Critical Information Infrastructure Protection (CIIP) Guidelines

1. Introduction:

a. This document offers guidelines for cyber security and protection of CII.

b. The goal of CII security and protection is to ensure that CI operations continue uninterrupted.

c. Regardless of the CI sector's or the CI service's level of maturity, the document offers the baseline cyber security requirements for all designated CIIs. The document also lists organizational and technical safeguards that designated CII Owners (CIIO) should implement to preserve CII systems and communications.

d. Based on the CII's cyber security risk profile, the CIIO is expected to take further steps to reinforce the CII's cyber security beyond those outlined in this document.

2. Designated CII and CIIO

a. As per PECA 2016, critical infrastructure (CI) means critical elements of infrastructure namely assets, facilities, systems networks or processes the loss or compromise of which could result in ***major detrimental impact on the availability, integrity or delivery of essential services*** – including those services whose integrity, if compromised could result in significant loss of life or causalities – taking into account significant economic or social impacts or significant impact on national security, national defence or the functioning of the state.

b. CERT rules 2023 define CII as critical elements of infrastructure including but not limited to facilities, systems, networks or processes, information systems programs or data of ***critical sectors.***

c. NCSP 2021 define critical sectors as Government systems, utility infrastructure (electricity, gas, and water), education, health, transport system (air, road, rail, and

sea), emergency services, manufacturing facilities, banking and financial sector, telecommunication/ ICT sector, dams, etc.

d. Thus the infrastructure of the critical sector that fulfills the criteria given in 2(a) and has been designated as CII by the relevant Ministry or regulator is termed as ***designated CII*** in this document.

e. ***Designated CII owner (CIIO)*** means the legal owner or operator of the designated CII formally notified by the concerned ministry or regulatory authority.

3. Identification of CII

a. Identification of CII is a complex process with many relative concepts. As per OECD definition, *"Critical information infrastructures ("CII") should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy."*

b. Relevant ministry or regulator should develop a documented mechanism for identification of CII and notify the respective designated CIIO and CII. The "Guidelines for identification of CII" already issued by nCERT may also be referred for the purpose.

c. The Identification mechanism of CII by concerned ministry or regulator of CI should include assessment of the criticality of the concerned CII as well as its dependencies.

d. Criteria for identifying any information infrastructure as CII by a pronounced CI is relative to the sector however, it is important that appropriate rules are formed for the identification of CII by relevant ministry or regulator and following are taken into consideration while making the rules:

   i. The extent to which the sector or service's essential and fundamental operations depend on the network infrastructure, information system, etc.

   ii. The level of damage (definition according to the service involved) that might result in the event that any information system or network infrastructure is destroyed, ceases to function, or its data is breached;

   iii. The associated impact on other sectors and services.

e. It is important to manage CII identification carefully and diligently in order to avoid wasteful utilization of resources.

4. Protection Principles of CII

a. Protection and cyber security of CII should be focused on the continuity of the critical services and reducing the impact of any disruption caused by any environmental, natural, or cyber threats.

b. The implementation of cyber security should get adequate funding & resources, and top management should be involved in developing the structures and strategy for cyber security by making prompt and efficient business decisions on critical cyber security matters.

c. CIIO will be responsible for establishing and maintaining frameworks and policies to ensure the cyber security specific to its sector and service

d. The CIIO is responsible for making sure that the roles and responsibilities, that are pertinent to maintaining the cyber security of the CII, are documented and that the individual working for the CIIO is given responsibility for each of these roles.

e. The document of roles and responsibilities should include authorization of the roles and should be approved by top management.

f. CII should include in its board of directors or any equivalent structure at least one member with expertise in cyber security having the role of oversight of the cyber security program.

g. Each CII should conduct formal cyber security risk assessment of its complete infrastructure through appropriately qualified individuals. All implementation of security controls should be risk driven instead of an ad-hoc or impromptu approach.

h. Implementation of cyber security controls should be realistic, ensuring confidentiality, Integrity and Availability (CIA) of the CII after adequate analysis of the criticality of data and services and approvals of higher management including regulator of the sector, if applicable. For allocation of resources, priority should always be given to the assets "loss or compromise of which could result in ***major detrimental impact on the availability, integrity or delivery of essential services***", as stated in PECA 2016.

i. In any critical sector, if a new CII is to be established, information security should be implemented in the design phase.

j. Appropriate plan and polices for physical and environmental security should be established by CII.

k. Business continuity planning (BCP), Disaster Recovery Plan (DRP) should be a formal document with clarity of actions, roles and responsibilities, training, drill exercises, proper calculations of the recovery point objective (RPO) (specific to the maximum amount of data that may be lost during a disaster and should be used to guide backup strategies), the maximum tolerable downtime (MTD) and recovery time objective (RTO) (related to the duration of an outage). BCP should be realistic and appropriately approved by the higher management of CII and regulator of the CI sector, wherever applicable.

l. CII should conduct supply chain risk assessment and also ensure that acquisition of software and hardware undergoes appropriate testing and evaluation as per their policy.

m. CII should establish a mechanism of internal and external audits for ensuring compliance to the critical sector specific policies, documents and standards. Regulator of the critical sector, wherever applicable, will be responsible for the external audit oversight.

n. Sectoral CERTs should be established to deal with critical specific issues and should develop liaison with organizational CERTs of designated CII as well as nCERT.

o. CII should develop mechanisms for information sharing with sectoral CERTs on information security breaches, incidents, attacks etc. Appropriate mechanisms and criteria for escalation of information on incident to nCERT should also be developed.

p. CII should establish national and international linkages to remain abreast of new threats as well as technologies for cyber security and protection of particular sector.