ONLINE CERTIFICATION COURSE ON

CYBER SECURITY

FOR POWER PROFESSIONALS

100 HRS
DURATION

COMMENCING
19 JAN. 2026

Under the expert guidance of Sh. M.A.K.P Singh (Ex-Member Hydro, CEA & CISO, MoP, GoI)

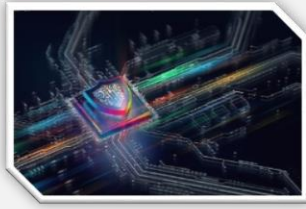
NODAL OFFICERS

Shri. Pradeep Kumar Gupta, Jt. Advisor (BD)
Cell: 9910378062, Email: pradeepgupta@cbip.org

Shri. Jaideep Singh, Chief Manager (T)
Cell: 9871718218, Email: jaideep@cbip.org

Organized By:
Central Board of Irrigation and Power
CBIP Centre of Excellence, Gurgaon

Supported By:
Central Electricity Authority of India



INTRODUCTION

Critical infrastructure systems, such as Power Generation, Transmission, Distribution Networks, Water Resources form the backbone of modern life. These platforms are increasingly interconnected through digital networks, creating a complex and integrated Energy Grid.

This interconnectivity along with Automation, increases efficiency, provides real-time monitoring and control, but also opens the door to cyber threats. A single breach can cause cascading effects across multiple systems, disrupting essential services including Power Generation, Transmission & Distribution and causing economic losses.

The once- believed air gap between IT (Information Technology) and OT (Operational Technology) systems no longer guarantees security. Even with firewalls, insiders or external attackers can exploit social engineering and may take control of both IT and OT systems, sometimes even remotely. Such breaches can expose sensitive operational data and enable Nation, State or non-state actors to plan advanced cyberattacks.

Cybersecurity in critical infrastructure is no longer optional- it's a national priority. Protection demands:

- Robust security frameworks and risk assessments.
- Continuous threat monitoring and incident response
- Awareness and training for operators and administrators
- Collaboration among technologists, policymakers, law enforcement agencies and judiciary etc.

As per the Central Electricity Authority (CEA) Guidelines on Cyber Security in the Power Sector, Central Board of Irrigation and Power (CBIP), has developed a comprehensive Online Certification Course on Cyber Security specifically designed for professionals in the Power Industry.

The structured training program offers Basic, Intermediate, and Advanced level modules, integrating both theoretical knowledge and hands-on practice to strengthen cyber resilience in Critical Infrastructure Systems such as Power Generation, Transmission and Distribution.

CBIP has successfully conducted two batches of the Online Certification Course on Cyber Security, which were attended by over 200 professionals from the Power sector, including the Renewable Energy domain. The program has significantly enhanced participants' understanding and capabilities in safeguarding the nation's critical energy infrastructure against emerging cyber threats.

The objective of Training Program is to

- Create cyber security awareness.
- Create a secure cyber ecosystem.
- Create a cyber-assurance frame-work.
- Strengthen the regulatory framework.
- Create mechanisms for security threat early warning, vulnerability management and response to security threats.
- Secure remote operations and services.
- Protection and resilience of critical information infrastructure.
- Reduce cyber supply chain risks.
- Encourage use of open standards
- Promote research and development in cyber security.
- Develop Human Resource in the domain of cyber security.
- Share information and cooperation.

DURATION AND METHODOLOGY OF COURSE

The course will be of 100 hours duration approx. 10 hrs / per week (2-hour sessions on alternate weekdays and 4-hour sessions on weekends). Weekday classes will be held in the evenings, while weekend sessions will be held during the day. A detailed day-wise schedule will be shared well in advance, prior to the commencement of the program. All sessions will be conducted online via MS Teams, and the access link will be provided by CBIP.

ABOUT CBIP

The Central Board of Irrigation & Power (CBIP), a premier institution established by the Government of India in 1927, has been serving the nation for over 98 years in the fields of Power, Renewable Energy, and Water Resources.

CBIP acts as a knowledge hub and exchange platform for the dissemination of technical expertise and professional experience, enabling engineers and professionals to update their knowledge and gain practical insights.

CBIP'S CORE OBJECTIVES

- To serve as a knowledge hub, disseminating cutting-edge technical expertise through publications, conferences, and workshops.
- To deliver specialized training programs that empower professionals in the Power, Renewable Energy, and Water Resources sectors with practical skills and industry insights.

STRENGTHS OF CBIP

- Legacy of over 98 years in disseminating knowledge in Power, Renewable Energy and Water Resources sectors.
- Institutional membership of almost all reputed utilities in these sectors, with a strong network of 3,000+ senior officers (Chief Engineer level and above).
- Access to highly reputed and experienced faculty owing to its vast network and legacy.
- Strong base of senior professionals with deep expertise across disciplines of Power and Irrigation.
- Secretariat to 10+ international organizations, with the Secretary, CBIP serving as Secretary/Member Secretary of their India chapters

FACULTY

The program will feature lectures delivered by renowned and well-experienced faculty members and distinguished subject experts drawn from the power industry, leading developers, and reputed manufacturers. Their rich professional expertise and practical insights will provide participants with a comprehensive understanding of the subject matter.

RECOGNISION / CERTIFICATION OF THE COURSE

The certificate will be issued by the Central Board of Irrigation & Power (CBIP), a reputed autonomous organization in the field of Power and Water Resources, with the course module recognized and supported by the Central Electricity Authority (CEA).

CBIP is recognized as a Category-I Training Institute by the Ministry of Power, Government of India, and is also an accredited training partner of the 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 may be made in two equal installments by non-sponsored participants- the first installment before commencement of the course and the second installment within 30 days from the date of commencement.
- 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 link:

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. pradeepgupta@cbip.org or jaideep@cbip.org).

ADDRESS FOR CORRESPONDENCE

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

Nodal Officers:

Shri. P. K. Gupta, Jt. Advisor (BD)
Mob: 9910378062, Email: pradeepgupta@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.

Join us in this learning journey and take the next step toward professional excellence. Please visit our website: www.cbip.org