REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA
NUMBER 82 OF 2022
ON
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

BY THE BLESSINGS OF ALMIGHTY GOD

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering : a. that the Government protects the public interest from all kinds of disturbances of Critical Information Infrastructure as a result of misuse of electronic information and electronic transactions that disrupt the public order;

b. that the disturbances of Critical Information Infrastructure may cause serious losses and impacts on the public interest, public services, defense and security, as well as the national economy.

c. that in order to provide direction, basis, and legal certainty in protecting Critical Information Infrastructure from all kinds of disturbances as a result of misuse of electronic information and electronic transactions, it is necessary to regulate the Critical Information Infrastructure protection.

d. that based on the considerations as referred to in point a, point b and point c, it is necessary to issue a Presidential Regulation on Critical Information Infrastructure Protection.

Observing : 1. Article 4 section (1) of the 1945 Constitution of the Republic of Indonesia;

2. Government Regulation Number 71 of 2019 on Operation of

Electronic System and Transaction (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to the State Gazette of the Republic of Indonesia Number 6400);

HAS DECIDED:

To issue: PRESIDENTIAL REGULATION ON CRITICAL INFORMATION INFRASTRUCTURE PROTECTION.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Presidential Regulation:

1. Critical Information Infrastructure, hereinafter abbreviated as CII, means an Electronic System that utilizes information technology and/or operational technology, both independently and interdependently with other Electronic Systems in supporting strategic sectors, which will have serious impacts on the public interest, public services, defense and security, or the national economy if there are the disturbances, damage, and/or destruction of the infrastructure.
2. Electronic System means a set of electronic devices and procedures which function to prepare, collect, process, analyze, store, display, announce, send and/or disseminate Electronic Information.
3. Electronic Information means one or a set of electronic data, including but not limited to text, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, access codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them.
4. Cyber Security means an adaptive and innovative effort in order to protect all layers of cyberspace, including the information assets contained therein, from both technical

and social cyber threats and attacks.

5. Cyber Incident means one or a series of events that disrupt or threaten the operation of the Electronic System.
6. Cyber Security Incident Response Team means a group of people who are responsible for handling Cyber Incidents in their defined scopes.
7. Ministries or Institutions mean State Administering Institutions in charge of supervising and issuing regulations on their sectors.
8. CII Operators mean State Administering Institutions, business entities, and/or organizations that own and/or operate a CII.
9. State Administering Institutions mean legislative, executive and judicial institutions at the central and regional levels and other Institutions established by legislation.
10. National Cyber and Crypto Agency (Badan Siber dan Sandi Negara), hereinafter referred to as the Agency, means a government agency that carries out government duties in the field of cyber security and cryptography.

Article 2

The arrangement of CII protection aims to:

a. protect the continuity of the operation of CII in a safe, reliable and trustworthy manner;
b. prevent disturbance, damage, and/or destruction to CII due to cyber-attacks, and/or other threats/vulnerabilities; and
c. improve preparedness in handling Cyber Incidents and speeding up recovery from the impact of Cyber Incidents.

Article 3

The scope of CII protection includes:

a. identification of CII sector and CII;
b. operation of CII protection;
c. development and supervision of the operation of CII protection; and
d. coordination of the operation of CII protection.

CHAPTER II
IDENTIFICATION OF CII SECTOR AND CII

Part One
Identification of CII Sector

Article 4

(1) CII sector includes:
   a. government administration;
   b. energy and mineral resources;
   c. transportation;
   d. finance;
   e. health;
   f. information and communication technology;
   g. food;
   h. defense; and
   i. other sectors determined by the President.

(2) Other sectors determined by the President as referred to in section (1) point i are strategic sectors which will have serious impacts on the public interest, public services, defense and security, or the national economy if there are the disturbances, damage, and/or destruction of the infrastructure..

(3) The Ministries or Institutions from CII sector as referred to in section (1) point a to point h are determined as follows:
   a. the Agency for the government administration sector;
   b. the ministry administering government affairs in the field of energy and mineral resources for the energy and mineral resources sector;
   c. the ministry administering government affairs in the field of transportation for the transportation sector;
   d. the financial sector regulatory and supervisory authority for the financial sector;
   e. the ministry administering government affairs in the field of health for the health sector;
   f. the ministry administering government affairs in the field of communication and informatics for the

information and communication technology sector;

g. the ministry administering government affairs in the field of agriculture for food sector; and

h. the ministry administering government affairs in the field of defense for the defense sector.

Article 5

(1) The President determines the other sectors as referred to in Article 4 section (2) and Ministries or Institutions in charge of the sectors upon the proposals of the Head of the Agency.

(2) The proposals for other sectors as referred to in section (1) are submitted to the President based on the results of the coordination meeting for the operation of CII protection.

(3) Other sectors and ministries or Agencies as referred to in section (1) are determined by a Presidential Decree.

Part Two

Identification of CII

Article 6

(1) Every Electronic System Operator within the CII sector as referred to in Article 4 section (1) is obligated to periodically identify the CII at least 1 (one) time in 1 (one) year.

(2) Every Electronic System Operator within CII sector is obligated to report the results of ithe identification of CII as referred to in section (1) along with the relevant information to the Ministries or Institutions.

(3) The Ministries or Institutions verify the result report of the identification of CII as referred to in section (2).

(4) The Ministries or Institutions determine:

a. the Electronic System as CII; and

b. the Electronic System Operator within the CII sector as a CII Operator,

based on the results of the verification of the CII identification report as referred to in section (3).

(5) Further provisions regarding the identification of CII, reporting of identification results, verification mechanism,

determination of CII, and determination of CII operator are regulated by an Agency Regulation.

CHAPTER III
OPERATION OF CII PROTECTION

Part One
CII Protection Framework and CII Protection Roadmap

Article 7

(1) The Agency prepares a CII protection framework as a guideline.

(2) The framework as referred to in section (1) contains at least:
   a. operation of CII protection;
   b. development and supervision of the implementation of CII protection in accordance with the provisions of legislation; and
   c. technology for CII protection.

(3) The Agency prepares the framework as referred to in section (1) by coordinating with the Ministries or Institutions.

(4) Further provisions regarding the framework as referred to in section (1) are regulated by an Agency Regulation.

Article 8

(1) The Ministries or Institutions prepare and determine a CII protection roadmap for a period of 5 (five) years by referring to the CII protection framework as referred to in Article 7 section (1).

(2) The CII protection roadmap as referred to in section (1) contains at least:
   a. the target for the operation of CII protection; and
   b. work plan of the operation of CII protection.

(3) The Ministries or Institutions review the CII protection roadmap as referred to in section (1) every year.

(4) In the event that it is necessary to change the CII protection roadmap based on the results of the review as referred to in

section (3), the Ministries or Institutions determine the changes to the CII protection roadmap.

(5) In performing the preparation as referred to in section (1) and the review as referred to in section (3), the Ministries or Institutions may coordinate with the Agency.

(6) The CII protection roadmap that has been prepared and determined as referred to in section (1) and changes to the CII protection roadmap as referred to in section (4) is submitted to the Agency.

Part Two
Implementation of Cyber Security Standards

Article 9

(1) The CII Operator must provide reliable and safe protection of CII and be responsible for the proper operation of CII.

(2) In providing CII protection as referred to in section (1), CII Operator is obligated to apply information security standards and/or other security standards set by the Ministries or Institutions and/or the Agency.

Part Three
Cyber Security Risk Management

Article 10

(1) Each CII Operator is obligated to implement Cyber Security risk management effectively.

(2) The implementation of effective Cyber Security risk management as referred to in section (1) must meet the following requirements:
   a. compliance with legislation;
   b. conformity with the applicable standards in each CII sector; and
   c. internal control system that applies to CII Operator.

(3) CII Operator is obligated to report the results of the implementation of Cyber Security risk management to the Ministries or Institutions.

(4) In the event that the Ministries or Institutions are the CII Operators, the Ministries or Institutions are obligated to report the implementation results of Cyber Security risk management to the Agency.

(5) Further provisions regarding the implementation and reporting of the results of the implementation of Cyber Security risk management are regulated by an Agency Regulation.

(6) Provisions regarding the implementation and reporting of the implementation results of Cyber Security risk management in CII sector are determined by the Ministries or Institutions with reference to the Agency Regulation as referred to in section (5).

Part Four
Cyber Incident Management

Article 11

(1) Cyber Incident Handling is carried out by a Cyber Security Incident Response Team.

(2) The Cyber Security Incident Response Team as referred to in section (1) consists of:
   a. national Cyber Security Incident Response Team;
   b. sectoral Cyber Security Incident Response Team; and
   c. organizational Cyber Security Incident Response Team.

Article 12

(1) The Agency establishes a national Cyber Security Incident Response Team as referred to in Article 11 section (2) point a.

(2) The Ministries or Institutions establish a sectoral Cyber Security Incident Response Team as referred to in Article 11 section (2) point b.

(3) The CII Operator establishes an organizational Cyber Security Incident Response Team as referred to in Article 11 section (2) point c.

Article 13

(1) The organizational Cyber Security Incident Response Team is obligated to report Cyber Incidents in the CII within its organization to the sectoral Cyber Security Incident Response Team with a carbon copy to the national Cyber Security Incident Response Team not later than 1 x 24 (one time twenty-four) hours after the Cyber Incidents in the CII are found.

(2) The reported Cyber Incidents as referred to in section (1) refer to the result of the implementation of risk management as referred to in Article 10 section (3).

(3) In the event that a sectoral Cyber Security Incident Response Team has not been established, the organizational Cyber Security Incident Response Team is obligated to report Cyber Incidents that occur in the CII within its organization to the Ministries or Institutionsaccording to the sector with a carbon copy to the national Cyber Security Incident Response Team not later than 1 x 24 (one time twenty-four) hours after the Cyber Incidents in the CII are found.

Article 14

(1) The organizational Cyber Security Incident Response Team is obligated to handle Cyber Incident in the CII within its organization.

(2) Cyber Incident Handling as referred to in section (1) is carried out at least through:

a. response and recovery of Cyber Incidents;

b. delivery of Cyber Incident information to the related parties; and

c. dissemination of information to prevent and/or reduce the impact of Cyber Incidents.

(3) If deemed necessary, sectoral Cyber Security Incident Response Team and/or national Cyber Security Incident Response Team provides assistance or coordinates assistance in the context of handling Cyber Incidents in CII based on the report as referred to in Article 13 section (1).

(4) If deemed necessary, national Cyber Security Incident Response Team provides assistance or coordinates assistance in handling Cyber Incidents in CII based on the report as referred to in Article 13 section (3).

Article 15

(1) CII Operator, Ministries or Institutions, and the Agency develop preparedness against Cyber Incidents.

(2) Implementation of Cyber Incident preparedness as referred to in section (1) is implemented through:
   a. preparation of a Cyber Incident response plan and business continuity plan; and
   b. implementation of Cyber Incident response simulation and business continuity simulation.

Article 16

(1) In the event that the Cyber Incident in CII continues to increase and has the potential to become a crisis, cyber crisis management is enforceable.

(2) Cyber crisis management as referred to in section (1) is carried out in accordance with the provisions of legislation.

Article 17

Further provisions regarding Cyber Security Incident Response Team, reporting, Cyber Incidents handling, and implementation of preparedness for Cyber Incidents as referred to in Article 12 to Article 15 are regulated in an Agency Regulation.

Part Five

Cyber Security Information Sharing and Analysis Forum

Article 18

(1) The Agency, Ministries or Institutions, and/or CII Operator may organize a Cyber Security information sharing and analysis forum in accordance with the provisions of legislation.

(2) The Cyber Security information sharing and analysis forum as referred to in section (1) may involve the other related parties.

CHAPTER IV
DEVELOPMENT AND SUPERVISION OF OPERATION OF CII PROTECTION

Part One
Human Resource
Capacity Building for CII Operator

Article 19

(1) Each CII Operator is responsible for the human resources capacity building for the CII Operator.

(2) The human resources capacity building for the CII Operator as referred to in section (1) is carried out at least through:
   a. the development of competency and/or certification;
   b. the transfer of technology and expertise; and
   c. the information security awareness raising.

(3) In performing the human resources capacity building as referred to in section (1), the CII Operator may collaborate with the Agency.

(4) The Agency prepares and determines guidelines on human resources capacity building in the field of Cyber Security.

(5) Ministries or Institutions determine provisions regarding human resources capacity building by referring to the guidelines determined by the Agency as referred to in section (4).

Article 20

(1) Every CII Operator is obligated to prioritize hiring Indonesian workers in operating CII.

(2) In the event that hiring Indonesian workers in carrying out CII as referred to in section (1) has not been fulfilled, the CII Operator may hire foreign workers in accordance with the provisions of legislation.

(3) Every worker of the CII Operator as referred to in section (1)

and section (2) is obligated to maintain the confidentiality of information in accordance with the provisions of legislation.

Part Two
Cooperation

Article 21

(1) Ministries or Institutions and CII Operators may cooperate domestically and internationally in the context of the operation of CII protection.

(2) Ministries or Institutions and State Administering Agencies other than regulatory authority and financial supervisors in carrying out international cooperation as referred to in section (1), consult and coordinate with ministries in charge of government affairs in the field of foreign affairs and the Agency.

(3) International cooperation as referred to in section (2) is carried out in accordance with the provisions of legislation governing international relations and treaties.

(4) Financial sector regulatory and supervisory authority in carrying out international cooperation as referred to in section (1) is carried out in accordance with the provisions of legislation.

(5) Ministries or Institutions and CII Operator who have an international cooperation as referred to in section (1), must inform the implementation of the cooperation to the Agency.

Part Three
Measurement of Cyber Security Maturity Level

Article 22

(1) The CII Operator must conduct measurements of Cyber Security Maturity Level independently at least 1 (one) time in 1 (one) year.

(2) The CII Operator report the result of the Cyber Security maturity level measurement as referred to in section (1) to the Ministries or Institutions.

(3) In the event that Ministries or Institutions serve as CII Operators, Ministries or Institutions report the result of the Cyber Security maturity level measurement as referred to in section (1) to the Agency.

(4) Ministries or Institutions in verifying the result of the Cyber Security maturity level measurement as referred to in section (2) may involve the Agency.

(5) Ministries or Institutions are obligated to inform the result of the Cyber Security maturity level measurement as referred to in section (4) to the Agency periodically at least 1 (one) time in 1 (one) year.

(6) The Agency verifies the result of the Cyber Security maturity level measurement as referred to in section (3).

(7) Further provisions regarding the Cyber Security maturity level measurement are regulated by an Agency Regulation.

(8) Ministries or Institutions may determine regulations regarding the Cyber Security maturity level measurement in their respective sectors as required by referring to the Agency Regulation as referred to in section (7).

CHAPTER V
COORDINATION IN OPERATION OF CII PROTECTION

Article 23

(1) The Agency serves as the coordinator for the operation of CII protection.

(2) The Agency as the coordinator for the operation of CII protection as referred to in the Article (1) has duties in:

a. evaluating the determination of CII sector;

b. evaluating the determination of CII;

c. proposing the determination and change of CII sector to the President;

d. determining the CII protection framework;

e. providing Cyber Security recommendations on CII to the Ministries or Institutions based on data and information obtained by the Agency; and

f. evaluating the implementation of CII protection policies.

Article 24

(1) The Agency as the coordinator for the operation of CII protection as referred to in Article 23, performs the coordination at least 1 (one) time in 1 (one) year or at any time if deemed necessary.

(2) In performing the coordination meeting as referred to in section (1), the Agency involves the related ministries/institutions and/or other parties as necessary.

Article 25

The Head of the Agency submits the report of the performance of duties as the coordinator for the operation of CII protection to the President 1 (one) time in 1 (one) year or at any time if deemed necessary.

CHAPTER VI

CLOSING PROVISIONS

Article 26

The implementing regulations of this Presidential Regulation must be issued not later than 18 (eighteen) months after this Presidential Regulation is promulgated.

Article 27

This Presidential Regulation comes into force on the date of its promulgation.

In order that every person may know hereof, it is ordered to promulgate this Presidential Regulation by its placement in the State Gazette of the Republic of Indonesia.

Issued in Jakarta
on 24 May 2022

PRESIDENT OF THE REPUBLIC OF INDONESIA,

signed

JOKO WIDODO

Promulgated in Jakarta
on 24 May 2022

MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA,

signed

YASONNA H. LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2020 NUMBER 129

Jakarta, 10 November 2022
Has been translated as an Official Translation
on behalf of Minister of Law and Human Rights
of the Republic of Indonesia
DIRECTOR GENERAL OF LEGISLATION AD INTERIM,

DHAHANA PUTRA