragraph (2) are formulated within a list.
(4) List as referred to in paragraph (3) is stipulated based on Regulation of the BSSN.

Article 11

(1) Organization of Cybersecurity and Defense is performed to mitigate risks and respond the occurrence of Cyberthreats.
(2) Cyberthreats as referred to in paragraph (1) consist of:
    a. Cyberincidents occurring within the Security Perimeter;
    b. Cyberattacks against Secured Cyber Objects;
    c. malicious software;
    d. contents containing destructive and/or negative contents;
    e. products, product prototypes, product designs, or inventions which may be used as Cyberweapon;
    f. efforts made deliberately to weaken, harm, and/or destroy Indonesian Cyber Interests; and/or

g. other forms of Cyberthreats.

Division Two
Mitigation of Cyberthreat Risks

Article 12

(1) Every organizer of Cybersecurity and Defense must implement mitigation of Cyberthreat risks to protect Secured Cyber Objects under its responsibility.

(2) Mitigation of risks as referred to in paragraph (1) is implemented by:

a. creating copies of every software needed to operate electronic system;

b. creating copies continuously toward data within the electronic system to be used as backup;

c. saving copies as referred to in paragraph a and paragraph b within different electronic system with the source of copies;

d. operating Cybersecurity and Defense operation center;

e. managing access within Security Perimeter under its responsibility;

f. periodically changing access code to electronic system;

g. creating standard operational procedures on mitigation of Cyberthreat risks, as well as periodically simulating such procedures to human resources within the internal scope of organization; and

h. performing various other risk-mitigation efforts in accordance with provisions as referred to under this Law.

Article 13

(1) Mitigation of Cyberthreat risks as referred to under Article 12 is implemented in accordance with special standards as determined by BSSN.

(2) BSSN implements governance and assessment toward the conformity of implementation of mitigation of Cyberthreat risks as referred to in paragraph (1).

Division Three
Cyberthreat Responses

Article 14

(1) Every organizer of Cybersecurity and Defense must implement Cyberthreat responses to protect Secured Cyber Objects under its responsibility.

(2) Responses as referred to in paragraph (1) are implemented by:

a. checking the integrity, availability, and functionality of Secured Cyber Objects under its responsibility when Cyberincident or Cyberattack is discovered;

b. recording and notifying every Cyberincident or Cyberattack occurring at Secured Cyber Objects under its responsibility to BSSN;

c. performing analysis on threat level of Cyberincident or Cyberattack occurring at Secured Cyber Objects under its responsibility;

d. performing deletion of malicious software from its electronic system;

e. stopping the use of electronic system which has been infected by Cyberthreat for a certain period of time;

f. performing termination of data connection from electronic system to another electronic system which is alleged to be the source of Cyberthreat;

g. implementing efforts as recommended by BSSN toward [*sic*] Cyberincident or Cyberattack which has occurred at Secured Cyber Objects under its responsibility, so that it does not spread or becomes dangerous;

h. performing notification to users of electronic system or customers on Cyberthreat responses which have been performed to protect Secured Cyber Objects under its responsibility; and/or

i. performing other means within Cyberthreat responses in accordance with this Law.

Article 15

(1) Threat levels of Cyberthreats as referred to under Article 14 paragraph (2) letter c consist of:

a. not dangerous;

b. low;
c. intermediate; and
d. high.

(2) Provisions on criteria of each threat level as referred to in paragraph (1) are addressed under Regulation of the Government.

Article 16

(1) Implementation of Cyberthreat responses as referred to under Article 14 and Article 15 must refer to special standards as determined by BSSN.

(2) BSSN implements governance and assessment toward the conformity of implementation of Cyberthreat responses as referred to in paragraph (1).

Division Four

Cyberwares

Article 17

(1) Cyberwares which are used for the organization of Cybersecurity and Defense at national Cyber infrastructures must possess product certificates.

(2) Product certificates as referred to in paragraph (1) are issued by BSSN.

(3) Provisions on product certificates as referred to in paragraph (1) are addressed under Regulation of the BSSN.

Division Five

Service Providers within Cybersecurity and Defense Sector

Article 18

(1) Service providers within Cybersecurity and Defense sector as referred to under Article 8 paragraph (2) letter b must possess license.

(2) License as referred to in paragraph (1) is granted for the following business activities:
a. management of Cybersecurity and Defense system;
b. penetration testing against security of electronic-system access; and

c. creation of cryptography algorithms.

(3) License as referred to in paragraph (1) is issued by BSSN.

(4) Provisions on licensing as referred to in paragraph (1) are addressed under Regulation of the BSSN.

Division Six
Competence of Human Resources

Article 19

(1) Organizers of Cybersecurity and Defense must employ human resources having competence within Cybersecurity and Defense sector.

(2) Competence as referred to in paragraph (1) refers to special standards as determined by BSSN.

Article 20

(1) Organizers of Cybersecurity and Defense may organize business activities within education and training sector to fulfill special standards as referred to under Article 19 paragraph (2).

(2) Business activities as referred to in paragraph (1) must possess accreditation as granted by BSSN.

Article 21

(1) To increase capacity and professionality of human resources, Organizers of Cybersecurity and Defense originating from the public may assemble and form profession's organizations within Cybersecurity and Defense sector.

(2) Profession's organizations as referred to in paragraph (1) may perform issuance of professional competence certificates to human resources who have fulfilled special standards as referred to under Article 19 paragraph (2).

(3) Issuance of professional competence certificates as referred to in paragraph (2) may only be performed by profession's organizations which have possessed accreditation as profession's certification institution.

(4) Accreditation as referred to in paragraph (3) is granted by BSSN based on recommendation from authorized profession's development institution in accordance with provisions under laws and regulations.

Division Seven
Enforcement of Governance

Article 22

(1) Organizers of Cybersecurity and Defense who fail to meet special standards as referred to under Article 13 paragraph (1), Article 16 paragraph (1), and Article 19 paragraph (2) are imposed with administrative sanctions.
(2) Administrative sanctions as referred to in paragraph (1) consist of:
    a. warnings;
    b. rejection of application for Cybersecurity and Defense access permit;
    c. temporary suspension of Cybersecurity and Defense access permit;
    d. permanent revocation of Cybersecurity and Defense access permit;
    e. temporary suspension of service providers' license;
    f. permanent revocation of service providers' license;
    g. temporary operational suspension or blocking of electronic system;
    h. permanent operational shutdown or blocking of electronic system; and/or
    i. imposition of administrative fines.

Article 23

(1) Organizers of Cybersecurity and Defense who do not use certified Cyberwares as referred to under Article 17 paragraph (1) are imposed with administrative sanctions.
(2) Administrative sanctions as referred to in paragraph (1) consist of:
    a. warnings;
    b. temporary operational suspension or blocking of electronic system;
    c. permanent operational shutdown or blocking of electronic system; and/or
    d. imposition of administrative fines.

Article 24

(1) Service providers within Cybersecurity and Defense sector who do not possess license when performing its business activities as referred to under Article 18 paragraph (3) are imposed with administrative sanctions.

(2) Administrative sanctions as referred to in paragraph (1) consist of:
   a. warnings;
   b. temporary operational suspension or blocking of electronic system;
   c. permanent operational shutdown or blocking of electronic system; and/or
   d. imposition of administrative fines.

Article 25

(1) Organizers of Cybersecurity and Defense who organize business activities within education and training sector as referred to under Article 20 paragraph (2), but do not possess accreditation, are imposed with administrative sanctions.

(2) Administrative sanctions as referred to in paragraph (1) consist of:
   a. warnings;
   b. temporary operational suspension or blocking of electronic system;
   c. permanent operational shutdown or blocking of electronic system; and/or
   d. imposition of administrative sanctions.

Article 26

(1) Profession's organizations which issue profession's competence certificates as referred to under Article 21 and do not possess accreditation, are imposed with administrative sanctions.

(2) Administrative sanctions as referred to in paragraph (1) consist of:
   a. warnings;
   b. temporary operational suspension or blocking of electronic system;
   c. permanent operational shutdown or blocking of electronic system; and/or
   d. imposition of administrative sanctions.

Article 27

(1) Organizers of Cybersecurity and Defense who are imposed with administrative sanctions as referred to under Article 22 up to Article 26 reserve the right to file defense [*upaya pembelaan*].

(2) Further provisions on administrative sanctions and defense as referred to in paragraph (1) are addressed under Regulation of the Government.

Division Eight

Losses Risks and Losses Insurance

Article 28

(1) Any Person who sustains losses due to the organization of Cybersecurity and Defense function and/or measure may file request for rehabilitation, compensation, and/or restitution.

(2) Rehabilitation, compensation, and/or restitution request as referred to in paragraph (1) are performed in accordance with provisions under laws and regulations.

Article 29

(1) Organizers of Cybersecurity and Defense may subscribe for Cyber insurance services to cover losses risks as a result from Cyberincident or Cyberattack.

(2) Cyber insurance services as referred to in paragraph (1) are organized by Indonesian insurance businesses.

Article 30

(1) Cyber insurance businesses as referred to under Article 29 paragraph (2) must possess human resources who are competent within Cybersecurity and Defense sector.

(2) Human resources who are referred to in paragraph (1) should at least cover:

a. Cyber underwriters (*penilai risiko*); and

b. Cyber loss adjusters [*penilai kerugian*].

(3) Competent human resources as referred to in paragraph (1) are proven by competence certificates as issued by BSSN.

(4) Further provisions on competence certificates as referred to in paragraph (2) are addressed under Regulation of the BSSN.

CHAPTER V
CYBERSECURITY AND DEFENSE SERVICES

Division One
Cybersecurity and Defense Operation Center

Article 31

(1) In the event of performing Cybersecurity and Defense activities, every organizer of Cybersecurity and Defense must establish Cybersecurity and Defense operation center.

(2) Cybersecurity and Defense operation center as referred to in paragraph (1) must be connected with national Cybersecurity and Defense operation center.

(3) Provisions as referred to in paragraph (2) are exempted for Cybersecurity and Defense operation center which is organized by micro-, small-, medium-enterprises, and cooperatives.

(4) National Cybersecurity and Defense operation center as referred to in paragraph (2) is organized by BSSN.

Article 32

Cybersecurity and Defense operation center as referred to under Article 31 paragraph (1) providers services consisting of:

a. operation of contact person or contact center for the reporting of allegations on Cyberincident or Cyberattack which will occur or had occurred;

b. processing of reports on allegation of Cyberincident or Cyberattack to be followed-up; and

c. provision of information on progress status of reports on allegation of occurrence of Cyberincident or Cyberattack to the reporter.

Article 33

Technical provisions on operational procedures for Cybersecurity and Defense operation center as referred to under Article 31 and Article 32 are addressed under Regulation of the BSSN.

Division Two

Habituation of Cybersecurity and Defense

Article 34

Every organizer of Cybersecurity and Defense should perform Cybersecurity and Defense habituation [*pembudayaan*] efforts, so that the quality of risk-management of Cyber utilization increases.

Article 35

Cybersecurity and Defense habituation efforts as referred to under Article 34 consist of:

a. management of information and documentation relating to Cybersecurity and Defense; [*sic*]
b. implementation of promotional activities, technical counseling, and/or scientific activities to increase public literacy and awareness of Cybersecurity and Defense; and
c. Granting of appreciation to any Person who has participated in realizing the purpose of the organization of Cybersecurity and Defense.

CHAPTER VI
CYBER DIPLOMACY

Article 36

(1) In the event of proposing Indonesian Cyber Interests on international level and participating in maintaining world peace, Cyber diplomacy should be performed through a set of efforts by using diplomatic methods and means within Cybersecurity and Defense sector.

(2) Cyber diplomacy efforts as referred to in paragraph (1) consist of:

a. participate in creating, formulating, proposing proposal or initiative on concept, norm, behavior, and international guideline within Cybersecurity and Defense, either bilaterally, regionally, or multilaterally;

b. participate in Cybersecurity and Defense problem-solving activities on bilateral, regional, or multilateral fora;

c. participate in the administration of international regime within Cybersecurity and Defense sector on regional or multilateral level;

d. enter into partnership, cooperation, and reciprocal relationship with various states and/or international organizations to increase national Cyber defense, to prevent Cyber misuses, and/or increase awareness on various types of world Cyber concepts and management systems;

e. urge regional states to increase Cybersecurity and Defense capacity and enforce joint-system to mutually share situational information on Cybersecurity and Defense vulnerability, threat, and event;

f. organize activities, meetings, or workshops to disseminate Indonesian Cybersecurity and Defense concepts and/or policies to other states; and

g. other efforts in accordance with provisions under laws and regulations and/or international laws.

Article 37

(1) Cyber diplomacy as referred to under Article 36 is performed by BSSN.

(2) BSSN collaborates and coordinates with ministry which is in charge of foreign affairs to perform Cyber diplomacy as referred to in paragraph (1).

(3) Ministry which is in charge of foreign affairs, in the event of making effective the performance of Cyber diplomacy as referred to in paragraph (1) and paragraph (2):

a. proposes to the President on the appointment of special ambassador who handles diplomatic relationship within Cybersecurity and Defense sector; and

b. determines attaché position on Cybersecurity and Defense at certain diplomatic representatives.

CHAPTER VII
LAW ENFORCEMENT

Division One
Screening of Contents and Digital Applications

Article 38

(1) BSSN performs screening of contents and digital applications which contain malicious software contents, to support protection efforts toward the public as users of digital applications.

(2) Provisions on operational procedures for screening of contents and digital applications as referred to in paragraph (1) are addressed under Regulation of the BSSN.

Division Two
Enforcement

Article 39

(1) BSSN performs enforcements against any Person who is proven to commit violations of Cybersecurity and Defense.

(2) Enforcements as referred to in paragraph (1) consist of:

a. handing down of administrative sanctions;

b. delegation of investigation result to authorized officials within criminal investigation sector;
c. filing of indemnity lawsuit; and/or
d. other measures in accordance with provisions under laws and regulations.

(3) Technical provisions on operational procedures for enforcement as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the BSSN.

Division Three

Supports During Law Enforcement Process

Article 40

(1) In the event of law enforcement process, BSSN provides supports during examination process of civil and criminal cases.
(2) Supports during examination process of civil cases as referred to in paragraph (1) are performed during inquisitorial [*pembuktian*] phase at courts.
(3) Supports during examination process of criminal cases as referred to in paragraph (1) are performed during preliminary investigation [*penyelidikan*], investigation [*penyidikan*], and/or inquisitorial phases at courts.
(4) Implementation of provision of supports as referred to in paragraph (1) is performed by BSSN in accordance with provisions under laws and regulations.

CHAPTER VIII

BSSN

Division One

Position

Article 41

BSSN assumes the position under and is held responsible to the President.

Division Two
Duties and Functions

Article 42

(1) BSSN assumes the following duties:
   a. organizes governmental affairs within Cybersecurity and Defense scope in effective and efficient manners;
   b. utilizes, develops, and consolidates all elements of stakeholders relating to Cybersecurity and Defense; and
   c. performs supervision on the usage of crypto products and organization of state crypto.

(2) Implementation of duty as referred to in paragraph (1) letter c is addressed under a separate law.

Article 43

BSSN organizes these functions:

a. Cybersecurity and Defense governance;
b. Cybersecurity and Defense services;
c. Cyber diplomacy;
d. law enforcement supports; and
e. development in the organization of Digital Certificates.

Division Three
Authorities

Article 44

BSSN assumes these authorities:

a. establishes and enacts regulations, special standards, and/or operational procedures within Cybersecurity and Defense on national scope;
b. formulates strategic framework and technical framework of Cybersecurity and Defense;

c. performs efforts on the realization of Indonesian Cybersecurity and Defense, domestically and overseas;
d. determines Security Perimeter;
e. grants, suspends, or revokes license, certification, or accreditation within Cybersecurity and Defense scope;
f. performs investigation, enforcement and imposition of administrative sanctions;
g. performs assessment, testing, penetration of security of electronic-system access, and/or audit of Cybersecurity and Defense; and
h. provides supports during criminal and civil law enforcement process.

Article 45

(1) In the event of supporting criminal law enforcement process as referred to under Article 44 letter h, BSSN performs:
   a. analysis of digital evidence;
   b. provision of expert testimonies within digital forensic sector; and/or
   c. provision of Cybersecurity and Defense technical supports during preliminary investigation and investigation phases.
(2) Supports of criminal law enforcement process as referred to in paragraph (1) are performed by BSSN if there is any written request from preliminary investigator, investigator, and/or public prosecutor to BSSN.
(3) Supports of civil law enforcement process as referred to under Article 44 letter h are performed by BSSN if there is any written request by the court.
(4) Implementation of criminal and civil enforcement supports as referred to in paragraph (2) and paragraph (3) are performed in accordance with provisions under laws and regulations.

Article 46

Asides from exercising authorities as referred to under Article 44, BSSN performs Detection, Identification, Protection, Countermeasure, Restoration, Monitoring, and Control of Secured Cyber Objects as referred to under Article 10 paragraph (2), both domestically and overseas.

Article 47

In the event of performing Detection as referred to under Article 46, BSSN performs these measures:

a. Cyberthreat Detection on data traffic;
b. Cyberthreat Detection relating to socio-cultural behaviors;
c. Detection on Cyberthreat potentials;
d. intelligent signals;
e. assessment, testing, and penetration of security of electronic-system access to discover the vulnerability and security loopholes relating to National Cyber Infrastructures;
f. Granting of license for the activities of researching and testing of Cybersecurity and Defense strength; and
g. other Detection measures in accordance with provisions under laws and regulations.

Article 48

In the event of performing Identification as referred to under Article [*sic*] 44, BSSN performs these measures:

a. Cyberthreat Identification on data traffic;
b. Cyberthreat Identification relating to socio-cultural behaviors;
c. Identification on Cyberthreat potentials;
d. Analysis on intelligent signals;
e. analysis on the results of assessment, testing, and penetration of security of electronic-system access relating to national Cyber Infrastructures;
f. Granting of license for the activities of researching and testing of Cybersecurity and Defense strength; and
g. other Identification measures in accordance with provisions under laws and regulations.

Article 49

In the event of performing Protection as referred to under Article 44, BSSN performs these measures:

a. governance on the utilization of cryptographic algorithms;
b. issuance of Digital Certificates at national Cyber infrastructures;
c. protection of Cyber inter-networks among organizers of Cybersecurity and Defense;
d. auditing of implementation of security standards;
e. planning of the needs of state crypto devices;
f. maintenance of state crypto devices;
g. management of crypto system key that is used for state crypto;
h. protection of security of frequency waves or signals;
i. counter-sensing [*kontra pengindraan*[;
j. management of grants; and
k. development of Cybersecurity and Defense communities.

Article 50

In the event of performing Countermeasure as referred to under Article 44, BSSN performs these measures:

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

Article 51

In the event of performing Restoration as referred to under Article 44, BSSN performs these measures:

a. dissemination of information to increase Cybersecurity and Defense awareness;
b. performance of investigation to urge restoration of losses or loss occurring at National Cyber Infrastructures; and
c. performance of follow-ups of investigation results through administrative efforts and/or other restitution [*pemulihan kerugian*] efforts in accordance with [*sic*] laws and regulations.

Article 52

In the event of performing Monitoring as referred to under Article 44, BSSN performs these measures:

a. governance of data and information relating to the occurrence of Cyberincident or Cyberattack which has occurred in the entire world;
b. governance of data and information relating to impact of Cyberincident or Cyberattack which has occurred in the entire world; and
c. study of data and information relating of Cyberincident or Cyberattack to formulate the best strategies and tactics in responding various development of Cyberthreats as designated to the Unitary State of the Republic of Indonesia.

Article 53

In the event of performing Control as referred to under Article 44, BSSN performs these measures:

a. licensing for service providers within Cybersecurity and Defense sector;
b. certification of Cyberwares as provided to be used at national Cyber infrastructures;
c. certification of Cyber underwriters (*penilai risiko*) and Cyber loss adjusters;
d. accreditation of education and training institution within Cybersecurity and Defense sector; and
e. accreditation of profession's certification institution within Cybersecurity and Defense sector.

Division Four

Organization

Article 54

BSSN consists of:

a. Head;
b. Vice Head;
c. General Secretariat;
d. deputy;

e. general inspectorate; and
f. other centers and/or working units according to prevailing rules and stipulations.

Article 55

(1) BSSN is headed by a Head and assisted by a Vice Head.
(2) Appointment and termination of Head of BSSN and Vice Head of BSSN as referred to in paragraph (1) are determined based on Decree of the President.

Article 56

(1) Head of BSSN is granted with financial allowances and facilities equivalent to minister.
(2) Vice Head of BSSN is granted with financial allowances and facilities equivalent to vice minister.

Article 57

(1) In the event of effectiveness and efficiency in the implementation of coordination and collaboration with Regional Government, BSSN establishes representative offices.
(2) Organizational structures and work procedures of representative offices as referred to in paragraph (1) are determined by BSSN.

Article 58

(1) In the event of meeting the needs of human resources for the implementation of duties, functions, authorities, and measures of BSSN within Cybersecurity and Defense scope, BSSN organizes official education [*pendidikan kedinasan*].
(2) Organizational structures and work procedures of official education as referred to in paragraph (1) are determined by BSSN.

Article 59

(1) In the event of organization of Cybersecurity for the electronic-based organization of the government, BSSN organizes the issuance of Digital Certificates services.
(2) Issuance of Digital Certificates services as referred to in paragraph (1) encompasses:

a. management for issuance of Digital Certificates using cryptographic algorithm basis for the creation of digital signature and authentication of identity of Person;
b. management for issuance of Digital Certificates using cryptographic algorithm basis for the creation of digital signature and authentication of computer or electronic system;
c. management for issuance of Digital Certificates using cryptographic algorithm basis for the creation of digital signature and authentication of computer network or cyber network; and
d. management for issuance of Digital Certificates using cryptographic algorithm basis for the creation of digital signature and authentication of electronic data or document.

(3) Issuance of Digital Certificates services as referred to in paragraph (1) and paragraph (2) may be granted to parties outside of Electronic-Based Governmental System if there is a request.

(4) Organizational structures and work procedures for issuance of Digital Certificates services as referred to in paragraph (1) are determined by BSSN.

Article 60

Further provisions on the organization of BSSN as referred to under Article 54 up to Article 59 are addressed under Regulation of the President.

Article 61

(1) Organization of Cybersecurity and Defense during state of war is performed under direct control of the President.

(2) Organization of Cybersecurity and Defense as referred to in paragraph (1) during state of war should obtain approval from House of Representatives.

CHAPTER IX
FUNDING AND PROCUREMENT

Article 62

(1) Funding for the organization of Cybersecurity and Defense is sourced from:
   a. State Revenue and Expenditure Budget;
   b. regional revenue and expenditure budget;
   c. national Cybersecurity and Defense development fund;
   d. grants; and/or
   e. other legitimate and non-binding sources of funding according to provisions under laws and regulations.

(2) Grants as referred to in paragraph (1) letter d may take form as:
   a. money;
   b. goods;
   c. facilities;
   d. devices; and/or
   e. services.

Article 63

(1) Money grant as referred to under Article 62 paragraph (2) letter a is deposited into national Cybersecurity and Defense development fund and be managed by BSSN.

(2) Results of the management of national Cybersecurity and Defense development fund as referred to in paragraph (1) are expended for:
   a. human resources development;
   b. research;
   c. granting of appreciation; and/or
   d. reserve fund to anticipate contingency needs on the occurrence of Cyberincident and/or Cyberattack.

(3) Further provisions on management of national Cybersecurity and Defense development fund as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the Government.

Article 64

(1) Grants in the form of goods, facilities, devices, and/or services as referred to under Article 62 paragraph (2) letter b, letter c, letter d, and letter e are managed by BSSN.
(2) Management of grants in the form of goods, facilities, devices, and/or services as referred to in paragraph (1) is used to increase the ability of organization of national Cybersecurity and Defense.
(3) Further provisions on management of grants in the form of goods, facilities, devices, and/or services as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the BSSN.

Article 65

(1) Central Government and Regional Government must allocate fund for the organization of Cybersecurity and Defense in State Revenue and Expenditure Budget and Regional Revenue and Expenditure Budget.
(2) Fund for the organization of Cybersecurity and Defense as referred to in paragraph (1) is designated for:
    a. human resources development; and
    b. establishment and/or strengthening of Cybersecurity and Defense devices and infrastructures.
(3) Further provisions on allocation and designation of Fund for the organization of Cybersecurity and Defense as referred to in paragraph (1) and paragraph (2) are addressed under Regulation of the Government.

Article 66

(1) Establishment and/or strengthening of Cybersecurity and Defense devices and infrastructures as referred to under Article 65 paragraph (2) letter b must fulfill the 50% (fifty percent) local component level provision.
(2) The 50% (fifty percent) local component level provision as referred to in paragraph (1) is implemented each for procurement of hardware and/or software.

(3) Implementation of the fulfillment of 50% (fifty percent) local component level provision as referred to in paragraph (1) is implemented by ministry which organizes governmental affairs within industrial sector and in coordination with BSSN.

(4) Further provisions on the fulfillment of 50% (fifty percent) local component level is addressed under Regulation of the Government.

Article 67

(1) Procurement of hardware and software as referred to under Article 66 paragraph (1) in certain conditions may be performed through direct appointment or direct procurement.

(2) Direct appointment or direct procurement in certain conditions as referred to in paragraph (1) is performed in cases of:
   a. emergency handling for public security and safety;
   b. complex works and only be performed by service providers within Cybersecurity and Defense sector which are very limited or may only be performed by rights holders;
   c. works which must be kept confidential in relation to state security and safety; and/or
   d. small-scale works.

(3) Direct appointment or direct procurement as referred to in paragraph (1) is performed in accordance with provisions under laws and regulations.

CHAPTER X

PROHIBITIONS

Article 68

Any Person is prohibited from deliberately [*dengan sengaja*] and without authority [*tanpa hak*] or unlawfully [*melawan hukum*] commits any act which causes National Cyber infrastructures to be interrupted and/or not functioning properly.

Article 69

Any Person is prohibited from deliberately and without authority or unlawfully produces, distributes, or provides device which is designed or developed specifically to facilitate act as referred to under Article 68.

CHAPTER XI
CRIMINAL PROVISIONS

Article 70

Any Person who meets elements as referred to under Article 68, is sentenced with imprisonment for 10 (ten) years at maximum and/or fines in sum of IDR 10,000,000,000.00 (ten billion rupiahs) at maximum based on the level of damage caused.

Article 71

Any Person who meets elements as referred to under Article 69, is sentenced with imprisonment for 10 (ten) years at maximum and/or fines in sum of IDR 10,000,000,000.00 (ten billion rupiahs) at maximum based on the level of damage caused.

Article 72

(1) Criminal provisions as referred to under Article 70 and Article 71 do not prevail for any Person who performs research and/or testing toward the strength of Cybersecurity and Defense at national Cyber infrastructures.
(2) Any Person who performs research and/or testing as referred to in paragraph (1) should be registered and possess license from BSSN.
(3) Provisions on procedures for research, testing, registration, and granting of license as referred to in paragraph (2) are addressed under Regulation of the BSSN.

CHAPTER XII
TRANSITIONAL PROVISIONS

Article 73

When this Law comes into force, all laws and regulations which address matters on Cybersecurity and Defense are declared valid, insofar that they are not in contradictory with provisions under this Law.

Article 74

Organizations or bodies which are elements to the organization of Cybersecurity and Defense which have existed continue to prevail until they are changed or replaced with new organizations or bodies based on provisions under this Law.

Article 75

BSSN must adjust with provisions under this Law, no later than 2 (two) years since this Law comes into force.

CHAPTER XIII
CLOSING PROVISIONS

Article 76

(1) Implementing regulations of this Law should have been enacted no later than 1 (one) year since this Law is promulgated.
(2) Central Government should report the implementation of this Law to the House of Representatives no later than 3 (three) years since this Law comes into force.

Article 77

This Law comes into effect on the promulgation date.

For the purposes of public cognizance, it has been ordered that the promulgation of this Law should be achieved through its publication in the State Gazette of the Republic of Indonesia.

Enacted 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 H LAOLY

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

DRAFT ELUCIDATION OF
LAW OF THE REPUBLIC OF INDONESIA
NUMBER ... OF ...
ON
CYBERSECURITY AND DEFENSE

I. GENERAL

Cyber system has been an important need for the Indonesian nation and society. The indication of it is that the society is now dependent to internet access and use of gadgets such as cellphones, computer devices, laptops and etc. to carry out their activities. On one hand, such condition makes Indonesia as a very huge market for various products relating to Cyber system. On the other hand, however, Indonesian Cyber system also becomes vulnerable to be classified as target or being misused by criminals, terrorists, and other parties who become hostile against Indonesia. Therefore, in order to realize national purpose as mandated by the Preamble of the 1945 Constitution of the Republic of Indonesia, various of multi-sectoral efforts to protect the entire Indonesian nation and entire Indonesian homeland, advances public welfare, develops nation's intellectual level, and participates in implementing world order, security from various Cyberthreats due to misuses of Cyber infrastructures and facilities or resources is needed to be provided.

Experiences which have been undergone by Indonesian nation gave a lesson that threats against safety, sovereignty, and security of Indonesian nation and state are tangible. Such threats may appear vividly and may also be hidden. Thus, existing foundations of Cybersecurity and Defense should be strengthened, synergized, and optimized, so that the Indonesian defense level in encountering multi-dimensional threats, either from domestic or overseas, become better.

Within the context of maintenance of Cybersecurity and Defense, strengthening of foundations may be construed as four things. Firstly, that all vulnerability which may increase threats or dangers in Cyber sector should be detectable and identifiable.

Secondly, all assets which are important for the livelihood of many people, should be protected or fortified from possibilities of sabotage, attack, or various other efforts to destroy or damage them. Thirdly, all sabotages, attacks, or various other efforts which are currently undergoing should be overcome immediately and damage, loss, or destruction which have existed should be restored immediately. Fourthly, all components in the organization of Cybersecurity and Defense, namely human, technical devices, and non-technical devices, should be able to be monitored and controlled, so they do not increase the amount or amplify the vulnerability.

Based on such understanding, then it is necessary for communal understanding that Indonesia cannot look threats in cyber sector narrowly only from technical aspects and only limited to the scope of attack that is designated to critical information infrastructures. Nonetheless, Indonesia is required to look threats in Cyber sector with broad perspective, including threats within the contexts of individual security, communal security, national security, and international security. Indonesia requires such broad insight, because world's civilization now has shifted to the fourth industrial revolution, namely artificial intelligence revolution which has the characteristics of massive utilization of high-level technology which is based on digital technology. Hence, objects of Cybersecurity and Defense maintenance are not only aimed to Cyber systems owned by Central Government or Regional Government, but also cover a handful of critical information infrastructures and vital Cyber system for the organization of electronic transactions and/or digital economy, which are majority owned by private parties.

Due to the broad scope of stakeholders in the maintenance of Cybersecurity and Defense, then any efforts of Cybersecurity and Defense maintenance should be based on effective collaboration among all national cyber components. Entire national cyber components, both existing in governmental sector and existing in private sector, should be synergized and be given proportional roles, so that they become a unity of national security component which is integrated and constantly

alert and prepared. It is also needed Cyber diplomacy efforts to advance entire Indonesian interests within Cybersecurity and Defense sector on international level.

By considering data relating to number of companies providing Cyber infrastructures, internet applications which are owned by domestic companies which are used massively, high figure of credit card and debit card numbers which have been issued, number of domestic companies which have expanded overseas and managed electronic systems overseas, as well as number of attempts or actual Cyberattacks occurring or aiming toward assets in Indonesia, then it may be concluded that currently, the risk profile of Indonesian Cyber has reached significant level to very huge level. With such Cyber risk profile, then ideally, ecosystem for the organization of Indonesian Cybersecurity and Defense should at least reach intermediate maturity level (*kematangan menengah*).

Cybersecurity and Defense ecosystem with intermediate maturity level is characterized with several things. Firstly, there is an organization of detailed Cybersecurity and Defense and based on formal rules and procedures. Secondly, there is governing body which performs supervision in objective and consistent manners against implementation of such formal rules or procedures. Thirdly, entire national Cyber components have possessed analysis mechanism and implementation of inherent risk management within strategic policies and operational business process of its institution.

Considering that it is impossible that the risk profile of Indonesian Cybersecurity and Defense to drop, then it is a *conditio sine qua non* [indispensable condition] that maturity level of Indonesian Cybersecurity and Defense ecosystem should be escalated, even higher than intermediate maturity level. If Indonesia able to realize conducive Cybersecurity and Defense climate, then Indonesian digital-economy market will grow bigger. Such condition will make the business of goods and/or services relating to cyber utilization, or specifically relating to Cybersecurity and Defense products to be more popular. Based on such condition, it is expected that

there will be greater job opportunities or entrepreneurship, as well as research, development, and innovation activities which grow and strengthen Indonesian economy.

Based on such understanding, then the organization of Cybersecurity and Defense needs to be regulated under a law. Such matter is necessary to accelerate the escalation of maturity level of Indonesian Cybersecurity and Defense ecosystem and maintain so that the implementation of governmental power within Cybersecurity and Defense sector is in line with the advancement of Indonesian Cyber Interests, respect to human rights, independence in innovation of science and technology, as well as advancement of national economy. Generally, this Law contains primary contents which are formulated systematically, as follows: organization of Cybersecurity and Defense, governance of Cybersecurity and Defense, Cybersecurity and Defense services, Cyber diplomacy, law enforcement, organizational of BSSN, funding and procurement, prohibitions, and criminal provisions.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

Letter a

"Sovereignty" means that organization of cybersecurity and defense should prioritize state integrity, national interests and advancement of Indonesian interests within Cybersecurity and Defense sector on international level.

Letter b

"Trustworthiness" means that organization of Cybersecurity and Defense is implemented using the basis of mutual trust principle among the parties in the utilization and management of Cybersecurity and Defense.

Letter c

"Professionality" means that organization of Cybersecurity and Defense is implemented by creating reliable Cyber ecosystem support capacity, good governance, as well as the fulfillment of capable human resources capacity.

Letter d

"Preparedness" means that organization of Cybersecurity and Defense is implemented based on ability and preparation in encountering any possibilities on the occurrence of Cyberthreats, Cyberincidents and/or Cyberattacks, as well as Cybercrisis.

Letter e

"Competitiveness" means that organization of Cybersecurity and Defense is implemented with the purpose of developing and advancing digital economy on the governance aspects of Cyberindustry, security of infrastructures and facilities, and competitive national cyber resources.

Letter f

"Legal certainty" means that organization of Cybersecurity and Defense is implemented within the framework of state law which prioritizes the basis of laws and regulations, propriety, and justice in every policy of organizers of Cybersecurity and Defense.

Letter g

"Collaborative" means that organization of Cybersecurity and Defense is implemented by all national Cyber components, both existing at state institutions, Central Government, Regional Government, as well as civil society organizations and private parties, in synergic manner in maintaining Indonesian Cybersecurity and Defense.

Article 3

Self-explanatory.

Article 4

Self-explanatory.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

Paragraph (1)

State institutions refer to state institutions as established based on 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 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

Other centers and/or working units refer to, among others, but not limited to, such as research and development centers, education and training centers, computer information datacenters, technical implementing units, and/or halls [*balai*].

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 ...