GOVERNMENT OF INDIA
CENTRAL ELECTRICITY AUTHORITY
Sewa Bhawan (North Wing), Room No. 622, 6th Floor,
R. K. Puram, New Delhi-110066
Tel. 011-26732632, email: celegal-cea@gov.in
Website: www.cea.nic.in

PUBLIC NOTICE

In exercise of powers conferred under Section 177 of the Electricity Act, 2003, the Central Electricity Authority (CEA), proposes to notify the following regulations:

1. **Draft Central Electricity Authority (Technical Standards for Construction of Electrical Plants and Electric Lines) (2nd Amendment) Regulations, 2025**

2. **Draft Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2025.**

The proposed drafts of both the regulations are available on the CEA Website **www.cea.nic.in** for inviting public comments. All the Stakeholders and 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 **07.11.2025.**

(Rakesh Kumar)
Secretary, CEA

[redacted]

NOTIFICATION

No. In exercise of the powers conferred by sub-section (1) of 177 read with sub-section (c) of 73 of the Electricity Act, 2003 (No. 36 of 2003), the Central Electricity Authority hereby makes the following regulations for Measures relating to Cyber Security in Power Sector, namely: -

Chapter-I
Scope and Definitions

1. **Short title and Commencement -** (1) These regulations may be called the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2025.

   (2) They shall come into force six (6) calendar months from the date of their publication in the Official Gazette.

   Provided that the Regulations 8(2), 8(17), 8(26), 8(32), 9(2) and 9(7) shall come into force on such dates, as may be specified by the Authority through separate orders.

2. **Scope and Extent of Applicability -** (1) These Regulations shall apply to:
   (a) all the Entities, which own, operate, or manage Operational Technology (OT) infrastructure associated with the Power System and their Information Technology (IT) infrastructure that is physically or logically connected to such OT infrastructure, for their existing as well as upcoming infrastructure.
   (b) Power Exchanges and Over the Counter Platforms, except Regulations 9, 16 and 17

   (2) Vendor shall comply with the Regulation 16 and Regulation 17 of these regulations, as applicable.

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

   (1) **Act:** means the Electricity Act, 2003 and amendment(s) thereof

   (2) **Business Continuity Plan:** means documented procedures that guide an organization to maintain a defined level of continued business operations

   (3) **Chief Information Security Officer:** means the designated employee of senior management level of an Entity, having knowledge of cyber security and matters related thereof, responsible for cyber security efforts and initiatives.

   (4) **CISO – MoP:** means Chief Information Security Officer of Ministry of Power designated by the Government of India.

   (5) **Computer Security Incident Response Team - Power**: means an organization established by the Ministry of Power as an extended arm of Indian Computer Emergency Response Team (CERT-In) for coordinating, reporting and responding to cyber security incidents in power sector.

   (6) **Critical IT System:** means Information Technology (IT) system(s) of an organization whose unavailability or degradation would adversely impact its business operations.

   (7) **Critical OT System:** means Operational Technology (OT) system(s) of an organization whose unavailability or degradation would adversely impact its business operations.

   (8) **Critical System:** means critical Operational Technology (OT) system(s) or critical IT system(s) or both, including Critical Information Infrastructure, as applicable, of an

entity

(9) **Critical Information Infrastructure:** means Critical Information Infrastructure as defined in explanation of sub-section (1) of Section 70 of the IT Act, 2000

(10) **Cyber Asset:** means the programmable electronic device(s), with or without computing capabilities, including its hardware, software, sub-components and data thereof that are connected over a network.

(11) **Cyber Asset Register:** means a record that contain list of all cyber assets and description thereof.

(12) **Cyber Crisis Management Plan:** means cyber crisis management plan as defined in section 2(1) of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

(13) **Cyber Resilience:** means the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber asset(s).

(14) **Cyber Security Audit :** means an audit to assess the cyber security posture, by a CERT-In empaneled auditor or any other auditor as may be designated by the Ministry of Power, Government of India through a separate order.

(15) **Cyber Security Breach:** means cyber security breach as defined in section 2(l) of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

(16) **Cyber Security Incident:** means cyber security incident as defined in section 2(l) of the IT Rules, 2013.

(17) **Cyber Security Policy:** means documented set of rules, procedure and processes for protecting information, computer resources, networks, devices, Industrial Control Systems and Operational Technology resources and to improve the cyber security posture thereof.

(18) **Cyber Sabotage:** means deliberate action(s) to disrupt, damage or destroy the information systems, networks, or data processed therein, for malicious purpose(s).

(19) **Distributed Generation Resource**: means a generating station feeding electricity into the electricity system at voltage level of below 33 kV, and includes grid-connected rooftop solar systems.

(20) **Electronic Security Perimeter:** means the logical border surrounding IT system(s) or OT system(s) or both that are electronically connected, within which the access is monitored and controlled for protection of such system(s).

(21) **Entity** : means Generating Companies including Captive Generating Plants, and Renewable Energy Generating Companies; organization deploying or operating Energy Storage System(s); Transmission Licensees; Distribution Licensees; National Load Dispatch Centre (NLDC); Regional Load Dispatch Centers (RLDCs); State Load Dispatch Centers (SLDCs); Renewable Energy Management Centers (REMCs), Power Exchanges and Over The Counter (OTC) platform.

(22) **Factory Acceptance Test :** means inspection and static or dynamic testing of equipment or major component(s) thereof conducted and documented at supplier's site or facility to establish the specified qualification(s) of an equipment or system.

(23) **IT System** : means the Information Technology system consisting of user endpoints, network resources, applications, servers and communication components deployed therein and having a physical or logical connection with the Operational Technology infrastructure.

(24) **Obsolete Asset**: means an asset declared by Original Equipment Manufacturer (OEM) or Original Equipment Supplier (OES), whose production and services are discontinued and its support is no longer available, and that asset is not suitable for its

intended purpose due to technological advancement, operational changes and may pose security or operational risk.

(25) **Operational Technology (OT)**: means programmable hardware or system that detects or cause changes through the direct monitoring or control of physical devices, processes and events.

(26) **Protected System**: means Protected System as defined in section 2(l) of the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

(27) **Remote Access**: means an access to any cyber asset of an organization through an external network.

(28) **Remote Operation** : means operation and control of OT system(s) of an Entity performed from a distant location of such OT system(s)

(29) **Self Audit** : means an audit by an entity in a financial year to assess its compliance with all applicable regulations specified in these regulations

(30) **Sensitive Information**: means the data or information that if disclosed, modified, or destroyed could negatively impact the privacy, integrity, security or operations of an organization or an individual.

(31) **Site Acceptance Test** : means testing conducted at the site of installation to verify that a system or equipment operates as intended in its final operational environment.

(32) **Software Bill of Materials**: means a formal record containing details and supply chain relationships of various components used in software.

(33) **Sub-sectoral Computer Security Incident Response Team** : means an entity designated by the Authority to assist Computer Security Incident Response Team (CSIRT) – Power in cyber security related matters.

(34) **Technical Criteria Certificate:** means a certificate issued to an organization by a designated certification body, accredited for, ensuring conformance to cyber security standards specified by the Government of India.

(35) **Threat**: means any circumstance or event having the potential to exploit a deficiency and negatively impact the confidentiality, integrity or availability of a cyber asset or IT system or OT system.

(36) **Vulnerability**: means vulnerability as defined in section 2(l) of the IT Rules, 2013.

(37) **Vendor**: means Original Equipment Manufacturer, Original Equipment Supplier, System Integrator, supplier of hardware or software associated with original equipment, contractor or service provider, including cloud service provider, and system integrator of Distributed Generation Resource owned by prosumer

(b) Words and expressions used but not defined in these regulations shall have their respective meanings assigned to them in the Act, Rules and Regulations made thereunder.

Chapter – II

Computer Security Incident Response Team (CSIRT) – Power

4. Computer Security Incident Response Team (CSIRT) – Power shall
   (1) be the coordinating agency for reporting and responding to cyber security incidents associated with power sector
   (2) be the nodal agency of power sector for analysis, prediction and prevention of cyber security incidents and dissemination of information thereof
   (3) collect data and information pertaining to any cyber security incident from an entity, including network architecture, details of assets, logs, cyber forensic records, forensic image, policies and procedures, any other relevant information

रविंदर 01/10/2025

in the form, manner and mode as specified by it.

Provided that sensitive data as well as sensitive information collected shall be protected against breaches and not be disclosed to any third party without explicit communication to the concerned entity.

5. The roles and responsibilities of CSIRT – Power, inter alia, include the following:
   (1) Collect and analyze cyber incidents, vulnerabilities and threats related to power sector
   (2) Predict cyber security incidents, threats and vulnerabilities related to power sector
   (3) Coordinate and collaborate with CERT – In, National Critical Information Infrastructure Protection Center (NCIIPC) and other agencies designated by the Government of India in the area of cyber security, to resolve the cyber security incidents related to power sector.
   (4) Issue alerts, advisories and guidelines in coordination with NCIIPC, CERT – In and any other agencies designated by the Government of India in the area of cyber security
   (5) Create or develop Standard Operating Procedures (SOPs), security policies, sub-sector specific benchmarks, security controls and best practices for incident response activities in consultation with CERT – In, NCIIPC, sub-sectoral CSIRTs, Electricity Regulatory Commissions and other agencies designated by the Government of India in the area of cyber security.
   (6) Proactive measures to increase the cyber security awareness through capacity building initiatives and interventions
   (7) Ensure the improvement of cyber security posture of the power sector by cyber security assessments, cyber security audits, certification audits, self-audits, third party audits and exercises, including mock-drills and simulations
   (8) Coordinate for laying down the sub-sector specific cyber security framework, protocols and rules
   (9) Advise the utilities in preparation of their Cyber Crisis Management Plan (CCMP) and assist them in getting their CCMP vetted by CERT – In.
   (10) Ensure that the entity tests and verifies the efficacy of their CCMP through scenario-based mock-drills
   (11) Coordinate with entity for ensuring the implementation of their CCMP during actual cyber crisis.
   (12) Facilitate and promote Research & Development (R & D) in the domain of cyber security through collaboration with Industry, Research Institutes and Academia.
   (13) Formulation and implementation of measures to ensure cyber security of supply chain of cyber assets specified by the Government of India or the Authority
   (14) Any other functions associated with cyber security related matters as directed by the Government of India or the Authority.

6. The directions of CSIRT – Power, in the matters related to cyber security of power sector, shall be complied with.
7. The Authority through a separate order may designate sub-sectoral CSIRTs in power sector for Generation, Transmission, Distribution, Grid Operation and any other sub-sector, along with their roles and responsibilities, to assist CSIRT – Power.

Chapter – III
General Cyber Security Requirements

8. The entity shall

(1) designate regular employees of the senior management as Chief Information Security Officer (CISO) and alternate CISO. Further, the entity shall

a) ensure that both the positions of CISO and alternate CISO shall not remain vacant at the same time

b) define roles and responsibilities of CISO and alternate CISO in accordance with the Government of India's regulatory framework and relevant guidelines.

c) ensure that the CISO reports to the head of the entity
Provided that in case, the State Load Dispatch Centre (SLDC) is not an independent entity, but part of a holding company or parent company, such SLDC shall have a separate CISO, who shall report to head of such holding company or parent company, as applicable and shall also have Alternate CISO

d) ensure an employee is designated as CISO, for a minimum period of three (3) years

e) role of the CISO is ring fenced to the tasks of cyber security related matters only.

f) provide contact details of the CISO and alternate CISO and updation thereof in public domain and communicate such details to CSIRT – Power as well as all internal and external stakeholders.

g) ensure CISO attends cyber security training courses for at least five (5) days in each financial year

(2) establish a dedicated Information Security Division (ISD) headed by CISO, within India, for dealing with all cyber security related matters and the same shall remain operational round the clock. Further,

a) the ISD shall be deployed with sufficient manpower
The indicative minimum manpower of ISD is given in Schedule – I.

b) the manpower deployed in ISD shall have valid certificate(s) of successful completion of domain specific cyber security course(s).

c) the manpower deployed in ISD shall attend cyber security training courses associated with Power Sector for at least five (5) man days in each financial year.

d) the manpower shall be deployed in ISD for a minimum tenure of three (3) years.

(3) have a defined and documented Cyber Security Policy (CSP), which is approved and reviewed annually by the head or board of the entity, as the case may be.

(4) prepare a Cyber Crisis Management Plan (CCMP) in consultation with CSIRT – Power, to manage and recover from all possible cyber crisis situations in shortest possible time with minimum impact on business operations.
Provided that the CCMP shall be vetted by CERT – In and approved by the head or board of the entity, as the case may be, prior to its implementation and reviewed at least once (1) in every year.

(5) ensure separation of IT networks containing Critical Information Infrastructure (CII) from internet as well as rest of the IT networks.
Provided that in case internet is required for IT networks containing CIIs, the same shall be sourced securely with suitable hardening measures as specified by designated agencies of the Government of India.

(6) ensure deployment of all required security devices, including firewalls at Electronic Security Perimeter (ESP), such that the deployed security system meets the requirements of, inter-alia, packet filtering; deep packet inspection; content, user and application based filtering; detection and inspection of encrypted traffic; intrusion detection and prevention; geo-fencing; facility for automatic signature and behavior updates; user controlled updates; detection, inspection and filtering based on signature and behavioral anomalies.

(7) ensure that any web service or web-based application including website, web portal, and Application Programming Interfaces (APIs), having public access, shall be deployed only after cyber security audit clearance.

Provided that any software update, including patch, in web applications and web services shall be deployed only after successful testing and confirmation by vendor such that the subject update is free from any cyber security vulnerability; and risk assessment by entity and after ensuring that such update is free from any cyber risk.

Provided that any software update qualified for prior requirement of cyber security audit, as specified in CSP, shall be deployed only after its cyber security audit clearance.

Provided that all software updates, those not necessitated for prior cyber security audit, shall be assessed during next cyber security audit.

(8) ensure deployment of all required security devices, including Web Application Firewall (WAF), such that the deployed security system for all critical web applications, identified as per the procedure detailed under CSP, meets the requirements of, inter alia, detection and filtering of web based encrypted traffic; ensuring bidirectional protection; facility for automatic signature and behavioral updates; intrusion detection and prevention, user controlled system updates; content, user and application based filtering; geo-fencing; detection, inspection and filtering of encrypted traffic based on signature and behavioral anomalies.

(9) identify and segregate systems as critical and non – critical systems, as per the procedure detailed in CSP

(10) ensure that remote access to cyber assets, if necessary, may be permitted only for troubleshooting and emergency requirements, as per the procedure specified under CSP.

Provided that such access for the cyber assets associated with non – critical system(s), may be permitted with approval of CISO, for troubleshooting and emergency requirements only, along with suitable security control measures.

Provided that approval for such access to critical systems or cyber assets thereof may be granted after a comprehensive risk assessment is conducted along with identification of effective measures thereof and such access shall be continuously monitored to detect any anomaly or unauthorized attempts

Provided that record of risk assessment, physical document of approval and logs w.r.t. each such access to critical system shall be maintained for a period as specified in data retention policy.

(11) conduct cyber security awareness program and cyber security exercises including mock-drills and tabletop exercises, at least once (1) in every six (6) months.

(12) ensure that sensitive information and sensitive data, including such data and information hosted on cloud, is stored in an encrypted, secured and protected environment and resides within India only.

(13) include all cyber security requirements as well as applicable cyber security rules,

regulations issued by the Government of India and Non – Disclosure Agreement (NDA) in Service Level Agreement (SLA) with the vendor(s), as specified under CSP, to ensure the confidentiality, integrity and availability of sensitive information, during their contract period as well as after completion of such contract period.
Provided that vendor(s) having cyber or physical access or both to the critical systems, including manpower of vendor engaged for operation or maintenance or both of such systems, may be permitted after carrying out personnel risk assessment and mitigative measures taken thereof along with an undertaking complying with SLA
Provided that in case of any cyber security breach, the entity shall enquire the matter and initiate disciplinary proceedings against such vendor(s), including cloud service provider(s), committing cyber security breach.

(14) ensure online and offline backups of all critical system(s) in a separate, safe and secure environment, as specified in CSP.
(15) facilitate a comprehensive cyber security audit encompassing all critical systems, as specified under Regulation 18 of these regulations, once (1) in every financial year but with a minimum and maximum gap of nine (9) months and fifteen (15) months, respectively, between two consecutive cyber security audits.
Provided that the cyber security auditing agency engaged by entity shall deploy its qualified personnel, but exclusive of any manpower deployed for such entity, if any
Provided that no three (3) consecutive such audits shall be carried out by the same auditing agency or personnel.

(16) ensure that all IT products procured are complied with and tested in adherence with the orders issued by the Government of India.
(17) ensure compliance with and acquire ISO / IEC 27001 certificate or Technical Criteria Certificate encompassing all critical systems.
Provided that no four (4) consecutive certification audits for the certification of ISO 27001 or Technical Criteria Certificate shall be carried out by the same auditing agency or personnel.

(18) maintain asset register(s)

a) for all cyber assets along with the requisite details including ownership, hardware, firmware, software and patch as per the procedure defined in CSP
b) recording the details of all critical systems along with the requisite details including its configuration, hardware, software, network architecture depicting data flows and communication protocols used therein

Provided that such register(s) shall be reviewed and updated at least once (1) in every financial year or upon commissioning of any new cyber asset or critical system, including replacements thereof, whichever is earlier.

(19) maintain Cyber Risk Assessment and Mitigation Plan (CRAMP) for all assets detailed in cyber asset register, as per the procedure defined in CSP
Provided that CRAMP shall be updated at least once in every six (6) months and reviewed at least once (1) in every financial year and such CRAMP shall be implemented to manage the vulnerabilities, threats and risks associated thereof

(20) ensure that the cyber security audit, including vulnerability assessment and

राकेश 21/10/2025

penetration testing (VAPT), is carried out prior to the commissioning of any new critical system, including replacement of such system and manage vulnerabilities and risks for critical system as per the mechanism defined in CSP

(21) furnish relevant information, including system details and functionality, of all new critical systems commissioned, including those replaced, as per asset register associated with critical systems to the CSIRT – Power within thirty (30) days of such commissioning or replacement.

(22) provide the relevant information to NCIIPC for identification of CII and within sixty (60) days of an asset being identified as a CII by NCIIPC, shall approach the appropriate government for notifying such asset as a Protected System.

(23) ensure that CII(s) and Protected System(s) are not discoverable on public platforms, unless approved by the head or board of the entity, as applicable, on the basis of business requirements, criticality and risk assessment of such system(s)

(24) ensure that the procurement process mandates inclusion and verification of necessary cyber security requirements during the Factory Acceptance Test (FAT) and Site Acceptance Test (SAT)

(25) ensure that the clocks of all relevant information processing systems within IT and OT systems, as applicable, are synchronized to a reference time source as provided in the CSP.

Provided that prior to selection of such reference time source, detailed cyber risk assessment shall be carried out

(26) ensure that all personnel, including personnel engaged by vendors in day-to-day operation and maintenance of all critical systems, have mandatorily undergone designated cyber security courses pertaining to power sector from training institutes recognized by the Authority.

(27) ensure that the systems, networks and applications associated with physical security of critical systems are logically as well as physically separated from the network of such systems.

(28) maintain Incident Response and Recovery Plan, as specified in CSP, to recover from cyber incidents and resume normal operations at the earliest

Provided that such plan shall be reviewed and updated at least once (1) in every six (6) months

(29) have surveillance and continuous monitoring of IT system(s) and OT system(s), as applicable, for identification of threats as well as vulnerabilities and provide incident response and remediation support thereof

(30) ensure that logs of all security devices deployed at ESP are enabled to record exchange of data and information flowing through such devices

(31) ensure regular review and updation of rules and policies of perimeter security devices

(32) ensure that the IT equipment and services are procured from trusted sources, in accordance with orders, directions, or guidelines issued by the Government of India from time to time.

(33) comply with the directions and requirements issued under the Information Technology Act, 2000 and with all rules and regulations made thereunder, in addition to these regulations.

राकेश
11/01/2025

Chapter – IV
Additional Cyber Security Requirements of Entities related to OT Systems.

9. In addition to requirements mandated for entities under the Regulation 8 of these regulations, the Entity shall

(1) ensure physical isolation of OT system(s) from internet as well as IT system(s).
Provided that in case such isolation, from IT system(s), is not possible due to business requirements, such IT and OT interconnection may be permitted, as per the procedure defined in CSP, with suitable hardened logical separation between OT system and IT system, on the basis of risk assessment of such interconnection and approval of head or board of the entity, as applicable.
Provided that such interconnection is continuously monitored for detection of malicious activities and corrective measures thereof.
Provided that such approval and logs associated with such interconnection shall be retained for a period as specified in data retention policy.

(2) ensure deployment of suitable perimeter level cyber security devices, including firewall, at point of inter-connection of OT system(s) with power system such that the deployed security system meets the requirements of, inter alia, detection and filtering of OT related protocols as well as traffic; content, user and application based filtering; deep packet inspection, intrusion detection; geo-fencing; user controlled updates; detection based on signature and behavioral anomalies and filtering thereof.
Provided that the updates, including, signatures for devices forming part of such security system shall be carried out in offline mode, as specified in CSP.

(3) ensure that control and operation of power system elements and exchange of information thereof, including real time data, shall be over a dedicated communication channel isolated from the internet, through perimeter level cyber security devices mandated under the Regulation 9(2) of these regulations, and shall be confined to national boundaries only.
Provided that for entities having business requirements or cross border power system elements, the exchange of information and real time data, as identified under CSP, may be permitted beyond the national boundaries through dedicated communication channel, isolated from internet, and along with cyber security devices mandated under the Regulation 9(2) of these regulations, subject to the condition that such information and data are monitored continuously to detect any anomaly or unauthorized attempt.
Provided that in case of exchange of real time information and data associated with end consumers, the same may be permitted through secured connection, isolated from public access, subject to the condition that exchange of sensitive information and data thereof over such connection shall be encrypted to ensure its confidentiality, integrity and privacy.

(4) ensure that if remote operation is necessary for business requirements, the same shall be, within India, with the prior approval of head or board of the entity, as applicable, as per the procedure specified in the CSP, through a dedicated communication channel, isolated from internet, having cyber security system mandated under the Regulation 9(3) of these regulations.

(5) ensure that all OT equipment, components and parts thereof deployed for control

and operation of power system shall be complied with relevant testing standards as well as orders issued by the Government of India.

(6) ensure that the communication channel and data of OT system(s) is isolated from that of IT system(s)

(7) ensure that the OT equipment and services are procured from trusted sources, in accordance with orders, directions, or guidelines issued by the Government of India from time to time.

Chapter – V
Functions of CISO and ISD

10. The CISO and Alternate CISO shall be the citizens as well as residents of India and shall possess a degree in engineering or equivalent from a recognized institute, with at least fifteen (15) years of experience in domain of power sector or Information Technology.
Notwithstanding anything above, the Authority may specify additional qualifications for CISO of entity, through separate orders.
Provided that in absence of CISO, the roles and responsibilities of the CISO shall be performed and executed by Alternate CISO.

11. The CISO shall
(1) be the nodal officer for all cyber security related matters
(2) coordinate with all concerned stakeholders associated with the cyber security related matters.

12. The functions of the CISO, with the assistance of the ISD shall include, inter-alia, the following:
(1) reporting of cyber security incidents within six (6) hours to CSIRT – Power
Provided that in case any incident is concluded as a cyber sabotage in critical systems, the same shall be reported within twenty four (24) hours
(2) quarterly review of compliances as mandated in CSP.
(3) implementation of cyber security control measures for critical system(s), as specified in CSP, to firm up their cyber resilience.
(4) in case of CII or protected system, implementation of cyber security control measure as per guidelines of NCIIPC.
(5) acting upon the cyber security related directives, guidelines and advisories issued by the Government of India, the Authority as well as CSIRT – Power.
(6) gathering of cyber threat intelligence, its analysis, identification of threat vectors, assessment of cyber security risks and mitigation measures thereof.
(7) sharing of the detailed report of detected cyber security incidents, Action Taken Reports, Root Cause Analysis and other relevant information with CSIRT – Power.
(8) retention of all cyber security related data, information and documents in the manner, form and period as specified in data retention policy
(9) custody of all documents specified in the Schedule – II of these regulations
(10) ensuring the updation of firmware and software of all critical systems, with patches digitally signed by OEM, as provided in CSP.
(11) ensuring the storage of logs of all ICT systems and logs as well as forensic records pertaining to cyber security incidents for the period, as specified in CSP
(12) providing required information, including allocated, used and unused public IPs, with CSIRT – Power

रोकेश
01/10/2025

(13) ensuring random testing of day-to-day operations of critical systems for being in conformance with its CSP and corrective measures thereof, if necessary.

(14) prepare a procedure to facilitate remote access to cyber assets associated with non-critical system(s), for troubleshooting and emergency requirements, including suitable security controls required and process to grant approval for such access

(15) prepare a procedure, as specified in CSP, to facilitate safe and secure remote operation of OT system(s) and updation thereof

(16) ensure the development, implementation, review and updation of CSP, CCMP, data retention policy and backup policy.

(17) ensure the preparation, updation and review of Asset Register(s) for cyber assets and critical systems as well as CRAMP.

(18) ensure synchronization of all IT systems and OT systems to the reference time source, as specified under CSP

Chapter-VI
Cyber Security Policy

13. The CSP shall be aligned with the Business Continuity Plan (BCP) of entity covering OT as well as IT environment, as applicable, and the same may include

(1) defined purpose and scope along with all applicable cyber security requirements and compliances thereof.

(2) for entities having Protected Systems, provisions ensuring alignment with NCIIPC guidelines and control requirements.

(3) defined roles and responsibilities of relevant internal and external stakeholders

(4) defined procedure to prepare cyber asset register, consisting of all cyber assets and classification thereof on the basis of their criticality and risk identified in CRAMP; and update such procedure; for detailed visibility and management of all cyber assets.

(5) defined procedure to identify all systems and classify such systems as critical systems, on the basis of a defined criteria considering their impact on the BCP; as well as record details of such systems in a register

Provided that such procedure shall be reviewed and updated at least once (1) in every financial year.

(6) defined procedure for CRAMP to identify vulnerabilities and threats against each cyber asset and risk(s) associated thereof; control and mitigation measures in commensuration with criticality of such risks and implementation thereof.

Provided that such procedure shall be reviewed and updated at least once (1) in every financial year.

(7) defined mechanism to manage the vulnerabilities and risks in critical systems by timely identifying deficiencies and threats in such systems, including receipt of associated information from internal and external sources, analysis of such information, risk assessment and management thereof.

Provided that such mechanism shall be reviewed and updated at least once (1) in every financial year or upon commissioning of any new critical system, including replacement thereof, whichever is earlier.

(8) procedure to identify and report cyber sabotages in critical systems, including receipt of such information from internal as well as external stakeholders

(9) defined Incident Response and Recovery Plan detailing list of all incidents, risk analysis and risk-based incident specific response plan for effective and timely

रविकेश 08/10/2025

restoration of affected system(s)

(10)mechanism for random testing of day-to-day operations of critical system(s), for being in conformance with applicable policies, rules and regulations issued by CSIRT – Power and other agencies designated by the Government of India in the area of cyber security.

Provided that such testing shall not interrupt the operations and functionality of such systems and safety thereof.

(11)Access Control mechanism to critical systems and cyber assets associated thereof, applications having public access, sensitive information and sensitive data, for user Access Management on the basis of Authentication, Authorization and Accounting criteria and criticality thereof.

Provided that a detailed procedure may be laid down to restrict the physical and logical access to documents and records specified under data retention policy

(12)Personnel Risk Assessment process to identify risks associated with personnel deployed by vendor, having authorized cyber or physical access to critical system(s) and assets associated thereof or engaged for Operation or Maintenance or both of such system(s), on the basis of their roles and responsibilities, including change in such roles and responsibilities; and mitigating measures thereof.

Provided that, for the employees, engaged in day-to-day O & M or having authorized cyber or physical access to critical system(s) and assets associated thereof, personnel risk assessment shall be carried out, on the basis of their roles executed and duration of deployment in such entrusted tasks, after their termination, resignation and superannuation from their employment

(13)mechanism to ensure that all access points to critical systems are secured physically and monitored continuously and also such access is restricted for physical protection of these systems and cyber assets associated thereof.

Provided that in case of a perceptible threat of physical damage to any of these systems or assets thereof, the physical access granted to any individual for such system or asset may be revoked.

(14)Cyber Supply Chain Risk Management process to identify and assess cyber security risks associated with supply chain of critical systems and services thereof along with mitigative measures.

(15)defined procedure for remote access to cyber assets, along with the details of authorization to grant approval for such access on the basis of their criticality, such that the such access is safe and secured through suitable control measures including minimum duration with least privileges, multi-factor authentication and geo-fencing

(16)defined procedure for remote operation of OT systems, to meet the business requirement, on the basis of assessment of cyber risks associated with such operation and mitigation measures thereof.

Provided that such procedure shall be reviewed and updated once (1) every year or upon any change necessitated to meet business requirements, whichever is earlier

(17)digital Data Protection and Privacy Policy in line with applicable Rules and Regulations issued the Government of India.

(18)defined backup policy to ensure that online or offline backup data or both, as applicable, of all critical systems is up to date, but not older than a month, and retained in a separate and safe environment for the period as specified in the data retention policy.

Provided that the backup policy shall be reviewed and updated at least once (1) in

every financial year and ensure that the integrity of backup data and its restoration is tested such that the same meets the requirements of BCP

(19) defined mechanism to ensure storage of sensitive data and its backup, as well as its transmission over dedicated communication channel or internet, is encrypted to ensure its confidentiality, integrity and availability

Provided that in case encryption of certain sensitive data is not feasible due to business requirements, the same, in unencrypted form, may be permitted over a dedicated communication channel.

(20) annual cyber security training program for capacity development of all personnel having authorized cyber or physical access or both to critical system(s) and assets associated thereof

(21) Internet Access Policy to monitor and restrict the internet traffic to ensure defined and authorized use only

(22) phase out plan for obsolete cyber assets as well as those assets nearing end of useful life and management thereof along with their safe and secure disposal.

(23) plan for collaboration with industry, stakeholders and academia to promote R & D activities in the domain of cyber security

Provided that scope and assets for such collaboration may be identified after carrying out detailed risk assessment and such collaboration shall be effected after signing of NDA

(24) define a criterion to classify the software updates, including patches, in critical systems, into two categories:

a) a software update that qualifies for requirement of prior cyber security audit before its deployment, and

b) a software update that does not require prior cyber security audit before its deployment but necessitates such assessment in next cyber security audit.

The indicative list of software updates, which requires prior cyber security audit, is provided at schedule – III.

(25) defined Change Management process to record changes implemented in all critical systems and to ensure that planned changes on such systems and cyber assets associated thereof are controlled.

Provided that such process shall ensure that software updates, including patches, qualified for prior requirement of cyber security audit shall be version controlled along with provision of roll-back.

Provided that the updates, including patches, in OT system(s) shall be digitally signed by OEM and such updates may be deployed in offline mode, after their risk assessment and successful testing in simulated environment. However, in case digital signature of OEM is not available for any patch, the source and authenticity of such patch shall be verified.

(26) a mechanism to facilitate storage of logs and forensic records as mandated in data retention policy, in a safe and secured environment.

(27) a procedure to select a time source, after assessing its associated cyber risks, for synchronizing all processing systems of IT and OT environment to such source.

Provided that the reference time source selected for OT system(s) shall be independent of internet.

(28) defined procedure for logical separation of OT system(s) from IT system(s) to

राकेश 01/01/2026

ensure safe and secure operation of both IT systems as well as OT systems

Provided that the identified data and information shall flow unidirectional only.

(29) defined procedure to identify and classify the data as well as information, including real time data, permitted to be communicated beyond national boundaries, on the basis of risk assessment and business requirements

(30) defined procedure to identify web applications along with a criterion to classify such applications as critical web applications, on the basis of their impact on business operations and continuity

(31) defined procedure for safe and secure disposal of out of service or obsolete cyber asset(s) and data stored therein

(32) defined procedure for safe and secure disposal of sensitive data and sensitive information

(33) data retention policy specifying manner and form of retention of various documents and records as well as data and information including,

a) backup of data of critical systems;
b) record of logs, risk assessment and approval thereof for each grant of remote access to critical systems;
c) logs and grant of approval associated with interconnection of OT system with IT system
d) cyber security documents including certificates of cyber security tests, FAT and SAT results, cyber security audit reports and other documents as mandated by the Government of India.
e) record of changes, including software updates and patches, implemented in critical systems

Provided that the data retention policy shall be reviewed and updated at least once (1) in every financial year and the data, information and documents shall be retained to ensure

a) at least last two (2) working data backups are available;
b) risk assessment, physical record of grant of approval and logs w.r.t each remote access to critical system(s) are available for at least one (01) year
c) reports of FAT and SAT are available throughout life of cyber asset;
d) record of risk assessment for remote operation in OT environment along with approval received thereof are available for at least one (1) year;
e) cyber security audit reports of last three (3) years are available
f) certification audit reports of last four (4) years are available
g) self-audit report of last three (3) years are available
h) logs of all ICT systems, interconnection of OT system with IT system and forensic records are available for a period of 180 days
i) the logs associated with an incident, including logs pertaining to 180 days prior and post to such incident, are available for atleast 365 days from occurrence of such incident

Provided that the access to such information, data and documents may be restricted to authorized persons only, on the basis of procedure defined under access control mechanism.

Provided that the Authority may, through separate orders, include any other document and specify any other manner, mode and period for retention of documents under data retention policy.

राकेश
akhaur

Chapter-VII
Cyber Crisis Management Plan (CCMP)

14. The CCMP shall
    (1) include detailed Standard Operating Procedure (SOP) to detect and identify all incidents, criteria to classify an incident as a crisis and list of all possible crisis scenarios;
    (2) identify stakeholders along with their roles and responsibilities for all possible crises and communication of such roles as well as responsibilities thereof;
    (3) include manner and mode of communication with internal as well as external stakeholders, for close coordination, during the crisis
    (4) include mitigative measures to minimize the impact and recover from crisis at the earliest

15. The entity shall
    (1) ensure availability of all essential communications with relevant internal and external stakeholders during cyber crisis.
    (2) test the efficacy of CCMP at least once (1) in every year through exercises and mock drills for selected scenarios out of all identified crisis scenarios specified under it
    Provided that the selection of scenarios in any year shall not overlap with the scenarios tested and verified earlier, unless the cycle of all listed scenarios has been completed for testing and verification.
    (3) prepare a detailed report of each actual crisis handled and recovered along with experience gained, lessons learnt, feedback received, lapses observed and proposed measures thereof
    Provided that the relevant information, including brief about actual crisis, its handling and takeaways shall be shared with CSIRT – Power and other stakeholders for collective improvement of cyber security ecosystem of power sector.
    Provided that the CCMP shall be updated by incorporating qualified observations of its own and that of other stakeholders to improve its cyber security posture.

Chapter-VIII
Cybersecurity Requirements for Vendor

16. The vendor shall
    (1) provide documented and tested procedures as well as recovery plan to the entity, for restoration of systems supplied by them from potential cyber crisis scenarios
    (2) ensure security patches and updates for all systems as well as components supplied by them are available to the entity throughout their contract period or useful life of such system(s), whichever is later
    (3) provide detailed document, to the entity, consisting of all requirements and processes, including security patches as well as updates required to be installed on the third-party components, to integrate a component or sub-system supplied by them
    (4) provide details of end of support or end of life of software, hardware and system to the entity, as applicable, supplied by them, including those sourced from third parties
    (5) provide Software Bill of Materials (SBoM) to the entity, as per CERT-In guidelines, comprising detailed list of all software components supplied by them for applications, including firmware, deployed in critical systems.

रोकेश
04/10/2025

17. In the case of Distributed Generation Resource(s) of prosumers, it shall be the responsibility of vendor to

(1) ensure that any application, associated monitoring and control servers, and the real-time data of such systems, including any data or information hosted on cloud platforms, be stored in an encrypted, secure, and protected environment, and shall reside exclusively within India.

(2) ensure that all remote control and telemetry communications between grid-connected devices, applications, aggregators, and distribution licensees, wherever real-time communication takes place, shall mandatorily be carried out through secure, authorized, authenticated, and encrypted channels.

(3) provide such information as may be required for the purpose of verification of a trusted source, in accordance with the orders, directions, or guidelines issued by the Government of India from time to time.

Provided that this Regulation for the existing Distributed Generation Resource(s) of prosumers shall come into force on such date, as may be specified by the Authority through separate order.

Chapter-IX
Cyber Security Audit

18. The entity shall ensure that

(1) cyber security audit shall be conducted, as per scope detailed in cyber security audit guidelines and directions issued by CSIRT – Power and other cyber security agencies designated by the Government of India.

(2) the scope of cyber security audit shall also include verification of closure of all audit findings identified in the previous cyber security audit.

(3) the auditor submits its cyber security audit report within six (6) weeks of its commencement and all critical and high-risk vulnerabilities shall be addressed within a period of one (1) month and medium as well as low risks vulnerabilities within a period of three (3) months from the date of submission of cyber security audit report by the auditor.

Provided that appropriate compensatory controls shall be deployed to contain critical and high-risk vulnerabilities, till audit clearance of such vulnerabilities

19. CISO shall review the audit compliances and ensure that the auditor shall submit its cyber security audit closure report within six (6) months from commencement of cyber security audit.

20. CISO shall report major audit findings, including critical and high risk vulnerabilities, observed in cyber security audit closure report along with any non – compliances with respect to critical systems to the head or board of the entity, as the case may be.

Provided that CISO – MoP may ask for audit closure report of any entity at any point of time for examination and, if need be, after seeking written clarification, with prior approval of the Government of India and prior notice to such entity, may appoint a third-party auditor for verification of audit compliances, the cost of which shall be borne by entity.

Provided that in case findings of third party audit are in variance with the observations of cyber security audit closure report, CISO – MoP may take further necessary action.

रोकड़ा 4/Feb/2025

Chapter-X
Miscellaneous

21. The entity shall conduct self – audit to assess its compliance with these regulations in a financial year and submit a compliance report thereof detailing list of all applicable regulations, compliance and reasons for non – compliance, if any, to the CISO – MoP by 30th June of next financial year.

    Provided that, for cybersecurity and compliance with these regulations, the head or board of the entity as the case may be, shall be responsible.

    Provided that the entity shall address the non-compliances in a time bound manner and ensure that all such non-compliances are addressed before self-audit scheduled in next financial year.

    Provided that CISO – MoP, based on the facts available or reported by any individual, may examine compliance report of any entity and after seeking written clarification, with prior approval of the Government of India and prior notice to such entity, may appoint a third party auditor to verify claim made by the entity, the cost of which shall be borne by such entity.

22. In specific cases, after seeking written clarification(s) and examination thereof, CISO MoP may recommend the Government of India, for initiation of appropriate proceedings under relevant provisions of IT Act, 2000 or file a petition before appropriate Commission for proceedings under section 142 of the Electricity Act, 2003.

23. **Power to Relax**

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

24. **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 interested 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 effect to the objectives of these regulations.

XXXXX

Schedule – I

Indicative minimum manpower required for ISD :

1. 04 (Four) officers or officials including CISO and Four (04) officers or officials for shift operations.
2. Besides these officers or officials, additional officers or officials may be placed to assist CISO in discharging duties mentioned in the Chapter V.

Schedule – II

The following documents and information shall be retained

1. Cyber Security Policy (CSP) along with documents and procedures listed therein
2. Cyber Crisis Management Plan (CCMP)
3. Data Retention Policy and all documents and information listed thereunder
4. ISO / IEC 27001 Certificate or Technical Criteria Certificate
5. Asset register(s) for cyber assets and critical systems
6. Cyber Risk Assessment and Mitigation Plan (CRAMP)
7. Incident Response and Recovery Plan
8. Cyber Security Incident Response and Recovery Plan
9. Software Bill of Material

Schedule III

The indicative criteria for software updates requiring Prior Cyber Security Audit

Software updates including modifications and enhancements to applications, websites, web portals, and associated systems meeting any of the following criteria shall mandatorily require a successful cyber security audit prior to deployment:

1. **Critical System Impact**: Updates that affect core operational processes, such as energy generation, transmission, distribution, or load management, wherein vulnerabilities could compromise the functionality or reliability of critical infrastructure.
2. **Access Control Modifications**: Updates that alter user authentication, authorization mechanisms, or administrative privileges, including those involving identity management systems or access control policies.
3. **Integration with Third-Party Systems**: Updates involving integration with external systems, applications, or third-party services, especially those that exchange sensitive data or enable cross-platform communication.
4. **Security Protocol Changes**: Updates introducing changes to encryption standards, data transmission protocols, or other security-related configurations that could impact the protection of sensitive information.
5. **Introduction of New Features or Interfaces**: Updates adding significant new functionalities, user interfaces, or APIs that could present potential attack surfaces.
6. **Resolution of Security Vulnerabilities**: Updates addressing previously identified Critical and High impact vulnerabilities, where an incomplete or improper implementation could exacerbate security risks.
7. **Incident Response and Monitoring Systems**: Updates affecting systems or tools related to cyber security monitoring, incident response, or log management, wherein any disruption could hinder the ability to detect or respond to threats effectively.
8. **Reform or Regulatory Mandated Systems**: Updates impacting systems subject to regulations or pursuant to reforms programs of appropriate government.

*****