NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

STANDARD OPERATING PROCEDURE (SOP)

Identification of Critical Information Infrastructure (CII) for Notification as Protected System

June 2017

NCIIPC, Block-III, Old JNU Campus
New Delhi - 110067

Table of Contents

Abbreviations/Definitions

CERT-In	**Computer Emergency Response Team - India**
CISO	**Chief Information Security Officer**
CII	**Critical Information Infrastructure**
MeitY	**Ministry of Electronics & Information Technology**
DG	**Director General**
DoT	**Department of Telecommunications**
IB	**Intelligence Bureau**
MHA	**Ministry of Home Affairs**
NCIIPC	**National Critical Information Infrastructure Protection Centre**
RTI	**Right to Information**
Cabsec	**Cabinet Secretariat**
SOP	**Standard Operating Procedures**
Appropriate Government	**As specified in IT Act 2000 (Amended 2008) *"Appropriate Government"* means as respects any matter.- (i) Enumerated in List II of the Seventh Schedule to the Constitution; (ii) Relating to any State law enacted under List III of the Seventh Schedule to the Constitution, The State Government and in any other case, the Central Govt.**

1. Introduction

Establishment of guidelines for identification and notification of CII is an important function assigned to NCIIPC.

2. Objective

This SOP aims to define protocols for the identification of Critical Information Infrastructure elements. These elements are then required to be notified by the "Appropriate Government" vide publishing in the gazette as Protected Systems.

3. Identification and Notification of CII as Protected System

3.1. As per Section 70 of IT Act 2000, CII is defined as "*The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety*."

3.2. An outline process for identification and notification of CII on an annual basis is given below:

3.2.1. The *"Appropriate Government"* shall identify the following:

3.2.1.1. Business processes having impact on national security, economy, public health and safety.

3.2.1.2. The Information infrastructure supporting those business processes.

3.2.1.3. Chief Information Security Officer (CISO) will be the nodal officer for this purpose.

3.2.2. CISO of the concerned organisation of the sector which is deemed critical shall consult NCIIPC for the purpose of CII identification.

3.2.2.1. CISO will check whether the information infrastructure (referred in Para 3.2.1.2) fits into the definition of CII in the Information Technology Act, 2000 (refer Para 3.1). If so, he will inform NCIIPC.

3.2.2.2. NCIIPC will assess whether such information infrastructure fits into definition of CII.

3.2.3. The concerned CISO of the organisation shall form a team which shall ensure that the details required by NCIIPC to assess the organisation's CII are available. These would at a minimum include:-

3.2.3.1. Network Architecture showing how CII is deployed along with details of various Hardware(s) /Software(s) including their version information.

3.2.3.2. Detailed Information Security Framework and V/T/R (Vulnerability/Threat/Risk) Assessment plan.

3.2.3.3. Controls for addressing risks identified through gap analysis.

3.2.3.4. Details of CII including point of contact in case of an incident, list of people along with their designations who are allowed to access CII and location of CII assets.

3.2.4. All such details with reference to the CII shall be sent to, and evaluated by NCIIPC to map their criticality with respect to the architecture and

deployment of the protected system within the overall architecture of the organisation, as well as the interdependencies between organisations.

3.2.5. NCIIPC would review details provided and revert with its recommendations to the concerned organisation with reference to the details received.

3.2.6. After agreement over inputs provided by NCIIPC the concerned organisation shall then send a list of identified CII along with the corresponding designations of people authorized to access it to "*Appropriate Government*" for comments and observations.

3.2.7. These documents shall be reviewed by the "Appropriate Government" based on the larger role of the protected system. On finalising their views, the documents would be returned to NCIIPC for further processing.

3.2.8. NCIIPC will then prepare a draft gazette notification keeping in mind the following considerations:-

3.2.8.1. Any specific details related to CII which can be used as an attack vector shall not be disclosed.

3.2.8.2. Such details shall remain confidential and would be exempted from RTI Act.

3.2.9. The draft approved by DG, NCIIPC shall be sent to DG, CERT-In Director, IB and MeitY for further comments and observations.

3.2.10. DG, CERT-In, Director, IB, Cabsec and MeitY will make further comments and observations over the draft and send their response back to DG, NCIIPC.

3.2.11. The draft after incorporating comments received from DG, CERT-In, Director, IB and MeitY is then sent to the "Appropriate Government" by NCIIPC.

3.2.12. The "*Appropriate Government*" would then review the draft and revert to NCIIPC with comments.

3.2.13. NCIIPC would incorporate any final comments and return the draft to the "*Appropriate Government*" for Gazette notification.

3.2.14. The "*Appropriate Government*" via a Gazette notification notifies the CII as Protected System.

3.2.15. The "*Appropriate Government*" by an order in writing shall authorise the designations of people who are authorised to access Protected Systems notified as above. Such orders should be classified and disseminated only on need to know' basis, as public knowledge of the same may increase their vulnerability from CI angle.

3.2.16. The copy of Notified Gazette should be sent to all organisations that are members of Advisory Committee of NCIIPC, and to all organisations that are members of the Multi Agency Cyber Audit Team for information and record.

4. Review

Present SOP shall be reviewed whenever there is a requirement of an update.

5. Process flow for CII Identification and Notification as Protected System