NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

STANDARD OPERATING PROCEDURE
(SOP)

Identification of PPP (Public-Private-Partnership) entities for partnership with NCIIPC and formulation of training requirements along-with guidelines for conducting training

June 2017

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

Table of Contents

Abbreviations

BFSI	Banking, Financial Services and Insurance
CERT- In	Computer Emergency Response Team - India
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
DeitY	Department of Electronics & Information Technology
DoT	Department of Telecommunication
IB	Intelligence Bureau
ICS	Industrial Control Systems
IDRBT	Institute for Development & Research in Banking Technology
IR	Incident Response
ISGF	India Smart Grid Forum
MoU	Memorandum of Understanding
NCIIPC	National Critical Information Infrastructure Protection Centre
NIIT	National Institute of Information Technology
OEM	Original Equipment Manufacturer
ONGC	Oil and Natural Gas Corporation
PPP	Public-Private-Partnership
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operation Centre
STQC	Standardisation Testing and Quality Control

1. Introduction

1.1. Developing and organising training and awareness programs is an important function assigned to NCIIPC. Keeping in mind the diversity of sectors, organisations and training requirements in Government and also the private & public sector organisations, NCIIPC needs to identify key PPP (Public-Private-Partnership) entities for partnership and formulating training requirements and undertaking training relevant to their area of operations.

1.2. To facilitate the above, a subgroup was constituted during the first NCIIPC Advisory Board Meeting, held on 11th December 2015. The subgroup included members from Ministry of L&J (Law and Justice), DoT (Department of Telecommunication), IB (Intelligence Bureau), DeitY (Department of Electronics & Information Technology) and NCIIPC. The subgroup was required to frame a SOP for "Identification of PPP for partnership with NCIIPC and formulation of training requirements along-with guidelines for conducting training".

2. Objective

This document provides standard operating procedure for identification of PPP entities for partnership and formulates training requirements and guidelines for conducting training for all stakeholders.

3. Identifying PPPs for partnership with NCIIPC

3.1. Broad parameters for identification of the partner agency/organisation for entering into a PPP are:-

3.1.1. The organisation must be actively engaged in Information Security formulation / implementations / management in a CII Sector, and/or must be recognised by the concerned Ministry. Sectoral Institutions such as Institute for Development & Research in Banking Technology (IDRBT) in BFSI (Banking, Financial services and Insurance), India Smart Grid Forum (ISGF) in Power Sector, Forums/Institutions under Department of Telecommunication (DoT) etc. would be given priority for engaging with PPP partnerships.

3.1.2. The organisation must organically possess the requisite skill set with minimum three years of experience in providing such training course and not perform outsourcing of manpower for conduct of training.

3.1.3. The organisation under consideration must not be blacklisted by any Government agency or authority.

3.2. Some suggested organisations include:-

3.2.1. Government R&D organisation such as Centre for Development of Advanced Computing (C-DAC).

3.2.2. Eminent Government recognised Universities.

3.2.3. Renowned Private Institutions.

3.2.4. Leading ICS/SCADA, OEMs and major public sector organisations such as Powergrid and ONGC.

3.2.5. Selection of private Institutions / organisation could be made in consultation with IB and CERT-In.

To identify a PPP for partnership with NCIIPC, operating procedures mentioned in subsequent paragraphs shall be followed.

4. PPP Proposals

4.1. To identify suitable PPPs across critical sectors, NCIIPC Sectoral coordinators, including Incident Response (IR), Security Operation Centre (SOC), and Research and Development units shall submit their PPP engagement proposals to NCIIPC for examination and approval.

4.2. The PPP proposal shall comprise:-

4.2.1. Details of proposed PPPs.

4.2.2. Description of proposed partner such as qualification and experience.

4.2.3. Expertise and skill- set such as certification level of instructors.

4.2.4. Demonstrated experience in delivery of similar trainings.

4.2.5. Demonstrated experience in working with public agencies.

4.2.6. Capacity to deliver the required quantity and quality of training / services.

4.2.7. Training proposals.

4.2.8. Proposed timelines for the training.

4.2.9. Training requirements of the sector along with desired qualification of the trainees.

4.2.10. Formulation of short term, mid-term and long term engagements.

4.2.11. Budgetary requirements.

4.2.12. Manpower and Infrastructure Requirements.

4.2.13. Additional resources and capacity (If any).

5. Assessments of PPP Proposals by Competent Authority

NCIIPC shall assess the proposals submitted by the Sectoral Coordinators and other NCIIPC Units for correctness, completeness, and feasibility. Further, in order to optimise, projects redundant or similar in nature may be merged by the Competent Authority.

6. Signing of Memorandum of Understanding (MoU)

A MoU shall be signed between NCIIPC and the PPP. The MoU shall outline the sections as mentioned at **Appendix-'A'**.

7. Steering Committee

NCIIPC shall constitute a Steering Committee for each PPP partnership. The Steering Committee shall be headed by the concerned Sectoral Coordinator and shall provide guidance, direction and control to the project and monitor progress or outcomes. Steering Committee shall have five members in total with members from NCIIPC, CERT-In and STQC along with two co-opted members to be nominated by DG NCIIPC. Secretariat support shall be provided by NCIIPC.

8. Training requirements and guidelines for Critical Sectors

8.1. Training Requirements

8.1.1. NCIIPC Training Curriculum

The training curriculum shall be aimed to train the Middle Level Management, Senior Level Management and Chief Information Security Officers (CISOs) about Critical Information Infrastructure Protection,

Information Security & Policies, Cyber Security, Vulnerability / Threat / Risk Analysis, Incident Management & Handling, Cyber Audit etc. The training curriculum is placed at **Appendix-'B'**.

8.1.2. Sector Specific Specialised Training

NCIIPC sectoral coordinators shall submit their sector specific specialised training requirements to Competent Authority. This process may be included in the PPP identification process as explained above.

8.2. Training Guidelines

8.2.1. CISO Training

For conducting the above training critical sector organisations may contact NCIIPC. NCIIPC, in turn may organise training in partnership with PPPs as described in paragraphs above.

However, the critical sector organisation may also organise the NCIIPC CISO Training Curriculum by hiring training entities suitable to their organisational needs. For example, an organisation may include the NCIIPC CISO Training Curriculum in its annual training plan and select a training provider on its own.

8.2.2. NCIIPC Workshops/Trainings

In addition to above, NCIIPC shall also regularly organise workshops/trainings for critical sector CISOs.

8.2.3. Certifications

The trainings may be followed by an exam or test, subsequent to which NCIIPC may provide certification to the trainees.

9. Review

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

Appendix- 'A'

Outline of Memorandum of Understanding (MoU)

1. Preamble of the project
2. Scope
3. Steering Committee
4. Intellectual Property Rights
5. Representations and Warranties
6. Confidentiality and Announcements
7. Term and Termination
8. Governing Law, Arbitration and Jurisdiction
9. Notice
10. Miscellaneous

National Critical Information Infrastructure Protection Centre

Training Curriculum

NCIIPC Training Curriculum is aimed at providing awareness to CISO and Management about their Critical Infrastructure and train them about Information Security & Policies, Cyber Security, Vulnerability/Threat/Risk Analysis, Incident Management & Handling, Cyber Audit etc.

2. The training curriculum is designed to train the Senior & Middle Level Management and is divided into two parts:-

Parts I- Aimed to aware & train the Middle Level Management and focused on Information Security.

Part II- Aimed to aware & train the Senior Level Management. It is more specific and focused on Critical Information Infrastructure Protection (CIIP)

3. The criteria for Senior and Middle Level Management are as follows:-

Senior Level Management

Designation: Director, Dy. Director, Asst Director, ED, COO, GM, Head, CISO, Jt. Secretary (Govt.)

Experience: More than 20 Years

Middle Level Management

Designation: GM, DGM, JGM, AGM, Head, Director (Govt.)

Experience: More than 15 Years

Course Type	Duration	Total Duration (Hrs)
Part - I **For Middle Level Management & Interested parties**	**02 weeks** (01 week = 5 working days; 01 Day = 7 hrs.) **OR** Can be conducted in 2 phases: **1st Phase** - 01 Week **2nd Phase** - 01 Week (15 to 30 days after commencement of Phase 01)	**70**
Part - II **For CISO, Middle & Senior level Mgmt**	**01 week** (01 week = 6 working days; 01 Day = 7 hrs.) **OR** Can be conducted into 02 Phases : **1st Phase** - 03 days **2nd Phase** - 03 Days (30 to 45 days after commencement of Phase 01)	**42**

Course Content

A. Basic Level (Part - I)

Module and Name	Objectives	Duration (approx.)
Module 1 – Overview of Information Security	• Understanding Information Security • Why Care About Security? • Understanding techniques to enforce IS in an organization	3 hrs
Module 2 - Overview of Security threats	• Overview of Information Security Threats • Types of threats – DDoS, Malicious codes, Espionage, etc • Identification of Threats • Modus Operandi • Sources of Threats • Best Practices or Guidelines used to Identify Threats • Best Practices or Guidelines used in mitigation of threats • Collaborate with peers and experts through different forums to understand contemporary issues and solutions	3 hrs
Module 3 - Information Security Vulnerabilities	• Why do Information Security Vulnerabilities exists • Understanding Security Vulnerabilities • Understanding Vulnerability Assessment Tools and Techniques • Techniques to Exploit Vulnerabilities • Techniques to Fix the Vulnerabilities • Best Practices and Guidelines to mitigate security Vulnerabilities	4 hrs
Module 4 – Risk Management	• What is Risk? • Relationship between Threat, Vulnerability& Risk • What Is the Value of an Asset? • What Is a Threat Source/Agent? • What Is a Control? • Risk Management • Different Approaches to Risk Analysis • Best Practices and Guidelines in Assessing and Calculating Risks	3 hrs

Module and Name	Objectives	Duration (approx.)
	• Develop and implement policies and procedures to mitigate risks arising from ICT supply chain and outsourcing. • Best Practices and Guidelines in Mitigating Risks. • Governance, Enterprise Risk Management, Proactive Risk identification & Management	
Module 5 - Network Protocols and Devices	• OSI Model • Data Encapsulation • OSI Layers • Protocols at Each Layer • Devices Work at Different Layers • Networking Devices • Firewall – First line of defense • Firewall Types • Firewall Placement • Firewall Architecture Types • IDS – Second line of defense • IPS – Last line of defense? • Host-based Intrusion Protection System • Network Service • VLAN concept in switch • Static and Dynamic Routing • Securing Internetworks using ACLs	8 hrs
Module 6 - Understanding Directory Services	• Introduction to Directory Services • Benefits of DS in a network • DS implementations in different Operating Systems • Introduction to active directory • Logical structure of active directory • Physical structure of active directory • Creating Domain • Creating Additional DC and Read Only DC • Understanding trees and forest • Creating and managing Global Catalog Servers • Understanding Sites and Securing domain/network through sites • Organizing resources in OU • Understanding Users and Groups	5 hrs

Module and Name	Objectives	Duration (approx.)
	concepts • Groups and their rights • Assigning permissions to users using group membership • Securing environment using Local and Domain Group policies • Group policies object and Group policy templates • Inheritance of group policies • Execution of Group Policies • Backup and Restoration of AD	
Module 7 - Access Control	• Access Control Administration • Accountability and Access Control • Trusted Path • Who Are You? • Authentication Mechanisms • Strong Authentication • Authorization • Access Criteria • Role of Access Control • Control Combinations • Accountability • Types of Classification Levels • Models for Access • MAC Enforcement Mechanism – Labels • Rule-Based Access Control • Remote Centralized Administration	4 hrs
Module 8 - Understanding Security Architecture and Technologies	• Access Control Administration • Accountability and Access Control • Security Features and Implications of technology solutions • Security Technologies and Techniques • Defense in Depth Security Model • Understanding of technology solutions deployed by the organization (servers, applications, databases, OS, routers, switch, etc.) • Hardening of IT and security solutions	4 hrs

Module and Name	Objectives	Duration (approx.)
	• Improving Security • Design, implement, and maintain security architecture of the organization • Best Practices and Security Guidelines • Creation of DMZ Zones for servers	
Module 9 - Understanding Cryptography, Tunneling, and Wireless Security	• Cryptography • Use of certificates in authentication, encryption, and e-commerce • What Is a Tunneling Protocol? • Wireless Technologies – WAP • Software Engineering and System Survivability	3 hrs
Module 10 - Securing your Database	• Database Security Issues • Redundancy and availability of Database • Types of attacks	2 hrs
Module 11 - Focus on Malware, viruses and how they subverts security	• Types of Viruses & Malware • Potential threats, Emerging class of Malware • Means of Propagating • Protection Measures • Special attention to critical infrastructure systems	3 hrs
Module 12 - Operations Security	• Operations Issues • Specific Operations Tasks • Fault-Tolerance Mechanisms • Backups • Facsimile Security • Email Security	5 hrs
Module 13 - Software Development Security	• How Did We Get Here? • Issues in application security (SQL injection, cross scripting, etc.) • Security in SDLC • Modularity of Objects and Security • Security of Embedded Systems • Common Gateway Interface • Virtualization • How to develop secure applications; Application security design	6 hrs
Module 14 - Physical Security	• Physical Security – Threats • Different Types of Threats & Planning • Entrance Protection	2 hrs

Module and Name	Objectives	Duration (approx.)
	• Perimeter Protection • Surveillance/Monitoring • Types of Physical IDS • Facility Attributes • Fire Prevention • Physical Security Compliance and Auditing • Convergence of physical and logical security	
Module 15 - Cloud Computing and Security	• Introduction • IAAS • PAAS • SAAS • Public Cloud • Private Cloud • Hybrid Cloud • Components of Cloud Computing • Understanding Network and security in Cloud • Understanding Data, Application, and Service Control and Ownership in Cloud • Security issues for Clouds • Legal and jurisdictional challenges • Evaluating security of cloud service providers • Standards and frameworks for security and privacy in the cloud • Resource scheduling • Third party secure data publication applied to cloud • Data and information Control Issues and Vulnerabilities • Security Compliance for Cloud Computing • Encrypted data storage for cloud	4 hrs
Module 16 – Securing Industrial Control Systems	• ICS Characteristics, Threats and Vulnerabilities. • ICS Security Program Development and Deployment. • Network Architecture. • ICS Security Controls.	4 hrs
Total Duration		**70 hrs**

B. Advanced Level (Part - II)

Module and Name	Objectives	Duration (approx.)
Module 17 - Business Continuity Plans	• Need of BCP • BCP standards and frameworks • Who Is Ready? • Pieces of the BCP • BCP Development • BCP Risk Analysis • Determining backup strategy • What Items Need to Be Considered in a Recovery? • BCP Plans Creation, Reviews, and Updates	3 hrs
Module 18 – Disaster Recovery Planning	• Proper Planning • Backup/Redundancy Options • Recovery Strategy • Recovery • Testing and Drills	3 hrs
Module 19 – Incident Management and Handling Process	• Seriousness of Computer Incidents • Incidents Management • Triage • Incident Notification and Communication • Guidelines for handling security Incidents • Role of CERT in case of Incident	3 hrs
Module 20 - Third Party Management	• Need for Third Party Management • Identification and management of Third Party Risks • Categorization of Third Parties Based on Risk Perception • Controls for Mitigating Third Parties Risks • Security Considerations when Procuring Services and Products from Third Parties • Auditing of Third Parties • Best Practices and guidelines for managing Third Party Risks	3 hrs
Module 21 - Legal Framework	• Need for Legal Framework and its enforcement • Types of Law • Historic Examples of Computer Crimes • IT (Amendment) Act 2008	3 hrs

Module and Name	Objectives	Duration (approx.)
	• National Cyber Security Policy Identification Protection & Prosecution • Role of Evidence in a Trial • Privacy of Sensitive Data • Sets of Ethics • GAISP- Generally Accepted Information Security Principles	
Module 22 - Privacy Protection	• Understanding Privacy as a Domain • Relationship between security and privacy • Revitalizing security program to enable Privacy Protection • Assess privacy implications of security technologies • Privacy impact assessment • Develop and implement privacy protection measures within the organization	3 hrs
Module 23 - Audit and Testing	• What is Information Security Audit? • Importance of Information Security Audit • Identifying the Information Security Audit Objectives • Audit Planning and preparations • Performing Security Audits and Reviews • Vulnerability assessment and Penetration testing • Code reviews • Audit Controls • Logical security audit • Ethics and codes of conduct for Auditors • Security Policies and Procedure Audits and Compliance Audits • Conduct and Close internal audits • Information Security audit tools • Reporting to senior management on defined parameters	4 hrs
Module 24 - Computer Forensics	• What is Computer Forensics? • What are the benefits of Computer Forensics? • Legal Aspects of Computer Forensics • Role of Computer Forensics in collection of evidence in Cyber Crimes • Digital Evidences • Spoliation and Data Fraud Cases	3 hrs

Module and Name	Objectives	Duration (approx.)
	• Understanding Digital Forensic Process and Procedures • Understanding Computer Forensic investigating and analysis procedures, techniques, and tools	
Module 25 - Information Security Policy and Procedures	• Understanding Security Frameworks • Security Standards • Understanding organizational requirements from an information security point of view • Security Policy, Procedures, and Practices • Develop information security policies and procedures • implement information security policies and procedures • Collaborate with other departments within the organization for effective implementation of security provisions. • Understand the organization and individual behaviors for information security • Update and upgrade Key Performance Indicators for security implementation • Best practices and Guidelines in developing information security policies and procedures	2 hrs
Module 26 - National and International Cooperation	• Global Issues • National Security and Cyber Security • Critical infrastructure protection • Bilateral cooperation • National cooperation Sectorial cooperation • Security Governance • International Information Security Organizations, standards, and Compliances • Information sharing and Incident management at the national and international levels • Global treaties, conventions, etc.	2 hrs
Module 27 - Identification of Critical Infrastructure	• What is "Infrastructure"? • "Critical" Infrastructure and "Key Resources" • Differentiating Critical and Non-Critical "Assets" • Challenges Identifying Critical Assets • Critical Infrastructure	2 hrs

Module and Name	Objectives	Duration (approx.)
	• Policy Issues	

Module 28 - Vulnerability/Threat /Risk Analysis	• **Vulnerabilities**
	  ○ Technology weaknesses
	  ○ Configuration weaknesses
	  ○ Security policy weaknesses
	• **Threats**
	  ○ Unstructured threats
	  ○ Structured threats
	  ○ External threats
	  ○ Internal threats
	• **Attacks**
	  ○ Reconnaissance
	  ○ Access
	  ○ Denial of service
	  ○ Worms, viruses, and Trojan horses
	• **Vulnerability Analysis**
	  ○ Policy identification
	  ○ Network analysis
	  ○ Host analysis
	• **Vulnerability-Threats Assessment for Enterprise Network**
	• **Threat and risk assessment/Analysis**
	• **Risk Assessment/Analysis**
	  ○ Identifying Potential Risks to Network Security
	  ○ Asset Identification
	  ○ Vulnerability Assessment
	  ○ Threat Identification
	  ○ Open Versus Closed Security Models
	• **Risk evaluation** - relationships - most critical assets, and threats - assets and the vulnerability impacts
	• **Threat and risk assessment/Analysis** -
	  ○ identify the safeguards to be adapted to maintain confidentiality
	• **Network security integrity strategy**
	  ○ identifying the areas of greatest risk and concentrate on those triggers like Trojan horses, viruses, and malwares
	• **Risk Assessment Framework**
	  ○ The Concepts of Return on
		4 hrs

Module and Name	Objectives	Duration (approx.)
	Investment ○ Botnets Propagation Mechanism ○ Vulnerability Access Control ○ Estimating Risk and Return on Investment • **The Emergence of Threats on Enterprise Network Information Systems** ○ Threats and the Vulnerabilities ○ Network Exploitation ○ Client – Side and Client to Client Exploitation ○ Governance, Enterprise Risk Management, Proactive Risk identification & Management • **Analysis Tools**	
Module 29 - Inter-dependencies with other sectors / organizations	• Cumulative effects of a single security incident on multiple infrastructures. • Interdependencies Control Strategy • Advantages of Interdependency Analysis • Survival from Disaster by Interdependencies Management	2 hrs
Module 30 - Incidence Response in the NCII domain	**"Network-Centric" Challenges** • Information Inundation • Networking for Networking's Sake Addressing Challenges and Leveraging **"Network Centric" Emergency Response** • Determining Information Requirements • Overcoming Challenges ○ Inaccessible ○ Incomplete ○ Irrelevant • Seizing the Information Domain • Shared Situational Awareness • Greater Mission Effectiveness • Support for Ad-Hoc Operations • Continuity of Operations	2 hrs
Module 31 – Senior Management support to Critical Information Infrastructure Protection	• Support security within the organization through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities • Ensuring the information security policy and the information security objectives are	3 hrs

Module and Name	Objectives	Duration (approx.)
	established and are compatible with the strategic direction of the organization. • Directing and supporting persons to contribute to the effectiveness of the information security management system. • Top management shall establish an information security policy. • Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	
Total Duration		**42 hrs**