GUIDELINES FOR IDENTIFICATION

OF

CRITICAL INFORMATION INFRASTRUCTURE

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE (NCIIPC)

Version 1.0 : August 2019

National Critical Information Infrastructure Protection Centre (NCIIPC)
(A unit under National Technical Research Organisation)
Block III, Old JNU Campus,
New Delhi – 110067

Toll Free : 1800 1144 30
Email : helpdesk1@nciipc.gov.in
helpdesk2@nciipc.gov.in

GUIDELINES FOR IDENTIFICATION OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

Relevant Acts and Rules

1. As per IT Act 2000 (amended 2008), **Critical Information Infrastructure (CII) means '*Computer Resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety*'**.

2. Section 70 of the IT Act 2000 lays down that *the appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System'.*

3. Gazette Notification G.S.R 18(E) dated 16 Jan 2014 designates the National Critical Information Infrastructure Protection Centre (NCIIPC), an organisation under the National Technical Research Organisation (NTRO), as the national nodal agency in respect of Critical Information Infrastructure Protection.

4. Gazette Notification G.S.R. 19(E) dated 16 Jan 2014 lays down the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013. Key sections of the Rules are:

(a) Section 2(e) of the Rules lays down that *"Critical Sector" means sectors, which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health or safety.*

(b) Section 4(3) of the Rules mandates the *identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same.*

(c) Section 4(5) of the Rules mandates that *the basic responsibility for protecting critical information infrastructure system shall lie with the agency running that critical information infrastructure.*

(d) Section 5 of the Rules lay down the *Manner of Performing Functions and Duties* and spell out the role and responsibilities of NCIIPC. It also lays down a mechanism for prioritization of actions against threats or vulnerabilities.

5. CII is very likely to be targeted by an attacker so as to disrupt or compromise an IT-enabled capability, service or process of national importance. These capabilities and services are delivered by organizations and enterprises in the critical sectors through various Business and/or Industrial Processes, which run on the underlying Information Technology (IT) and Operation Technology (OT) systems.

6. In order to have a consistent approach for identification of CII within and across all the Critical Sectors, a set of generic guidelines are enumerated in succeeding paras.

Identification and Assessment of CII

7. Assess the criticality of the Functions and Services provided by the Organization / Entity and the magnitude of impact on National Security, National Economy, Public Health or Public Safety in case of incapacitation / destruction of its ICT infrastructure based on the following parameters: -

(a) Impact on Customers, Business & Government functions based on:-

(i) Value of all types of Transactions per day.

(ii) Total number of Transactions per day.

(iii) Number of connected Devices and Network size.

(iv) Number of Customers of different categories.

(b) Timeframe (hours / days / weeks) after which the impact level of non-availability of the ICT infrastructure will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business and Government (shorter timeframe indicates more critical).

(c) Geographical or Environmental impact, if any, of incapacitation / destruction of the underlying ICT infrastructure (area, city, district, state, region, nation-wide or even across international boundary).

(d) Level of Dependency to include:-

(i) Cascading impact of non-availability of functions and services due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other critical sectors / sub-sectors.

(ii) Dependence of essential functions and services on other critical sectors / sub-sectors.

8. If the above assessment indicates that functions and services of the organization / entity have a significant impact nationally, there is a need to evaluate various Business and/or Industrial Processes of the organization / entity from the point of view of identifying those computer resources, the incapacitation or destruction of which may have a debilitating impact on National Security, National Economy, Public Health or Public Safety. Following parameters can be considered for identification of critical business and/ or industrial processes of the organisation:-

(a) Size & Economic Value of the Business /Industrial Process based on:-

  (i) Value of all types of Transactions processed per day.

  (ii) Total number of Transactions processed per day.

  (iii) Number of connected Devices and Network size of the Business /Industrial Process.

  (iv) Number of Customers of different categories serviced.

(b) Criticality of the Business Process and estimated magnitude of impact on National Security, National Economy, Public Health, Public Safety, Customers, Business and Government in case of incapacitation/ destruction of the underlying ICT infrastructure.

(c) Timeframe (hours / days / weeks) after which the impact level of non-availability of the Business /Industrial Process will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business and Government (shorter timeframe indicates more critical).

(d) Level of Dependency.

  (i) Impact of non-availability of Business /Industrial Process due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other Critical Sectors.

  (ii) Dependence of the Business / Industrial Process on other critical sectors/sub sectors.

9. Based on expert judgement and estimation of the above parameters, various Business and/or Industrial Processes are then grouped as critical or non-critical. NCIIPC may be consulted for any clarification in the CII identification process. Consequently, the underlying computer resources of critical processes along with their interconnected dependencies will be categorized to be CII.

10. The appropriate government may, in consultation with NCIIPC, declare the identified CII of the concerned organization through an 'Office Memorandum'. If needed, it may further choose to declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System' through notification in the Official Gazette.

11. For Protected Systems as well as the declared CIIs, *'Rules for the Information Security Practices and Procedures for Protected System',* promulgated vide Gazette Notification dated 22 May 2018 (Regd No D.L.-33004/99), shall be suitably adapted by the Information Security Steering Committee (ISSC) of the organization.