
# ACPET's Comments on the draft Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024

In response to the Central Electricity Authority's (CEA) draft regulations on Cyber Security in the Power Sector, ACPET has carefully reviewed the proposed framework and prepared detailed comments and suggestions. Our objective is to contribute to the development of a secure, resilient, and forward-looking power sector capable of addressing emerging cyber threats.

This document presents our observations and recommendations aimed at strengthening the cyber security infrastructure outlined in the draft regulations. We hope these insights will assist in refining the regulatory approach and ensuring its successful implementation across the industry.

As cyber threats continue to evolve, it is imperative that our regulatory framework remains robust and flexible. ACPET remains committed to supporting efforts that fortify the power sector's defences against these growing challenges.

## INTRODUCTION

The Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024, represent a significant step towards bolstering the cyber resilience of India's power sector. Given the criticality of electricity infrastructure and the increasing sophistication of cyber threats, these regulations are essential to protect the nation's energy security. However, there are a few areas where, it is suggested that, the regulations could be further strengthened and clarified.

## SPECIFIC COMMENTS ON KEY PROVISIONS AND ANALYSIS:

- **Definitions and Scope:** The regulations provide clear definitions of key terms, ensuring a common understanding among stakeholders. The wide scope of applicability, encompassing responsible entities, regional power committees, and associated organisations, demonstrates the government's commitment to a comprehensive approach. The following are however suggested:
    - **Critical Assets:** The definition could be more specific to include assets, facilities, systems, and equipment that are essential for the continuous operation of the power grid, including but not limited to critical substations, transmission lines, generation plants, control centres, and communication infrastructure.
    - **Special attention is drawn to the need to cover and define areas relating to additional vulnerabilities arising out of the increasing renewable energy component in the grid.**
    - **Vulnerability Assessment:** Consider defining the specific methodologies and tools that should be used for vulnerability assessments such as network scanning, penetration testing, and vulnerability scanning. It may specify that Vulnerability Assessment shall mean a process of identifying and quantifying vulnerabilities using recognised methodologies and tools, such as network scanning, penetration testing, and vulnerability scanning.

- **CSIRT-Power:** The establishment of a dedicated Computer Security Incident Response Team (CSIRT)-Power is indeed a crucial step. Its role in setting cyber security frameworks, serving as a point of contact, and coordinating incident responses is pivotal for effective threat management. However, the following are suggested.
    - **Mandated Membership:** It is suggested that the regulations can also mandate the membership of key stakeholders, such as representatives from the Central Electricity Authority, the Ministry of Power, the National Critical Information Infrastructure Protection Centre (NCIIPC), the Computer Emergency Response Team-India (CERT-In), and other relevant stakeholders to ensure effective coordination and information sharing.

- **Incident Response Plan:** It is proposed that the regulations may offer more specific guidance on the development and implementation of incident response plans, including requirements for detection, containment, eradication, recovery, and lessons learned. It can also specify the periodicity at which the plan shall be tested and updated.

- **General Cyber Security Requirements:** The regulations mandate various security measures, including the appointment of CISOs, development of cyber security policies and crisis management plans, and deployment of security devices. These requirements align with industry best practices and are essential for safeguarding critical infrastructure. However, the following are suggested.

  - **Remote Access:** If possible, the regulations may offer more specific guidance on the security measures that should be implemented for remote access, such as the use of VPNs and multi-factor authentication.

  - **Cyber Security Awareness:** Provision of more specific guidance on the content and frequency of cybersecurity awareness programs, including topics such as phishing, social engineering, incident reporting and best practices for password management may please be considered.

- **Roles and Responsibilities of responsible entities:** The regulations clearly outline the roles and responsibilities of responsible entities, CISOs, and the Information Security Division (ISD). This ensures a clear division of labor and accountability. However, the following are suggested.

  - **Third-Party Audits:** The regulations can mandate periodic regular third-party audits by qualified auditors having expertise in power sector cyber security to verify compliance with regulations.

  - **Supply Chain Security:** The regulations may provide more specific guidance on supply chain security, including requirements for vendors to provide security certifications, such as ISO 27001, and undergo regular security assessments to identify and mitigate risks.

  - **Para (9) may be amended as follows:** Ensure physical separation between critical OT system and enterprise IT system. In case, physical separation is not possible, suitably hardened logical separation shall be ensured.
    *Provided that Enterprise IT networks having identified Critical Information Infrastructure shall be isolated from other/ rest of IT networks. Risk associated with IT – OT integration should be assisted and necessary. Security control should be deployed to mitigate all possible risks. It should be approved by the board of directors. Further, RE shall ensure continuous monitoring of the IT – OT integration to have complete visibility of the traffic flowing to capture the presence of any malicious activity.*

  - **Following Paras may be added:** Establish Security Operation Center (SOC) to carry out day to day security operations activities in the Security Operation

Centre (SOC), like surveillance and monitoring of IT and OT systems and assets, support the identification of threats and vulnerabilities, provide incident response and remediation support. Cyber Security logs, alerts and events from all IT and OT equipment should be available in Security Operation Center.

- Additionally, while the roles of CSIRT-Power and CCMP, as defined in the draft rules, take precedence after occurrence of a Cyber incident, SOC may be considered as a critical step towards pro-actively preventing Cyber Incidents.

- In point 8 of Chapter V "Functions and Responsibilities of Information Security Division," the requirement of a SOC with focus on Red-team as well as blue-team may be explicitly defined. SOC needs to be manned by cutting-edge Cyber Security experts working round the clock.

- The same could also be explicitly spelt out in the point 6 of Chapter IV "Roles and Responsibilities of Responsible Entities."

- The proposed framework in the draft rules outlines baseline requirements for the Cyber Security Policy and General Roles and Responsibilities. It could lay more emphasis on a proactive approach to preventing cyber attacks. In the current era of cyber warfare, where determined nation-state actors employ Advanced Persistent Threats, a proactive approach is essential to ensure the cyber security of a sector as critical as power. With a view to address this it is recommended that Security Operations be explicitly mandated as a function of the Information Security Division in Chapter V. Additionally, the manpower of the ISD, as detailed in Schedule I Part I of the rules, may be enhanced to include skilled personnel with red-teaming and blue-teaming capabilities.

- **Cyber Security Policy:** The requirement for a comprehensive cyber security policy is a positive development. The policy should address a wide range of aspects, including asset management, risk assessment, access control, and incident response. However, the following are suggested.

  - **Data Privacy:** The regulations may include more specific guidance on robust data privacy requirements, including data classification, access controls, and encryption, particularly in relation to personal data in accordance with applicable laws and regulations.

  - **Supply Chain Risk Management:** The regulations may include more specific guidance on supply chain risk management to assess and mitigate risks associated with third-party vendors, including requirements for vendors to provide security certifications and undergo security assessments.

  - **Vulnerability Assessment and Penetration Testing (VAPT)**: These are mentioned at point (16) of Chapter VII "Cyber Security Policy" which talks of VAPT prior to commissioning of a system. Security Operations and VAPT shall be a continuous activity for pro-actively detecting vulnerabilities in live Cyber Critical systems and may be explicitly laid out in the rules.

- **Following may be considered for addition:**
  (a) There should be clear SOP to decide useful life of the system, after which it will become obsolete.
  (b) Responsible Entity shall identify all the legacy systems along with their potential cyber security vulnerabilities and shall ensure that controls are implemented according to the defined information security risk treatment process such as:

  i. Implementation of strict and appropriate network segmentation
  ii. Remote access for configuration and maintenance purpose should be avoided.
  iii. It should be ensured that equipment and components used for maintenance and configuration purposes of legacy systems are adequately secured.

  (c) Usage of external removable and mobile devices should be restricted in critical and associated networks. If their usage is unavoidable, SOP for secure usage should be formulated incorporating provision for scanning of such devices for malicious code and mitigation of all associated risk prior to allowing the device to connect to OT devices or CII.

  (d) Regular conduct of penetration testing of IT and OT including CIIs as per guidelines issued separately.

- **Cyber Crisis Management Plan (CCMP):** The CCMP is undoubtedly a vital tool for coordinated responses to cyber incidents. Its development and regular review are essential to ensure preparedness and effectiveness. However, the following are suggested.

  - **Testing and Exercises:** The regulations may additionally mandate regular testing and regular tabletop exercises and simulations to Test, the effectiveness of their CCMP with a view to ensure its effectiveness. Such exercises may be conducted at least annually and involves key stakeholders from across the organisation.

  - **Recovery Time Objective (RTO):** Each Responsible entity shall define Recovery Time Objective (RTO) for every Cyber Asset (whether Critical or otherwise). RTO is the maximum time a Cyber Asset can be in-operational after an outage, without causing significant damage to the business. Ensuring strict RTO is an essential component in preparing a Recovery Plan and ensuring Business Continuity. This requirement for RTO may be explicitly incorporated in point 17 of Chapter VIII - Cyber Crisis Management Plan.

- **Additional Cybersecurity Requirements for Vendors:**
    - It is proposed that the regulations may require vendors to provide security certifications, such as ISO 27001, to demonstrate their commitment to cybersecurity. Certifications should be current and relevant to the services or products being provided.
    - **Following Para may be considered for addition:** Security related aspects to be incorporated in Service Level Agreement (SLA) with the OEM/ Vendor/ Third party. SLA should also incorporate penalty clauses for non-compliance.

- **Cyber Security Audit:** The regular cyber security audits proposed in the regulations are a necessary component of a robust security posture. The regulations mandate such audits and provide guidelines for their conduct. However, the following is suggested.
    - **Audit Scope:** The regulations may provide more specific guidance on the scope of cybersecurity audits, including requirements for assessing the effectiveness of cybersecurity controls and identifying vulnerabilities and evaluating compliance with applicable regulations. It is also suggested that Audit should cover a wide range of areas, including network security, application security, data security, and incident response.
    - **Para 25 can also include IEC 62443:** The Cyber Security audit shall be conducted through a CERT-In empanelled Cyber Security Auditor or cyber security auditor as per NCIIPC scheme as and when the same comes into existence. These Cyber Security audits shall be carried out as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335, ISO/IEC 27017, *IEC 62443* and any other Cyber Security audit directions issued by the Authority.
    - **Following Para may be considered for inclusion:** Auditor shall have power sector domain expertise to conduct audit of OT systems. In addition, selection of the auditing agencies may be based on Quality Cost Based Selection (QCBS) basis and not just L1 basis for improving the quality of Audit. Independent External Auditor should be engaged directly by the entity not by OEM/ vendor of the system.

- **Physical Security:** The emphasis laid by the regulations on physical security is equally important, as physical access can provide a pathway for cyberattacks. The regulations mandate measures to protect critical assets and restrict physical access. However, the following is suggested.
    - **Specific Measures:** Provision of more specific guidance on physical security measures, such as the use of security cameras, intrusion detection systems, and access control systems and physical barriers, to protect critical infrastructure from unauthorised access and physical threats maybe considered.

- **Critical Information Infrastructure (CIIs) Identification:** The regulations correctly require entities to identify and report CIIs to NCIIPC, ensuring that critical systems receive the necessary protection. However, the following may be considered.
    - **Prioritisation:** The regulations may include guidance on the prioritisation of CIIs for protection based on their criticality to the to the operation of the power grid. Critical CIIs shall be identified and protected using appropriate security measures.

- **Schedule –I, Part-I: Indicative minimum required officers/officials in ISD.**
    - **Following Para may be considered for addition:**
      ISD should have expertise in Cyber Risk Management, Technology & System Security Architect, Cyber Security Analysis, Vulnerability and Threat Analysis, Security Operations Analyst, Internal Audit capabilities etc.

**GENERAL SUGGESTIONS:**

While the draft covers many critical aspects, the following additions would make it more comprehensive and operationally effective:

- **Enhanced Threat Intelligence:**
    - Implementation of automated mechanisms for ingesting and disseminating threat feeds.
    - The CSIRT team should create guidelines for threat prioritization based on sector-specific risks.
    - Develop procedures for secure sharing of sensitive threat information.

- **Detailed OT Security Guidelines:**
    - Specify requirements for air-gapping/ physical isolation from the internet of critical OT systems, such as data backup protocols and usage of faraday cages for systems that are electrically sensitive or have.
    - Develop guidelines for secure remote access to OT environments. Every instance of remote access should be approval based to infuse accountability rather than an encompassing approval.
    - Mandate regular vulnerability assessments specific to OT systems.
    - Establish protocols for secure firmware updates in OT devices.
    - Develop standards for OT system hardening and configuration.
    - Establish requirements for OT-specific security monitoring tools.

  - Specification of security in converged environments, i.e., environments where IT and OT assets require sharing of a common network.

- **Comprehensive Supply Chain Security:**
  - Vendor Management protocols for continuous monitoring of supplier security postures, or at the least, requirement of cybersecurity testing reports submission.
  - Develop standards for hardware supply chain security.
  - Establish requirements for third-party code audits and reviews.
  - Extending the requirement of SBOM, create guidelines to assess possible risks from fourth party (supplier's suppliers) deliverables.
  - Extend the requirement of cybersecurity training for maintenance personnel to outline protocols that manage compromise risks and leakage of information.
- **Cybersecurity Metrics and Reporting:**
  - Establish guidelines for risk quantification in terms of impact to the nation's functioning.
  - Create dashboards for real-time visibility into sector-wide cybersecurity posture. Personnel with diverse levels of information access should be able to view the current cybersecurity posture and risks of the assets under their purview.
  - Infrastructure monitoring should be put in place to continuously assess the network gateways that connect to the public internet for vulnerabilities, and malicious traffic (payloads, source, and destination reputation, etc.).
  - Establish comprehensive guidelines for log collection, retention, and analysis to ensure the right amount and quality of data is present for CSIRT to investigate when deemed necessary.
  - Create protocols for automated alert triage and response.
  - Establish requirements for threat hunting activities.
  - Use of honeypot for deception as a precautionary measure.
  - Develop guidelines for user and entity behavior analytics (UEBA).
  - Create standards for asset discovery and vulnerability management integration.
  - Establish protocols for continuous compliance monitoring.
- **Third-Party Risk Management:**

- Establish requirements for third-party employee background checks.
- Create protocols for managing fourth-party and Nth-party risks.
- Develop guidelines for secure decommissioning of third-party services and exit protocol with appropriate documentation.

- **Regular Review Mechanism:**
  - Establish a framework for continuous regulatory gap analysis
  - Develop protocols for emergency regulatory updates in crisis situations.
  - Establish guidelines for measuring the impact of regulatory changes.
  - Develop standards for aligning national regulations with international best practices through R&D, industry engagement and continuous benchmarking with international frameworks such as NIST, NERC and IEC.
  - Create protocols for sunset reviews of outdated regulations.

- **Miscellaneous:**
  - Enhance Enforcement Mechanisms: Consider providing penalties or sanctions for non-compliance to incentivise adherence to the regulations.
  - Facilitate Collaboration: Foster collaboration between industry stakeholders, academia, and government agencies to share best practices and address emerging threats.
  - Promote Awareness: Conduct regular awareness programs and training sessions to educate personnel about cyber security risks and best practices.
  - Review and Update Regularly: Regularly review and update the regulations to ensure they stay relevant and effective in the face of evolving threats.
  - The regulations could also draw from the recommendations of the Niti Aayog published in March 2024 titled “Final Report on “Domestic Manufacturing Capacity & Potential Cyber Security Challenges in the wind sector and Way Forward”. A copy thereof is enclosed for ready reference.

## CONCLUSION

The Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024, represent a significant step towards safeguarding India's critical power infrastructure. It is felt that by implementing these regulations, the power sector can further enhance its cyber resilience and protect against the growing threat of cyberattacks. However, continuous evaluation, refinement, and enforcement are essential to ensure their long-term effectiveness.