NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

STANDARD OPERATING PROCEDURE (SOP)

Incident Response

June 2017

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

Table of Contents

Abbreviations

NCIIPC	National Critical Information Infrastructure Protection Centre
CII	Critical Information Infrastructure
OEM	Original Equipment Manufacturer
IR	Incident Response
SI	System Integrator
FTP	File Transfer Protocol
OIC	Officer In Charge
SIEM	Security Information and Event Management
OS	Operating System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
CERT-In	Computer Emergency Response Team - India
CISO	Chief Information Security Officer
SOC	Security Operation Centre

1. Purpose

Purpose of this SOP is to establish protocols for response to security incidents impacting National Critical Information Infrastructure.

2. Tasking

To be first responders for any incidents reported or observed by any elements of our CII.

3. Composition of Incident Response Team

The NCIIPC IR team shall comprise following members depending upon the impact/extent of the incident:-

3.1. Team Lead / Incident Response Coordinator / Alternate Team Lead (to be nominated on rotational basis, every quarter)

3.2. Sectoral Coordinator (of the concerned sector)

3.3. Domain Experts (Technology Specific / Vulnerability Analyst)

3.4. Domain Expert (Live/Dead Forensics)

3.5. Domain Expert (Network Forensics)

4. Toolkits

NCIIPC IR Team should be prepared with Forensics accessories (CD/DVD, HDD, software tools etc) and if required they may help the victim organisation in collecting logs/mirror images.

5. Reporting, Management and Escalation

5.1. Procedure (External)

5.1.1. In case of any security incident, the victim organisation should report the same to NCIIPC at the earliest. Any of the following channels could be used:-

5.1.1.1. Via email to ir@nciipc.gov.in incorporating details of the incident and Incident Response form.

5.1.1.2. Calling Helpline Number (1800114430).

5.1.2. Must nominate a suitable official and convey his contact information to NCIIPC. This individual must be able to provide technical details related to the incident. Alternatively, he must be able to make the required technical personnel available.

5.1.3. Should also arrange meeting with OEM /System Integrator (SI).

5.1.4. Provide all relevant logs to NCIIPC through secure FTP hosted by NCIIPC. Log files need to be password protected and password should be communicated through any media other than internet.

5.1.5. Should also take necessary in house administrative approvals and clearance for visit of Incident Response Team to the incident site or data centre facility.

5.2. Procedure (Internal)

5.2.1. Publish helpline numbers and email IDs.

5.2.2. On reporting of an incident to the 24x7 helpdesk, the OIC helpdesk will contact Director NCIIPC and the Team lead followed by as per the list available to the helpdesk. Officer receiving intimation about the incident will report the same to Director NCIIPC and Team Lead.

5.2.3. Team Lead will contact the victim organisation immediately through the official Landline of Director NCIIPC and understand the nature of the incident. The team lead will instruct to the team to assemble at NCIIPC SOC.

5.2.4. During the first contact with the victim organisation, Team Lead will ask the victim organisation to provide following information:-

5.2.4.1. Dully filled IR Form – the form can follow – just note down what is conveyed.

5.2.4.2. Logs of relevant network devices/SIEMs/OS /Applications and IDS/Firewall/IPS.

5.2.4.3. Mirror image of the compromised system (for root-cause analysis and tracking the attacker).

6. Incident Mitigation

6.1. If the victim organisation is outside Delhi, depending upon the severity and impact of incident if there is a requirement, IR team will visit the victim organisation in order to provide assistance to mitigate the incident and collect the evidence for root cause analysis.

6.2. If the victim organisation is Delhi based and there is a requirement to visit the organisation's location, Team Lead will arrange the visit of the IR NCIIPC team within shortest possible time.

6.3. Other Stakeholders will be incorporated based on the nature of the incident.

7. Information Dissemination

7.1. Sectoral coordinator will send a copy of advisory/incident report to Team Lead. Team Lead will distribute a generic advisory to all CIIs through the sectoral coordinators, after obtaining due approval from Director, NCIIPC. Dissemination of such information must be on a need to know basis, depending on the nature and severity of the incident.

7.2. Sectoral coordinator will send a copy of the advisory/incident report to the concerned Ministry's CISO for information.

7.3. Incident Response will be done in close coordination with CERT-In. As and when required official communications shall be by means of email/letters as per the situation.

7.4. All NCIIPC officials shall follow the standard operating procedure of communication from CIIs or any other agency. Except the IR telephonic communications of urgent nature, all other official communications shall be done only after the due approval of DG NCIIPC.

8. Review

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