**GOVERNMENT OF INDIA**
**CENTRAL ELECTRICITY AUTHORITY**
**(MINISTRY OF POWER)**
**Sewa Bhawan (North Wing), Room No. 622, 6th Floor,**
**R. K. Puram, New Delhi-110066**
**Tel. Fax -011-26103246, email: celegal-cea@gov.in**
**Website: www.cea.nic.in**

# PUBLIC NOTICE

In accordance with the Section 177 of the Electricity Act, 2003, the Central Electricity Authority (CEA)**,** proposes to notify the **draft Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024.** The proposed draft regulations are available on the CEA Website www.cea.nic.in for inviting public comments. The Regulations can also be inspected in the office of Chief Engineer (Legal), Sewa Bhawan (North Wing), Room No. 622, 6th Floor, R. K. Puram, New Delhi-110066 on any working day till **10th September, 2024** between 1100 hrs to 1600 hr**s.**

2. All the Stakeholders including the public are requested to send their comments on the draft regulations to Chief Engineer (Legal), Sewa Bhawan (North Wing), Room No. 622, 6th Floor, R. K. Puram, New Delhi-110066 by post or through e-mail (celegal-cea@gov.in) latest by **10th September, 2024.**

**(Rakesh Kumar)**
**Secretary, CEA**

# NOTIFICATION

**No.** ---------- In exercise of the powers conferred by sub-section (1) of 177 of the Electricity Act, 2003 (36 of 2003), the Central Electricity Authority hereby makes the following regulations for Measures relating to Cyber Security in Power Sector, namely: -

## Chapter-I

1. **Short title and Commencement.** - (1) These regulations may becalled the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2024.

   (2) They shall come into force six calendar months, from the date of their publication in the Official Gazette, except for the Regulations 7(4), 8(2), 8(3),7(11)(b),8(5),9 which may come in to force on such date as the Authority may notify. These regulations shall come into force on such date as the Authority may notify. Provided that different dates may be appointed for commencement of different regulations.

   (3) **Scope and Extend of Applicability:** These regulations shall apply to all Responsible Entities, Regional Power Committees, Appropriate Commission, Appropriate Government and Associated Power Sector Government Organizations, Training Institutes recognized by the Authority, Authority and Vendors.

2. **Definitions**, - (a) In these regulations, unless the context otherwise requires, -

   (1) Accreditation: shall mean the process of verifying that an organization is capable of conducting the tests and assessments against a product/process that are required to be certified.

   (2) Accreditation Body: shall mean an organization that has been accredited to verify the credentials and capabilities of the organizations that wish to become a certification body.

   (3) Asset: shall mean anything that has value to the organization.

   (4) Attestation: issue of a statement, based on a decision, that fulfilment of specified requirements has been demonstrated

   (5) Certification: third-party attestation related to an object of conformity assessment, with the exception of accreditation.

   (6) Certification Body: shall mean an organization that has been accredited by an accreditation body to certify products/ process against a certification scheme.

   (7) Certification Scheme: certification scheme is a conformity assessment scheme that includes selection, determination, review, decision and finally certification as the attestation activity.

   (8) Chief Information Security Officer: means the designated employee of Senior management, directly reporting to Managing Director /Chief Executive Officer/Secretary of the organization, having knowledge of information security and related issues,responsible for cyber security efforts and initiatives including planning, developing, maintaining, reviewing and implementation of Information Security Policies

(9) Critical Assets: shall mean the facilities, systems and equipment which, if destroyed, degraded or otherwise declared unavailable,would affect the reliability or operability of the Power System.
(10) Critical Cyber Assets: shall mean cyber assets essential to the reliable operation of critical asset.
(11) Critical Systems: a group of critical Assets and/or Critical Cyber Assets or parts that work together.
(12) Critical Information Infrastructure: shall mean Critical Information Infrastructure as defined in explanation of sub-section (1) of Section 70 of the Act.
(13) Cyber Assets: shall mean the programmable electronic devices,including the hardware, software and data in those devices that areconnected over a network, such as LAN, WAN and HAN.
(14) Cyber Crisis Management Plan: shall mean a framework for dealing with cyber related incidents for a coordinated, multi- disciplinary and broad-based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical processes.
(15) Cyber Resilience: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, orcompromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.
(16) Cyber Security Breach: shall mean any cyber incident or cyber security violation that results in unauthorized or illegitimate accessor use by a person as well as an entity, of data, applications, services, networks and/or devices through bypass of the underlying cyber security protocols, policies and mechanisms resulting in the compromise of the confidentiality, integrity or availability ofdata/information maintained in a computer resource or cyber asset.
(17) Cyber Security Incident: shall mean means any real orsuspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorizeduse of a computer resource for processing or storage of informationor changes to data, information without authorization.
(18) Cyber Security Policy: shall mean documented set of business rules and processes for protecting information, computer resources, networks, devices, Industrial Control Systems and other OT resources.
(19) Electronic Security Perimeter: shall mean the logical border surrounding a network to which the Cyber Systems of Power Systemare connected using a routable protocol.
(20) Information Security Division: shall mean a division accountable for cyber security and protection of the Critical System of the Responsible Entity.
(21) Internet: The single interconnected world-wide system of commercial, government, educational, and other computer networks that share the set of protocols specified by the Internet Architecture Board (IAB) and the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).
(22) IT System: a collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage,

manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected.

(23) Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices thatinteract with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

(24) Protected System: shall means any computer, computer system or computer network of any organization notified under section 70 of the Act, in the official gazette by appropriate Government.

(25) Responsible Entities: shall mean power sector entities deploying Operational Technologies with or without IT systems, including Generating companies including the captive plants,Renewable Energy Sources, Energy Storage System, Transmission Licensees including deemed transmission licensee, Distribution Licensees, National Load Dispatch Centre, Regional Load Dispatch Centers, State Load Dispatch Centers, Control Centers of distribution licensee, Central Transmission Utility, State Transmission Utilities, and Renewable Energy Management Centers, forecasting service provider, Traders, Power Exchanges, Qualified Coordinating Agencies.

(26) Software Bill of Materials: a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercialsoftware components. The SBOM enumerates these components in a product.

(27) Vulnerability: weakness of an asset or control that can be exploited by one or more threats.

(28) Vulnerability Assessment: shall mean a process of identifyingand quantifying vulnerabilities.

(29) Vendors: Vendor includes Original Equipment Manufacturer, Original Equipment Suppliers, System Integrator, Associated Hardware/ Software Component Suppliers, and Service Providers.

2 (b) Words and expressions used and not defined in these regulations but defined in the Information Technology Act, 2000 and the Electricity Act, 2003 shall have their respective meanings assigned to them in the respective Acts.

## Chapter-II

## CSIRT-Power

3. Computer Security Incident Response Team (CSIRT)-Power as may be established under CEA, shall collect traffic data, generated, transmitted, or stored in computer resources of all Responsible Entities in power sector, to enhance cyber security and for identification, analysis and prevention of cyber intrusion or spreadof computer contaminant or any other work, as directed by the Authority through a separate order.
4. CSIRT-Power shall have roles and responsibilities including the followings-(1)

laying down the Cyber Security framework and protocol for the Power Sector.
(2) serve as a Point of Contact and Responsible Agency of the Power Sector for responding to and prevention of cyber security incidentsin the Power Sector.
(3) reviewing the Cyber Security arrangements in the different wings from time to time and strengthening such arrangements.
(4) Coordinate, share, collect, analyse cyber threats related to Power Sector.
(5) Create/develop Standard Operating Procedures (SOPs), security policies, best practices for incident Response activities in consultation with CERT-In and NCIIPC.
(6) Issue, Analysis, follow-up action on Alert and Advisories in coordination with NCIIPC, CERT-In and MHA.
(7) Implement Cyber Crisis Management Plan for the Power Sectorin coordination with CERT-In
(8) Collaboration with CERT-In and NCIIPC to resolve the CyberSecurity incidents.
(9) Proactive measures to increase the cyber security awareness and improving the cyber security posture of the Power Sector including audits, assessments and exercises.
(10) Work closely with CERT-In and active participation in all cyber security related activities & initiatives suitable to the Power Sector
(11) Facilitate and promote research & development in relevant subject domain pertaining to cyber security in collaboration with Research Institutes and Academia.
(12) Implementation of Scheme of Trusted Vendor System for PowerSector as and when notified.
(13) Security Control Selection & Tailoring Process for Power Sector
(14) Any other functions related to cyber security issues as directedby Ministry of Power, the Authority, CERT-In and NCIIPC.

5. The Authority may also designate sub sectoral CERTS in Power Sector for Generation, Transmission, Distribution, Grid Operation toassist CSIRT-Power in hierarchical structure and shall carry out functions, as directed by the Authority through a separate order.
6. The directions of CSIRT-Power shall be complied with, and if askedfor, documents related to Cyber Security shall be submitted.

## Chapter-III

## General Cyber Security Requirements

### Applicable to all Entities listed under Regulation 1(3).

7. The Entity shall

(1) designate regular employees of the senior management level as CISO and alternate CISO who shall be Indian nationals (by birth) and define their roles and responsibilities, ensuring that the role of the CISO is ring fenced to tasks of Cyber Security. The designated CISO shall report to the CEO/Head of the Responsible Entity. In absence of CISO, the roles and responsibilities of CISO shall be executed byAlternate CISO.
Provided that both the posts of CISO and Alternate CISO do notremain vacant at

the same time.

(2) have a defined, documented and maintained Cyber Security Policy which is approved by the Board or Head of the entity as a casemay be.

(3) Have a Cyber Crisis Management Plan (CCMP) which is approvedby the Board or Head of the entity as a case may be.

(4) ensure deployment of all required security devices, such as appropriate firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) capable of identifying behavioural anomaly, including deployment of Web Application Firewall for the protectionof critical web-based applications.

(5) ensure that all websites, web portals, applications, and web services as well as any update undergo and successfully pass a cyber security audit before being hosted on the Internet.

(6) ensure that a comprehensive cyber risk assessment isconducted, and effective measures for identified cyber risks are implemented before grant of approval for remote access to cyber assets.

Provided that, such remote access shall be limited to the minimum necessary duration, with least privilege, ensuring multi-factorauthentication to verify the identity of remote users.

(7) conduct periodically, Cyber Security awareness program and Cyber Security exercises including mock drills and Tabletop exercises.

(8) ensure that all engaged personnel sign an undertaking, includinga non-disclosure agreement, to protect the confidentiality, integrity, and availability of sensitive information and implement an enquiry process to investigate an event of Cyber Security breach.

Provided that disciplinary process shall be implemented to act against personnel committing a Cyber Security breach.

(9) report Cyber Security incidents within prescribed time limits to CSIRT-Power along with CERT-In and NCIIPC.

(10) ensure online and offline backups of all critical and other required systems as stated in their Cyber Security policy, in separate and secure environments.

(11) facilitate a comprehensive Cyber Security audit

(A) for the IT system twice a year, the first audit period between April and September, and the second audit period between October and March with a gap of atleast four months between these two audits.

(B) once a year for the OT system, as applicable.

## Chapter-IV

## Roles and Responsibilities of Responsible Entities

8. Responsible Entities shall(1) establish an Information Security Division (ISD) dedicated to ensuring Cyber Security, headed by the CISO and remain operational round the clock. Sufficient workforce and infrastructure support shall be ensured for ISD.

(2) acquire ISO/IEC 27001 certificate by certification bodies, preferably accredited by the Indian Accreditation Body or acquire Basic Technical Criteria certificate as and when issued by the Authority through a separate order.

(3) ensure that all personnel engaged in the operation and maintenance of IT & OT systems, including personnel from Contractors and Vendors, have mandatorily undergone designated Cyber Security courses from training

institutes as directed by the Authority through a separate order.

Provided that CISO and members of the ISD shall attend CyberSecurity training program for at least ten person-days per year oras may be directed by separate order by the authority to upgradethe necessary competencies.

(4) ensure the availability of essential communications withrequired internal & external stakeholders for management of crisis, natural disasters, or other emergencies.

(5) ensure deployment of all required security devices, such asappropriate firewalls, IDS, IPS capable of identifying behaviouralanomaly in both IT and OT environment as applicable, including deployment of Web Application Firewall for the protection of critical web-based applications.

Provided that Responsible Entity shall ensure deployment of suitable perimeter Cyber Security devices such as appropriate Firewall with hardened configuration at their point of connection with power system.

(6) ensure that control and operation of power system elements are prohibited over Internet.

Provided that power system elements are controlled and managed from within national boundaries only, and real-time data of grid operations and status information is not transferred across the border.

(7) ensure that its Critical Information Infrastructure is not discoverable on public platforms unless permissible in Cyber Security policy case to case basis.

(8) ensure physical isolation of critical OT system from Internet.

(9) 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 separated from other/rest of IT networks.

(10) in case remote operation is required, ensure the implementation of a secure architecture that includes deploymentof next-generation firewalls with hardened configurations, andhaving IDS/IPS, to protect against unauthorized operations. Provided that, these systems are connected with secure, encrypted,and dedicated communication channels isolated from internet traffic and shall be monitored continuously.

(11) ensure that no equipment, component, software or applicationis deployed in the production environment without successfultesting and is verified before being used in the power system. Provided that the Responsible Entity shall ensure the testing of allequipment, components, and parts imported for use in the PowerSupply System and Network for any kind of embedded malware,Trojan, or cyber threat and for adherence to Indian Standards in compliance with the orders issued by the Ministry of Power fromtime to time in this regard.

(12) ensure that as and when Ministry of Power, Government ofIndia stipulates the Model Contractual Clauses on cyber security,the applicable clauses are included in their procurement bid invited for of all ICT based components/equipment/systems as well as services

(13) ensure that as and when Ministry of Power, Government ofIndia stipulates the Scheme of Trusted Sources in power sector, all the designated ICT based Equipment and Services are sourced from listed Trusted Sources only.

# Chapter –V

## Functions and Responsibilities of Information Security Division (ISD)

9. ISD shall be manned by sufficient numbers of officers, having validcertificate of successful completion of domain specific Cyber Security courses.

The indicative minimum manpower of ISD is given in Part-I of theSchedule I.

10. ISD shall carry out the Functions of including the following

(1) to implement measures for Cyber Security of the Critical Information Infrastructures (CIIs) as identified by NCIIPC and the notified Protected Systems by appropriate Government as per IT Act, 2000.
(2) to review the Cyber Security Policy of the Responsible Entity annually and its compliance measures on a quarterly basis.
Provided that such a review shall include items as given in Part-II of Schedule I.
(3) to test randomly, the day-to-day operations of Critical System for being in conformance with Cyber Security Policy and advisories, guidelines and directive issued by NCIIPC, CERT-In, CSIRT-Power and take required actions.
(4) to act upon the directive, guidelines, and advisories issued by NCIIPC, CERT-In, CSIRT-Power and the Authority.
(5) to share the details of the detected cyber security incidents,Action Taken Reports, Root Cause Analysis and other incident related reports with CSIRT-Power along with CERT-In and NCIIPC.
(6) to gather cyber threat intelligence, identification of threat vectors and evaluation for Cyber Security risks including internal risks and external risks by analyzing Cyber Security logs, alerts and events.
(7) to maintain an updated inventory of all IT and OT assets, including hardware assets, software assets, and other associated assets, and a record of documented network architecture depicting data flows.
(8) to identify and select Cyber Security control measures that commensurate with the criticality of Cyber Security risks.
(9) to implement process to receive, analyze and respond to disclosed vulnerabilities from internal and external sources.
(10) to implement mechanism for timely identifying, assessing and managing Cyber Security threat and vulnerabilities.
(11) to retain Cyber Security documents like certificates of Cyber Security tests, FAT, SAT results, and Cyber Security Audit reports for the period as directed by the Authority through a separate order.
(12) to report cyber sabotage in the Critical System to CSIRT-Power within 24 hours of detection or within period as directed by the Authority through separate order.

11. ISD shall ensure the followings, across its Responsible Entity: -

(1) the updation of the firmware/software with the digitally signed OEM validated patches only.
(2) cyber security hardening of deployed security devices, networkdevices,

host devices etc.,

(3) the enforcement of strict and approved protocol for grant ofremote access as laid in their Cyber Security Policy.

(4) the storage of logs of all of their ICT systems for a rolling period of 180 days or for a period as directed by the Authority through a separate order.

(5) secured preservation of logs and forensic records pertaining to Cyber Security incidents for at least 180 days or for a period as directed by the Authority through a separate order.

(6) identification and documentation of cyber asset wisevulnerabilities, as and when known, discovered, or disclosed publicly by the OEM/third party.

(7) that the Cyber Security requirements are included in the FAT and SAT requirements during the procurement of equipment/ components/ parts.

(8) updated record of Configuration details of Critical System is maintained.

(9) that the clocks of all relevant information processing systems within IT and OT systems are synchronized to a reference time source.

(10) inclusion of Cyber Security requirements in Service Level Agreement (SLA) with Cloud Service Provider following applicablegovernment guidelines, rules, and regulations and inclusion of withthe approved.

(11) storage of Cyber Security-related documents and records in secure and controlled environments, with access restricted to authorized personnel only.

(12) on-boarding of required information including allocated, used and unused public IPs with Threat Detection Portals of cyber security agencies.

(13) that all OT equipment/systems supplied by the successful bidder are accompanied by a certificate obtained by the vendor from acertification body for conformance to IEC 62443-4 standards.

# Chapter-VI

## Chief information Security Officer (CISO) and Alternate CISO

12. CISO & Alternate CISO shall possess a degree in Engineering with at least fifteen years of experience in power sector domain or 10 years of experience in IT/Cyber Security.

Provided that they conform to other required qualifications, as and when, issued by the Authority through a separate order. The CISOs shall acquire these qualifications within six months of their issuance or within a period as may be directed by the Authority through a separate order.

13. The CISO shall be the nodal officer for all cyber security related issues, coordination with the authorities/ agencies handling Cyber Security subject matters including handling of all communicationsrelated to CCMP.
14. The details of the CISO and alternate CISO shall be communicatedto CSIRT-Power and to all internal and external stakeholders of organizations, including publication on the website.
15. The CISO shall be the custodian of all the cyber security relateddocuments as specified in IS 16335.

# Chapter-VII

# Cyber Security Policy

16. **Cyber Security Policy shall include**

(1) defined Purpose, Scope, roles and responsibilities of their internal and external stakeholders. It shall contain applicable compliance and legal requirements including review schedule, Monitoringmechanisms and reporting metrics.

(2) asset management processes including asset identification and classification process.

(3) defined Cyber Risk Assessment and Risk Treatment Plan, with an approved risk matrix and risk acceptance criteria for both IT and OT environment. The same shall be approved by the Board of Directorsof the Entity.

Provided that Cyber risk assessment shall be conducted annually and shall consider but not limited to, all cyber assets identified/notified as Critical Information Infrastructure/Protected Systems, critical and high-risk cyber assets as identified in the Cyber Security risk assessment and risk treatment plan.

(4) defined policy for Personnel Risk Assessment, which shall include the process and controls to mitigate risks from Personnel after their termination from employment or upon change of their job responsibilities

(5) Vulnerability Management Process for periodic identification and closure of vulnerabilities,

(6) defined Access Control for user Access Management including Authentication and Authorization for granting access.

(7) defined physical Access controls defining rules for physical access to critical cyber assets and mechanisms for protecting against environmental threats.

(8) designed and documented annual cyber security training program for personnel having authorized cyber or authorized physical access to their Critical Systems.

(9) defined and documented Change Management process to ensure that all changes in software and/or update shall be version controlled with roll-back provision.

Provided that, there shall be defined and documented patch management procedures that shall include the identification, categorization, and prioritization of security patches, and the time frame for application and process to check and verify the authenticity, integrity, and compatibility of security patches and system updates shall be defined.

(10) defined backup policy to ensure that all backup data is being retained at least for the period of one calendar year or as directed bythe Authority through a separate order. Backup policy shall havemechanism for verification and testing of the integrity of all the backup data as well as the restoration processes.

Provided that Backup of all sensitive data shall be encrypted duringboth transmission as well as storage. Access of such backup data shall be secured and restricted to authorized personnel only.

(11) defined and documented, risk-based Cyber Security Incident Response and Recovery Plan for effective response and the timely restoration of systems.

(12) defined and documented digital Data Protection and PrivacyPolicy in line with notified Government Rules and Regulations, which shall include encryption for sensitive data when data is at rest on the device or on a removable media or in

transit.

Provided that sensitive data, such as Personally Identifiable Information (PII), stored on or sent to or transmitted fromtelecommuting devices shall be protected from unauthorized accessor corruption.

(13) provisions for secured use of external removable and mobile devices including restriction on the use of Bring Your own Device (BYOD) within critical & associated networks.

(14) defined and documented Internet Access Policy to monitor and regulate the use of internet.

(15) management and phase out plan for obsolete cyber asset, thatare already outlived their useful life or nearing the end of their usefullife.

Provided that documented Standard Operating Procedure (SOP) forthe safe and secure disposal of obsolete system shall be in place.

(16) Process for vulnerability scanning and penetration testing priorto the commissioning of any system in case of replacement obsolete system.

(17) password Policy that includes strong Password controls for authorized access to systems, applications, networks and databases.

(18) plan for collaboration with other industry stakeholders and academia to promote R&D activities in the domain of Cyber Security.

(19) plan for Cyber Supply Chain Risk Management that includes provision of Cyber Security requirements in outsourcing and Non-Disclosure Agreement in the Service Level Agreement.

(20) procedure for identifying and reporting of sabotage in CriticalSystem.

## Chapter-VIII

### Cyber Crisis Management Plan (CCMP)

17. CCMP shall include cyber event categorization, criteria(s) for identifying event as crisis, identified stakeholders and their responsibilities, Standard Operating Procedure to manage the cybercrisis and Communication methodologies during crisis with impacted parties, internal/ external stakeholders, and key users.
18. CCMP shall be prepared in consultation with concerned Sectoral- CERTS and vetted by CERT-In, the vetted CCMP shall be approvedby their Board of Directors and reviewed annually, or after any major change, whichever is earlier.
19. In the CCMP, Recovery Plan(s) for every Critical System shall be defined and documented and same shall be communicated to allconcerned Personnel.
20. CISO shall be responsible for ensuring implementation of CCMP.

## Chapter-IX

### Additional Cybersecurity Requirements for Vendor

21. The vendor shall provide documented and tested procedures andrecovery plan for restoration of the system from potential cyber crisis scenarios.
22. The vendor shall ensure that the security patches and updates aremade available for all system components, supplied by them throughout the entire contractually stipulated operating time.

Provided that, where the vendor has not provided entire systems, it shall indicate the necessary requirements and process to install security patches and other

updates on the third-party components, if integrated in the system.

23. The vendor shall inform the End of Support/ End of life of all hardware/ software/ system, including those of third parties, supplied by them.
24. The vendor shall provide Software Bill of Materials stating detailedlist of used software components in case of Critical Applications, supplied by them.

## Chapter-X

### Cyber Security Audit

25. The Cyber Security audit shall be conducted through a CERT-In empaneled Cyber Security Auditor or cyber security auditor as per NCIIPC scheme as and when the same comes into existence. TheseCyber Security audits shall be carried out as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335, ISO/IEC 27017 and any other Cyber Security audit directions issued by the Authority.
26. The Cyber Security audit and their compliance report shall be reviewed by CISO. Critical vulnerabilities and major non- compliances identified in critical information infrastructure during internal and external cyber audits shall be presented to the Board ofDirectors.
27. The audit report shall be submitted within 6 weeks of itscommencement and within the same audit period.

Provided that all critical and high-risk vulnerabilities shall be addressed within a period of one month and medium & low risks vulnerabilities before the commencement of the next audit.

Further, provided that effective closure of all identified vulnerabilities shall be verified during the conduct of next audit.

28. No three consecutive Cyber Security audits shall be done by thesame Auditing Agency and in the case of certification audit, the third audit shall be done by a different group of Auditors.

## Chapter-XI

### Physical Security

29. All cyber and non-cyber critical assets shall be identified and protected and all access points to the Critical System shall be secured physically and monitored by employing physical, human, and procedural controls such as the use of Security Guards, CCTVs,Biometric, card access systems, mantraps, bollards, etc. whicheverappropriate.
30. Physical access to OT and Industrial Control System (ICS) Systemsshall be restricted.

Provided that the grant of physical access to the Critical Systems shall be revoked in case of a perceptible threat of physical damage.

31. The Systems, Networks, Applications used for ensuring effective physical security shall be kept separated from the network of critical systems.

## Chapter-XII

## Critical Information Infrastructure (CIIs) Identification

32. For the identification of CIIs, all information required by NCIIPC shallbe provided.

Provided that Upon receipt of the communication regarding declaration of CIIs from NCIIPC, the organization shall, within 15 calendar days, approach the appropriate government for notification of their declared CIIs as "Protected Systems" in the Official Gazette, in accordance with the provisions of Section 70 of ITAA 2008.

33. Details of new cyber assets shall be submitted to NCIIPC, within 30 days of their commissioning.

## Chapter-XIII

## Miscellaneous

34. **Monitoring and Compliance**

(1) Assessment of Compliances

The performance of all organizations with respect to compliancewith these regulations shall be assessed periodically.

(2) Monitoring of Compliance

(1) In order to ensure compliance, two methodologies shall befollowed:
(a) Self-Audit
(b) Compliance Audit

(2) Self Audit:
(a) All organizations shall conduct annual self-audits to review compliance of these regulations and submit the reports by 31stMarch of every year.
(b) The self-audit report shall inter alia contain the followinginformation with respect to non-compliance:
(i) Sufficient information to understand how and why the non-compliance occurred.
(ii) Extent of damage caused by such non-compliance.
(iii) Steps and timeline planned to rectify the same.
(iv) Steps taken to mitigate any future recurrence.

(c) The self-audit reports by all Responsible Entity, associated Government Organizations (CPRI, PFC, REC, BEE, Training Institutes), and Vendors shall be submitted to the CISO-MoP andCSIRT-Power.

(d) The self-audit reports of Power Sector IT Infrastructure of Appropriate Government, RPCs, Appropriate Commissions shallbe submitted to CISO, MoP.

(e) The deficiencies shall be rectified in a time-bound manner within a reasonable time.

(f) CISO, MoP shall continuously monitor the instances of non- compliance of the provisions of these regulations and endeavor to sort out all operational issues and deliberate on the ways in which such cases of non-compliance shall be prevented in future.

(g) CISO, MoP may initiate appropriate proceedings upon receiptof the report under sub-clauses (e) of this clause.

Provided that CISO, MoP may report the non-compliance of any regulations to CERT-In and NCIIPC for appropriate action under IT Act 2000 and Amendment thereof.

Furthermore, provided that CISO, MoP may initiate action for non-compliance of these regulations under section 146 of theElectricity Act, 2003.

(h) In case of non-compliance with any provisions of these regulations, the matter may be reported by any person to theCISO-MoP or the Authority.

(3) Independent Third-Party Compliance Audit:
CISO, MoP or the Authority may order independent third-party compliance audit for any organization as deemed necessary based on the facts brought to the knowledge of CISO, MoP or theAuthority.

35. **Power to Relax**

The Authority through an order, for reasons to be recorded inwriting, may relax any of the provisions of these regulations on its own motion or on an application made before it by an affected person to remove the hardship arising out of the operation of anyof these regulations, applicable to a class of persons.

36. **Power to Remove Difficulty**

If any difficulty arises in giving effect to the provisions of these regulations, the Authority may, on its own motion or on an application made before it by the affected person, by order, make such provisions not inconsistent with the provisions of the Act or provisions of other regulations specified by the Authority, as may appear to be necessary for removing the difficulty in giving effectto the objectives of these regulations.

**Schedule-I**

**Part-I: Indicative minimum required officers/officials in ISD.**

1. Minimum Work Force required for setting up an ISD:
    a. 04 (Four) officers including CISO and 04 officers/officialsfor shift operations.
    b. Besides these indicated officers/ officials additional officers/officials can be placed exclusively for cyber security task like conducting Internal Cyber Security Audit, Mock-Drills/ Exercise, VAPT, coordination, and execution of tasks related tocompliance of cyber security Guidelines, Regulations, advisory and alerts etc.2. The officers/officials deployed in the ISD shall have valid certificate of successful completion of Cyber Security courses as issued by the Authority through a separateorder. The officers/officials shall acquire these certificates within six months of their issuance or within a period as may be directed by the Authority through a separate order.

**Part II - The review of the Cyber Security policy implementationmust include:**

i. Review of current cyber security capabilities including capabilities of cyber security deployed Cyber Security tools and implemented Cyber Security processes and procedures.
ii. To Review the efficacy of cyber security preparedness.
iii. Review of goals set for a targeted level of cyber resilience.
iv. Review of Incident response plan to improve upon cyber resiliencelevel and strengthening of cyber security incident handling capabilities.
v. Review of measures for improvement in Cyber Security posture.

**Part III - Guidance on Awareness Programs**.

Personnel having authorized cyber or physical (escorted or unescorted)access, must receive on-going reinforcement on cyber security best practices. The cyber security best practices dissemination may be done through mechanisms such as:

i. Direct communications (e.g., emails, memos, computer-basedtraining, etc.).
ii. Indirect communications (e.g., posters, intranet, brochures, etc.).
iii. Management support and reinforcement (e.g., presentations,meetings, etc.).