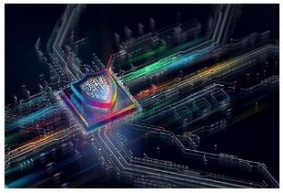

INTRODUCTION

Critical infrastructure systems like those driving power generation, water treatment, electricity production and other platforms are interconnected to form the energy "grid". Although beneficial to the public this grid is vulnerable to cyber-attacks.

Cyber intrusion attempts and cyber- attacks in any critical sector are carried out with a malicious intent. In the power sector it is either to compromise the power supply system or render the grid operation insecure. Any such compromise may result in mal-operation of equipment, equipment damages or even in a cascading grid blackout.

The much-hyped air gap myth between IT and OT Systems now stands shattered. The artificial air gap created by deploying firewalls between any IT and OT System can be jumped by any insider or an outsider through social engineering. After gaining the entry inside the system through privilege escalation, the control of IT network and operations of OT systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/ State sponsored or non-sponsored adversaries and cyber attackers to design more sinister and advanced cyber-attacks.

In order to decrease the risk, leaders/ operators must identify and focus on the elements of cyber-risk to target. More specifically, the many components of cyber-risk must be understood and prioritized for enterprise cybersecurity efforts. Also, there is a need to increase awareness, and development of human resources trained in cyber security technology along with policy makers, law enforcement, judicial actors, who are also equally necessary.

The objective of Training Program is to

- Creating cyber security awareness.
- Creating a secure cyber ecosystem.
- Creating a cyber-assurance framework.
- Strengthening the regulatory framework.
- Creating mechanisms for security threat early warning, vulnerability management and response to security threats.
- Securing remote operations and services.
- Protection and resilience of critical information infrastructure.
- Reducing cyber supply chain risks.
- Encouraging use of open standards
- Promotion of research and development in cyber security.
- Human resource development in the domain of cyber security.
- Information Sharing and cooperation.

DURATION AND METHODOLOGY OF COURSE

The duration of the course will be 100 Hrs. having 2 hours each on alternate days and 4 hours on week-end. The timing of the lecture will be preferably in evening on weekdays and daytime on Saturday / Sunday. The exact day wise schedule shall be available well in advance, before commencement of the sessions of the program. The classes will be conducted in Online mode through MS Teams platform, link of which will be shared by CBIP.

ABOUT CBIP

Central Board of Irrigation & Power (CBIP) a premier Institution, setup by GOI in 1927, is serving the nation in the disciplines of Power, Renewable Energy and Water Resources Sectors for more than 97 years.

It is an exchange and knowledge bank for dissemination of technical knowledge & professional experience to help Engineers / Professionals to update their knowledge and gain practical know-how.

CBIP'S MAIN OBJECTIVE IS

- To disseminate technical knowledge through various modes, e.g., publication of technical documents, organizing conferences /workshops.
- To provide specialized training to the professionals in the Power, Renewable Energy and Water Resources Sectors.

STRENGTHS OF CBIP

- More than 97 years old establishment into dissemination of knowledge in Power, Irrigation and Renewable sectors.
- Almost all reputed utilities of Power, Irrigation and Renewable sectors of the country are the institutional members and at least 3000 senior officers of the level

of Chief engineer and above from these sectors are the members.

- Easy availability and access to the reputed and highly experienced faculty because of above two facts.
- Has a strong base of the very senior officers with deep experience of various disciplines of Power and irrigation sector.
- Has the secretariat of at least 10 international organizations and the Secretary CBIP is the secretary or the member secretary of their India chapters.

FACULTY

Renowned / Reputed and well experienced faculty members / subject expert from Power Industry / Developers / Manufacturers will be delivering the lectures.

RECOGNISION / CERTIFICATION OF THE COURSE

Certificate will be issued by Central Board of irrigation & Power (CBIP) which is a reputed autonomous body in the field of Power & Water Resources with the course module recognised and supported by CEA.

CBIP institute has been recognized as Category-I training Institute by Ministry of Power, Govt. of India and also a recognized training partner of National Skill Development Corporation (NSDC), Power Sector Skill Council (PSSC) and Skill Council for Green Jobs (SCGJ)

COURSE FEE

The Course Fee will be

- Rs. 28,000/- per participant for non- members
- Rs 25,200/- per participant for members of CBIP & SPE.

GST @ 18% shall be payable extra. GST No. 06AAAJC0237F1ZW

PAYMENT PLAN

- Full payment in 02 equal installments for non-sponsored participants. 1st installment at the time of commencing the course & 2nd installment within 30 days from commencement of the course.
- Sponsored participants may pay in single installment.

TO REGISTER

The prospective participants, desirous of attending the above course may register themselves by clicking the following button:

CLICK TO REGISTER

Or by sending the following details to CBIP by email at training@cbip.org
Title of Course:_____
Name:_____
Qualification:_____
Organization /Institute(if any):_____
Mailing address: _____
E-mail:_____
Mob:_____

BANK DETAILS

Payments of course fee should be made by cheque at par/Demand Draft drawn in favour of "**Central Board of Irrigation and Power**", payable at Gurgaon.
or
Online transfer the amount to **Indian Overseas Bank**

Beneficiary Name: Central Board of Irrigation & Power
SB Account No.: 236701000000922
IFSC: IOBA0002367
Branch Code: 2367
Address: Indian Overseas Bank, SCO 26, Sector-31, Gurgaon, Haryana, PIN-122002

**It is compulsory that the details of the payments are shared with CBIP via mail (i.e. mrchauhan@cbip.org or jaideep@cbip.org).

ADDRESS FOR CORRESPONDENCE

A. K. Dinkar, Secretary, CBIP
Sanjeev Singh, Director, CBIP

Nodal Officers:

Shri. M. R. Chauhan, Jt. Advisor (BD)
Mob: 9910378129, Email: mrchauhan@cbip.org
Shri. Jaideep Singh, Chief Manager (T)
Mob: 9871718218, E-mail: jaideep@cbip.org

CENTRAL BOARD OF IRRIGATION & POWER
Malcha Marg, Chanakyapuri, New Delhi -110021
Phone: 011 26115984, E-mail: cbip@cbip.org

CBIP CENTRE OF EXCELLENCE
Plot No-21, Sector-32, Gurgaon, Haryana
Phone: 0124 4035267, E-mail: training@cbip.org

PROGRAM MODULE

S. N.	MODULE/TOPIC	CONTENTS
1.	**Basic Level Cyber Security Training Program for Power Professionals**	
1.1	Introduction to Cyber Security	Introduction to Cyber Security as Cyber Risk Management • What is Cyber Security? • What is Cyber Risk? What factors contribute to CyberRisk? • Basic Risk Models • Cyber Security of IT vs. OT • NIST Cyber Security Framework
		Thinking like a Cyber Security Aware Operator • Device/End Point Security • Server Security • Network Security • Application Security • ICS and SCADA Security
1.2	Network Security	Network Security Fundamentals • Network Diagramming, Zoning and Segregation (Firewalls) • Network Cyber Threats • Network Protocols and their security Issues ➢ DNS, TCP/IP, LAN, Physical Layer Security ➢ Wifi Security ➢ Intranet Security • Mitigation Techniques
		• Firewall • Intrusion Detection and Intrusion Prevention • Detecting Network based Attacks • Encryption, Hashing, Digital Signature • Router Security
1.3	Application Security	Security Threats to Applications – Stand alone, Networkbased applications, Web applications • Application Security Threats and Problems • Application Security Threat Detection and Mitigation • Vulnerability Assessment and Penetration Testing (VAPT)
		• Web Application Security Threats and Attacks • Web Application Attack Detection • SSL/TLS and Digital Certificates • Capturing Web traffic • Web Application VAPT
1.4	Best Practices andAwareness	• NESCOR guide to vulnerability assessment • Security assessment strategy • Risk Assessment
		• Authentication and Authorization • Malware Detection • Network Traffic Analysis • Phishing Awareness • Remote Session Security
1.5	Case studies	Solar, Wind, Pipeline, Black Energy 3 & Stuxnet - Lessons Learnt
		Emerging Technology in Cyber Security: • Intrusion detection system (IDS) • Deception technology • Data diode • SIEM (Security Information and Event Management) • SOC (Security Operation Center) • Technologies for anomaly detection in power system
2	**Intermediate Level Cyber Security Training Program**	
2.1	Risk Driven Cyber Security and Cyber Security MaturityModel	Introduction to Risk Driven Cyber Security • Risk Assessment Methodology • Risk Driven Cyber Security Levels • NIST CSF and 5 core functions
		• NIST CSF Tiers and Maturity Models • Cyber Security Maturity Model
		Implementing IDENTIFY Function • Asset Enumeration, Asset Management System • Asset Vulnerability Assessment • User Life Cycle
		• Authentication and Authorization Technologies • Threat Models based on Asset Vulnerabilities
2.2	Risk Driven Protection and Detection Techniques	Protection Function • Configuration Management • Malware Analysis • Vulnerability Assessment and Pen-Testing • Perimeter Security
		• Risk Analysis and Appropriate Protection Functions • Encryption, Hashing, Digital Signature • Digital Certificates • Web Application Protection
		Detection Function • Intrusion Detection and Intrusion Prevention • Detecting Network based Attacks • End Point Intrusion Detection and Protection
		• Tools for Continuous Monitoring (SIEM, SOC) • Escalation of Cyber Events
2.3	Risk Driven Response	Response Function • Response Planning • Analysis and Forensics • Mitigation Planning
		• Ransomware Attack Response • Supply Chain Attack Response • Risk Assessment Update • Communication and Escalation

2.4	Recovery	• Ransomware Attacks • Backup Process • Recovery from Backups
		• Drills for Recovery • Communication
2.5	Detailed Risk Assessment Methodology	• ISO27001 Risk Methodology • System Architecture diagram • Network Architecture Diagram
		• Dependence Analysis (OEMs and other Service Providers) • Other Risk Factors
		• Risk Matrix • Threat Intelligence • Likelihood Computation
		• Risk Measurements • Risk Based Security Profile
2.6	Need for Organizational Security Policy, Policy Adoption and Policy Implementation	Working Together in formulating Cyber Security Policy for your organization (Interactive)
		Discussing policy formulated, Discuss Implement ability, Fitment to Risk Profile (Interactive)
3	**Intermediate Level Hands-On Practice on Cyber Security for Power Engineers**	
3.1	Hardening Your System	LAB: Hands on Malware Analysis • Manual Tools to check malware • Using File Hashes and Use of Virus Total to check against existing malware
		LAB: Operating System Hardening • Understanding the concept of O/S Hardening against Vulnerabilities • Lynis Tool for Linux • Windows Group Policy Edit Tool • Openscap and Scap Workbench for Configuration Audit
3.2	Finding Security Flows	Application Security • Buffer Overflow Lab • Integer Overflow Lab • Privilege Escalation Labs
		Web Security • Command Injection Lab • SQL Injection Lab • Cross-site Scripting Lab • Cross-site Request Forgery Lab
3.3	Network Security Lab	Network Labs • Arp Spoofing Lab • Packet Sniffing and Packet Analysis Lab • Man-in-the-Middle Attack • Network reconnaissance Lab
		Wifi Network Lab • Password sniffing in wifi network • Reconnaissance on wifi network using aircrack-ng • Wifi password cracking lab
3.4	Intrusion Detection Lab	• Using Snort NIDS • Using Zeek/ Bro NIDS • Visualization of network traffic data
		• Host/Endpoint Intrusion Detection Lab using Wazuh
3.5	Deception Technology Labs and Organizational Security Policy Lab	• Honeypots for Threat Intelligence Collection Lab • Use of Honey Tokens
		Organization Level Security Policy– Requirements, Discussions and Formulation (Discussion Oriented Lab)
4	**Advance Level Cyber Security Training Program for Power Professionals**	
4.1	Cyber Security & Protocol Vulnerability	Introduction to Cyber Security for Critical Infrastructure: • ICS Security • SCADA Security
		• OSI Model
		Understanding of Protocol Vulnerability: • PCN Protocols • Modbus
		• IECTC 57 Protocol
4.2	Standards & Practices	Standards & Best Practices: • NIST SP 80-161 • NERC - CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)
		Incident response & incident reporting
		IEC 62443 Standards: • Zones and Conduits • Patch management
		• Risk Assessment • Security Requirement
4.3	Vulnerability & Malware	Device Level Vulnerability: • Embedded Security • Firmware Analysis • Side Channel Attack
		Malware Analysis: • Static Analysis • Dynamic Analysis
4.4	VAPT	Vulnerability Assessment and Penetration Testing – I • Vulnerability identification • Common SCADA vulnerabilities • Physical access • Vulnerability scanning
		• Server OS testing • Patch levels • Default and insecure configurations

		Vulnerability Assessment and Penetration Testing – II • Authentication and remote access • Attacking ICS & Protocols • Attacking standard services (HTTP, FTP)
		• Attacking server OS • Attacking ISC Protocols • Attacking wireless communications
4.5	Vulnerability Assessment & Forensic	Host, application and platform fingerprinting: • Host and port scanning/Security considerations • Scanning tools and techniques • Scanning ICS/SCADA networks
		• Vulnerability identification • Common SCADA vulnerabilities • Physical access • Vulnerability scanning
		• Server OS testing • Patch levels • Default and insecure configurations
		SCADA Forensic: • Network communications RF signal capture & analysis • Sniffing network traffic
		• Device functionality analysis • Attacking ICS • Attacking standard services (HTTP, FTP) • Attacking server OS
		• Attacking ISC Protocols • Attacking wireless communications • WEP/WPA2 password cracking
5	**Advance Level Hands-On Practice on Cyber Security for Power Professionals**	
5.1	VAPT	LAB: Hands on Penetration Tests: • Penetration Tests of Device and system (Pen Test)/ Physical test • Facility for manually verifying the compliance against NERC • CIP & IEEE 1686 Guidelines. • Application layer protocol and its security extensions test
		LAB: Hands on • IP Scanning • Port scanning tools
5.2	SecurityControls	Physical security & safety • Categorization of system controls • Identification/authentication/Authorization (IA&A) • Remote access security and Encryption. • Logical security
		LAB: Hands on • Concept of UTM box • Firewall details • Security Architecture • Intrusion Detection system • IDS/IPS (Introduction to Snort) • Patch management
5.3	Policy &practices	Strategic Planning and Building a Roadmap forSecuring Critical Infrastructure • Incident response • Active Directory and group policy
		ICS / SCADA Security Maturity Model • Summary of good security practices, depth in defense • Security solutions - Data Diodes, SIEM, SOC/ NOC
5.4	Securing Systems and Brainstorming Policies	An overview of the NIST Cyber security Framework forCritical Infrastructure (Part I) and (Part II)
		Brain storming on relevance of NIST framework in Indiancontext specially for LDCs.
5.5	Lessons Learned	Case study 2 - Ukrainian Power Grid (BlackEnergy3) Cyber- attack & Group discussions on lessons learned from Ukrainian PowerGrid (BlackEnergy3) Cyber attack
		Case study 1 – STUXNET &Group discussions on lessons learned from STUXNET WEP/ WPA2 password cracking.