Whitepaper

Payatu

Draft CEA Cybersecurity Regulation 2024:

A Step to Secure India's Power Sector



Copyright notice:

This white paper is the property of Payatu Consulting Pvt. Ltd. No part of it may be reproduced, distributed, or transmitted in any form or by any means, except as permitted below: You may print or download extracts to a local hard drive for your personal, non-commercial use. You may copy the content to individual third parties for their personal use, provided you acknowledge this white paper as the source.
You may not, without our express written permission, distribute or commercially exploit the content. You may not transmit it or store it on any other website or in any other electronic retrieval system.

Copyright@ 2025 Payatu Consulting Pvt. Ltd. All Rights Reserved.

Table of Contents

1. Introduction....4
2. Key Objective of the Proposed Regulations....5
3. Chapter-wise Insights....6
4. High-level Checklist to Comply with Draft Regulations....8
5. Conclusion....9
6. How Can Payatu Help?....10
7. References....11

About the Author....12

1.0

Introduction

As India's power sector becomes increasingly dependent on digital technologies and faces a sharp rise in cyber threats, the **Central Electricity Authority (CEA)** has released the **Draft CEA Cyber Security Regulations, 2024**. It is a critical step in strengthening India's critical power infrastructure. The draft is subject to consultation with various stakeholders, and the final rules have not yet been issued. Building on the CEA (Cyber Security in Power Sector) Guidelines, 2021, the draft expands its scope with a stronger focus on incident response, vendor security, and, operational technology (OT) systems.

These regulations will introduce mandatory cybersecurity audits, define clear roles for CISOs, and set out incident response frameworks. In this whitepaper, we will walk you through the draft overview with key insights for chapter-specific information regarding the draft regulation to help you understand the responsibilities of various stakeholders concerning their specific roles and steps to achieving compliance.

Scope and Applicability

These regulations will apply to all entities in the power sector, including generating companies, transmission licensees, distribution licensees, and control centres. They also require all vendors, contractors, and government organizations dealing with the power sector to adhere to them.



2.0

Key Objectives of the Proposed Regulations

The key objectives of this 2024 Draft Regulations are aligned with what we often recommend to our clients in critical infrastructure sectors:

1. Structured Governance in Cyber Security Programs:
Defining and documenting information security frameworks of the organization.

2. Building Cyber Resiliency:
The required efficiency to cope, adapt and rapidly recover from a cyber-attack.

3 Formalizing Incident Response:
A well structured incident response and crisis management plans for faster and effective responses to cyber incidents.

4. Mandatory Audits and Compliance:
Regular audits will help entities to identify and rectify security gaps before they can be exploited by threat actors.

5. Vendor and Supply Chain Management:
Extending security requirements across the vendors and supply chain and defining assurance requirements.



3.0

Chapter-wise Insights

Chapter I: General Provisions

This chapter defines the regulations' applicability and clarifies that these rules apply to all stakeholders involved in the supply chain—from power generation and transmission distribution companies to vendors. Important definitions, such as Critical Cyber Assets and Cyber Resilience, help everyone understand what types of assets and capabilities need protection.

Chapter II: Composition of Computer Security Incident Response Team (CSIRT-Power)

The creation of **CSIRT-Power** is one of the most pioneering aspects of the regulation. It will serve as a central point of contact for handling cyber incidents in the power sector. It will help manage and mitigate cyber incidents capable of disrupting the stability and security of power infrastructure. CSIRT-Power will collect and analyse traffic data to identify potential cyber threats, providing a comprehensive view of the threat landscape. CSIRT-Power has already been set up in April 2023.

Additionally, Sectoral Computer Emergency Response Teams (CERTs) have been set up for the thermal, hydro, transmission, distribution, grid operations, and renewable energy sectors. **CSIRT-Power** collaborates with sectoral CERTs for specific sectors, such as transmission and renewable energy.

Chapter III: General Cybersecurity Requirements

This chapter outlines basic yet fundamental cybersecurity practices entities must adopt. These efforts include designating **CISO** and **Alternate CISO**, promulgating a cybersecurity policy, deploying security controls (e.g., firewalls, IDS/IPS, etc.), etc.

Chapter IV: Roles and Responsibilities of Responsible Entities

This chapter clearly defines the cybersecurity responsibilities of power sector entities. Key highlights of these responsibilities are the establishment of a **24/7 active ISD**, the need for cybersecurity training for all personnel, acquiring an ISO/IEC 27001 certificate, and ensuring physical and logical segregation between the IT and OT domains.

Chapter V: Functions and Responsibilities of Information Security Division (ISD):

This chapter enlists the ISD's functions in protecting CIIs and protected systems, including policy implementation, compliance review, incident reporting, and threat intelligence management. The ISD will ensure asset vulnerability management and retain secure documentation.

ISD will enforce measures at the entity level using security controls such as system hardening, secure remote access, and cybersecurity requirements in procurements and SLAs. The chapter also emphasizes adherence to the directives of NCIIPC, CERT-In, and CSIRT-Power to maintain a robust level of cybersecurity.

Chapter VI: Chief Information Security Officer (CISO) and Alternate CISO

This chapter contains minimum requirements for CISO & Alternate CISO Qualifications. The CISO will have to serve as the nodal officer for cybersecurity, coordinate with authorities, communicate CCMP matters, and make sure cybersecurity documents are secured as per IS 16335.

Chapter VII: Cyber Security Policy

This chapter presents minimum requirements to be included in the cybersecurity policies of all entities in the power sector.

Chapter VIII: Cyber Crisis Management Plan (CCMP)

This chapter outlines the key requirements of the Cyber Crisis Management Plan (CCMP), which includes event categorization, crisis criteria, stakeholders' roles, SOPs, communication methods, and recovery plans for critical systems. CERT-In should vet and approve the CCMP.

Chapter IX: Additional Requirements for Vendors

This chapter highlights that vendors are required to deliver regular security updates and patches throughout the lifecycle of their products, ensuring their long-term security against cyber threats. It also includes a recovery and restoration plan along with an intimation of the end of life and end of support of all supplied materials.

Chapter X: Cyber Security Audit

This chapter stresses the need for regular cybersecurity audits to maintain an organization's overall security posture. IT systems are supposed to be audited bi-annually, whereas OT systems are supposed to be audited annually. The regulations also stress the need to address vulnerabilities through timely and systematic patching.

Chapter XI: Physical Security

This chapter highlights the physical security requirement for all critical cyber and non-cyber assets.

Chapter XII: Critical Information Infrastructure (CIIs) Identification

This chapter contains requirements for CII identification and notification. All entities must provide the information NCIIPC requires to identify CII. Details of new cyber assets need to be submitted within 30 days.

Chapter XIII: Miscellaneous

This chapter explains the monitoring and compliance framework, focusing on third-party audits and self-audits to ensure cybersecurity laws are followed. It describes the rules for sending yearly self-audit reports to CISO-MoP and CSIRT-Power, including non-compliance details and actions to fix issues. It also includes rules for reviewing cybersecurity policies, training staff, and raising awareness through ongoing education. To address operational problems, the authority can still change or relax regulations.

4.0

High-level Checklist to Comply with Draft Regulations

The entities in the energy sector can use the following checklist to align their efforts with the Draft Regulations:

Governance:
- Appoint an adequately qualified Chief Information Security Officer (CISO) and alternate CISO.
- Establish a documented and approved Cybersecurity Policy.
- Establish an Information Security Division (ISD). The minimum workforce required for setting up an ISD is 04 (Four) officers, including a CISO and 04 officers/officials for shift operations.

Cyber Crisis Management Plan (CCMP):
- Create and implement a Cyber Crisis Management Plan approved by the entity's senior management.
- Ensure communication protocols and reporting formats are in place with CSIRT-Power and CERT-In for incident reporting

Cybersecurity Controls:
- Ensure the firewalls, IDS/IPS systems, and Web Application Firewalls are appropriately deployed.
- Ensure that websites, web portals, or applications have passed cybersecurity audits before hosting on the internet.
- Restrict remote access, especially remote access to OT infrastructure.

Training and Awareness:
- Ensure all individuals, including contractors and vendors, receive obligatory cybersecurity training.
- CISOs and ISD personnel should undergo at least 10 person-days of cybersecurity training yearly.

Vulnerability Management:
- Perform a vulnerability assessment and fix/remediate any problems found.
- Make sure important/critical system updates and security fixes are done regularly.

Incident Reporting:
- Report cybersecurity incidents to CSIRT-Power, CERT-In, and NCIIPC within prescribed timeframes.

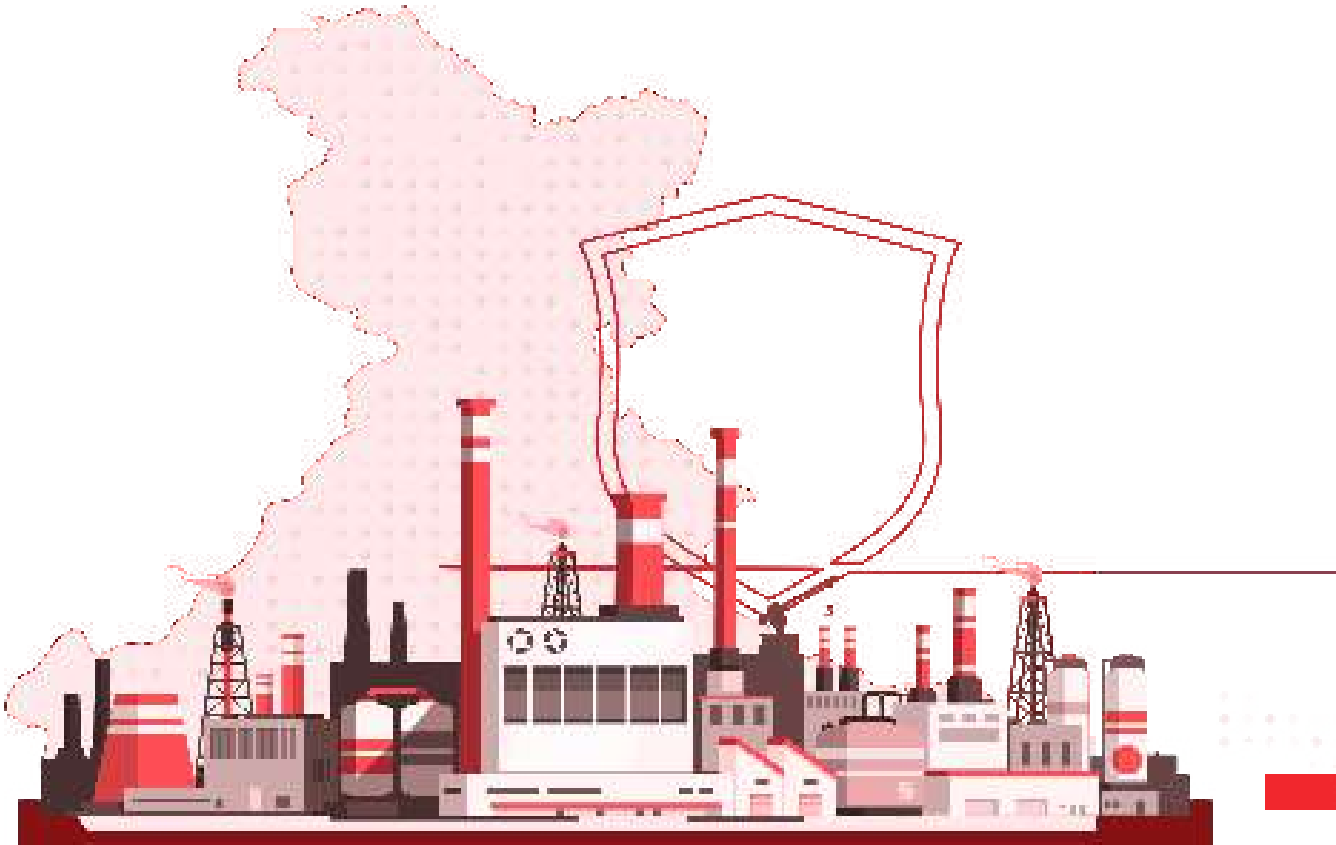
Audits and Assessments:
- Conduct bi-annual IT system cybersecurity audits and an annual OT system audit.
- Address all critical and high-risk vulnerabilities within a defined timeframe.
- Send audit reports to relevant authorities within six weeks after finishing the audit.



5.0

Conclusion

The Draft CEA Cyber Security Regulations, 2024 will change how the power sector handles cybersecurity. It sets clear rules for managing cybersecurity, responding to incidents, and ensuring compliance. These regulations will be a step towards safeguarding critical power infrastructure from ever-evolving cyber threats.



6.0

How Can Payatu Help?

Compliance with these exhaustive regulations is challenging. Payatu offers professional assistance for compliance and security:

Policy Development:
Customized cybersecurity policies in accordance with regulatory compliance.

Training:
Training programs ensure that all individuals, including employees, contractors, and vendors, receive obligatory training and acquire the required skills and certifications.

Audit Support:
Pre-audit assessment with actionable remediation recommendations.

Incident Response:
Design and implementation of effective response frameworks.

Ongoing Compliance:
Perform a vulnerability assessment and fix/remediate any problems found.
Make sure important/critical system updates and security fixes are done regularly.

The collaboration with Payatu will enable entities in the energy sector to confidently address the challenges of complying with the Draft CEA Cyber Security Regulations, 2024.

7.0

References

CEA (Cyber Security in Power Sector) Guidelines, 2021
Draft Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024



About the Author



Abhishek Pandey
Senior SCADA Security Consultant - Payatu

Abhishek Pandey brings over **seven years of research and industry experience**, along with three years in academia, specializing in **Operational Technology (OT) and Industrial Control Systems (ICS) Cybersecurity**.

His expertise spans **risk consulting, vulnerability assessment, network architecture review, IT/OT integration security**, and compliance with globally recognized frameworks including **IEC 62443, NIST 800-82**, and **ISMS standards**.

Abhishek has contributed to critical cybersecurity projects across **India and the Middle East**, helping industrial enterprises and critical infrastructure operators strengthen their cyber resilience.

To learn more, connect with him on LinkedIn.

About Payatu

Payatu is a research-powered cybersecurity consulting and training company delivering deep technical expertise across offensive security, secure design, and infrastructure risk assessments. It is present in over 20+ countries, and has domains spanning across IT, OT, Cloud, IoT, and embedded security. Payatu's comprehensive service offerings cater to modern security needs across critical infrastructure, applications, products, and engineering environments.

CORE SERVICE OFFERINGS

CRITICAL INFRASTRUCTURE & OT SECURITY

Payatu provides end-to-end OT/ICS cybersecurity services aligned with IEC 62443, NIST800-82, NCIIPC directives, and CEA Guidelines. Maturity and risk assessments, passive scanning, zone-conduit modelling, and secure architecture design are at the top of its capabilities. Clients are assisted in validating cybersecurity requirements during FAT/SAT, developing minimum baseline security standards (MBSS), and implementing asset inventory and monitoring solutions. Payatu's OT GRC advisory ensures governance frameworks are practical, compliant, and tailored to industrial environments.

PRODUCT & IoT SECURITY

Security assessments for embedded systems, IoT devices, and edge platforms, covering firmware, communication protocols, device-to-cloud data flow, and hardware-level protections are delivered exceptionally. The services also include threat modeling, fuzzing, exploitability testing, and secure product development advisory to ensure resilient design across all connected components.

WEB, MOBILE & CLOUD SECURITY

Payatu performs comprehensive VAPT of modern web, mobile, and cloud-native applications, including APIs and third-party integrations. Its coverage includes OWASP-ASVS mapping, business logic flaw detection, cloud misconfiguration reviews, and in-depth analysis of IAM, storage, and deployment risks across AWS, Azure, and GCP environments.

RED TEAMING & THREAT INTELLIGENCE

Payatu's red teaming services simulate real-world threats across IT and OT environments, emulating advanced adversaries through lateral movement and persistence. It also delivers cyber threat intelligence (CTI) services, including dark web monitoring, infrastructure threat feeds, brand monitoring, and targeted campaign tracking, to detect and respond to evolving risks.

DEVSECOPS & SECURE CODE REVIEW

Payatu embeds security directly into your development workflows through end-to-end DevSecOps consulting. This includes secure code reviews, IaC audits, configuration analysis, and pipeline security controls. The approach covers static code analysis, secure coding practices, and remediation guidance to empower development teams to shift security left.

TRAINING & LAB DEVELOPMENT

Payatu builds custom hands-on labs and training programs focused on IoT, ICS, offensive security, exploit development, and red teaming. Its offerings are designed for engineers, SOC teams, and practitioners and include both instructor-led and self-paced formats. With proprietary platforms and tailored ICS challenge labs, we deliver real-world, scenario-based cybersecurity learning environments.

CONTACT US

Payatu Security Consulting Pvt. Ltd.

info@payatu.io

+91 20 41207726

www.payatu.com