




भारत सरकार
Government of India
विद्युत मंत्रालय
Ministry of Power
केन्द्रीय विद्युत प्राधिकरण
Central Electricity Authority
सूचना प्रौद्योगिकी एवं साइबर सुरक्षा प्रभाग
Information Technology & Cyber Security Division

विषय : CEA (Cyber Security in Power Sector) Guidelines, 2021.

CEA is mandated to prepare 'Guidelines on Cyber Security' in Power Sector under the provision of regulation (10) of the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019. Guidelines on Cyber Security in Power Sector incorporating the cardinal principles has been prepared by CEA. In compliance to the provision of the above regulation, **CEA (Cyber Security in Power Sector) Guidelines, 2021** are issued for compliance by all entities listed in the clause 2.3 (Applicability of the Guidelines) of the guidelines.

Encl: Guidelines on Cyber Security


07/10/21
(V.K. Mishra)
Secretary CEA

CEA (Cyber Security in Power Sector) Guidelines, 2021

1.0 Background

- 1.1 Cyber intrusion attempts and Cyber-attacks in any critical sector are carried out with a malicious intent. In Power Sector it's either to compromise the Power Supply System or to render the grid operation in-secure. Any such compromise, may result in mal-operations of equipments, equipment damages or even in a cascading grid brownout/blackout. The much hyped air gap myth between IT and OT Systems now stands shattered. The artificial air gap created by deploying firewalls between any IT and OT System can be jumped by any insider or an outsider through social engineering. Cyber-attacks are staged through tactics & techniques of Initial Access, Execution, Persistence, Privilege Escalation, Defence Evasion, Command and Control, Exfiltration. After gaining the entry inside the system through privilege escalation, the control of IT network and operations of OT systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/State sponsored or non-sponsored adversaries and cyber attackers to design more sinister and advanced cyber-attacks.
- 1.2 Government of India has set up the Indian Computer Emergency Response Team (CERT-In) for Early Warning and Response to cyber security incidents and to have collaboration at National and International level for information sharing on mitigation of cyber threats. CERT-In regularly issues advisories on safeguarding computer systems and publishes Security Guidelines which are widely circulated for compliances. All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct cyber security audit of their entire Cyber Infrastructure including websites at regular interval through CERT-In empanelled Auditors so as to identify gaps and appropriate corrective actions to be taken in cyber security practices. CERT-In extends supports to enable Responsible Entity in conducting cyber security mock drills and in assessment of their preparation to withstand cyber-attacks. The Responsible Entity must submit Reports of Cyber Audit of cyber security controls, architecture, vulnerability management, network security and periodic cyber security drills to sectoral CERT as well as CERT-In. Team of experts shall review these reports and shortcomings if any in the compliances shall be flagged by them. CERT-In on regular basis also conducts workshops and training programs to enhance Cyber awareness of all Stakeholders.
- 1.3 Ministry of Power has created 6(six) sectoral CERTs namely Thermal, Hydro, Transmission, Grid Operation, RE and Distribution for ensuring cyber security in Indian Power Sector. Each Sectoral CERT has prepared their sub-sector specific model Cyber Crisis Management Plan(C-CMP) for countering cyber-attacks and cyber terrorism. Each Sectoral CERT has circulated their model C-CMPs for preparation and implementation of organization specific C-CMP by each of their Constituent Utility.
- 1.4 All Responsible Entities, Service Providers, Equipment Suppliers/Vendors and Consultants engaged in Power Sector are equally responsible for ensuring cyber security of the Indian Power Supply System. They are to act timely upon each threat intelligence,

advisories and other inputs received from authenticated sources, for continuous improvement in their cyber security posture.

- 1.5 In the current Indian scenario though many cyber security directives and guidelines exists, but none of them are power sector specific. Ministry of Power has directed CEA to prepare Regulation on Cyber Security in Power Sector. And as an interim measures CEA has been directed to issue Guideline on Cyber Security in Power Sector, under the provision of Regulation 10 on Cyber Security in the “Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019”.
- 1.6 The Guidelines on Cyber Security, in the form of Articles written below, requires mandatory Compliance by all Responsible Entities. The Guidelines shall come into effect from the date of issue by Central Electricity Authority, New Delhi.
- 2.0 Hereby the Guidelines on Cyber Security are drawn in the form of Articles for compliance by the Requester as well as User under the following provision of Regulation 10 on Cyber Security, in the “Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019”.

“The requester and the user shall comply with cyber security guidelines issued by the Central Government, from time to time, and the technical standards for communication system in Power Sector laid down by the Authority.”

2.1 **Objective of issuing Guideline:**

- a) Creating cyber security awareness
- b) Creating a secure cyber ecosystem,
- c) Creating a cyber-assurance framework,
- d) Strengthening the regulatory framework,
- e) Creating mechanisms for security threat early warning, vulnerability management and response to security threats,
- f) Securing remote operations and services,
- g) Protection and resilience of critical information infrastructure,
- h) Reducing cyber supply chain risks,
- i) Encouraging use of open standards,
- j) Promotion of research and development in cyber security,
- k) Human resource development in the domain of Cyber Security,
- l) Developing effective public private partnerships,
- m) Information sharing and cooperation
- n) Operationalization of the National Cyber Security Policy

2.2 Within the text of these Articles, ‘**Responsible Entity**’ shall mean all:

- a) Transmission Utilities as well as Transmission Licensees,
- b) Load despatch centres (State, Regional and National),
- c) Generation utilities (Hydro, Thermal, Nuclear, RE),
- d) Distribution Utilities
- e) Generation Aggregators,
- f) Trading Exchanges,
- g) Regional Power Committees, and
- h) Regulatory Commissions.

2.3 **Applicability:**

All Responsible Entities as well as System Integrators, Equipment Manufacturers, Suppliers/Vendors, Service Providers, IT Hardware and Software OEMs engaged in the Indian Power Supply System.

2.4 **Scope:**

2.4.1 **Control Systems for System Operation and Operation Management.**

- a) Grid Control and Management Systems,
- b) Power Plant Control Systems,
- c) Central Systems used to monitor and control of distributed generation and loads e.g. virtual power plants, storage management, central control rooms for hydroelectric plants, photovoltaic/wind power installations,
- d) Systems for fault management and work force management,
- e) Metering and measurement management systems,
- f) Data archiving systems,
- g) Parameterisation, configuration and programming systems,
- h) Supporting systems required for operation of the above mentioned systems,

2.4.2 **Communication System.**

- a) Routers switches and firewalls,
- b) Communication technology-related network components,
- c) Wireless digital systems.
- d) Control Centre to Control Centre Communications for data exchange on ICCP.
(IEC 61850/60850-5/TASE.2/)

2.4.3 **Secondary, Automation and Tele control technologies**

- a) Control and Automation components,
- b) Control and field devices,
- c) Tele control devices,
- d) Programmable logic controllers / Remote Terminal Units, including digital sensor and actuators elements,
- e) Protection devices,
- f) Safety components,
- g) Digital measurement and metering installations,
- h) Synchronisation devices,
- i) Excitation Systems,

3.0 **Definition of Terms:**

1. **Access Management:** shall mean set of policies and procedures of the Responsible Entity for allowing Personnel, devices and IoT to securely perform a broad range of operational, maintenance, and asset management tasks either on site or remotely as laid down in Clause 5.2.5 of IS 16335.
2. **Accreditation:** shall mean the process of verifying that an organisation is capable of conducting the tests and assessments against a product/process that are required to be certified.

3. **Accreditation Body:** shall mean an organisation that has been accredited to verify the credentials and capabilities of the organisations that wish to become a certification body.
4. **Act:** shall mean the Information Technology Act, 2000 (21 of 2000)
5. **Asset:** shall mean anything that has value to the organization.
6. **Certification:** shall mean the process of verifying that a product has been manufactured in conformance with a set of predefined standards and/or regulations by an organisation, that is accredited to conduct the certification process
7. **Certification Body:** shall mean an organisation that has been accredited by an accreditation body to certify products / process against a certification scheme.
8. **Certification Scheme:** shall mean the processes, paperwork, tools, and documentation that define how a product or manufacturer is certified
9. **Chief Information Security Officer:** shall mean the designated employee of Senior management level directly reporting to Managing Director/Chief Executive Officer/Secretary of the Responsible Entity, 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
10. **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 Supply System.
11. **Critical System:** shall mean cyber assets essential to the reliable operation of critical asset. Critical System consists of those cyber assets that have at least one of the following characteristics:
 - a) The cyber asset uses a routable protocol to communicate outside the electronic security perimeter.
 - b) The cyber asset uses a routable protocol within a control centre.
 - c) The cyber asset is dial-up accessible.
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 are connected 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 Security Breach:** shall mean any cyber incident or cyber security violation that results in unauthorized or illegitimate access or 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 of data/information maintained in a computer resource or cyber asset.
16. **Cyber Security Incident:** shall mean any real or suspected adverse cyber security event that violates, explicitly or implicitly, cyber security policy of Responsible Entity resulting in unauthorized access, denial of service or disruption, unauthorized use of computer resource for processing or storage of information or changes to data or information

without authorization, leading to harm to the power grid or its critical sub-sectoral elements Generation, Transmission and Distribution.

17. **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.
18. **Electronic Security Perimeter:** shall mean the logical border surrounding a network to which the Cyber Systems of Power Supply System are connected using a routable protocol.
19. **Information Security Division:** shall mean a division accountable for cyber security and protection of the Critical System of the Responsible Entity.
20. **Protected System:** shall mean any computer, computer system or computer network of the Responsible Entity notified under section 70 of the Act, in the official gazette by appropriate Government.
21. **Security Architecture:** shall mean a framework and guidance to implement and operate a system using the appropriate security controls with the goal to maintain the system's quality attributes like confidentiality, integrity, availability, accountability and assurance.
22. **Vulnerability:** shall mean intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence
23. **Vulnerability Assessment:** shall mean a process of identifying and quantifying vulnerabilities

4.0 Standards

Reference	Description
ISO/IEC 15408	Common Criteria Certification Standard
ISO/IEC 17011	General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
ISO/IEC 21827	Systems Security Engineering - Capability Maturity Model (SSE-CMM)
ISO/IEC 24748-1	Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management.
ISO 27001/2	Information Security Management
ISO/ IEC 27019	Information technology — Security techniques — Information Security controls for the energy utility industry
ISO/IEC 61508	Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
IEC 61850	Communication networks and systems for power utility automation
IEC 62351	Standards for Securing Power System Communications
IEC 62443	Cyber Security for Industrial Control Systems
IS 16335	Power Control Systems – Security Requirements.

5.0 Abbreviations

Abbreviations	Description
a) BES	Bulk Electric System

b)	CDAC	Centre for Development of Advanced Computing
c)	CEA	Central Electricity Authority
d)	CERC	Central Electricity Regulatory Commission
e)	CERT	Computer Emergency Response Team
f)	CERT-In	Indian Computer Emergency Response Team
g)	CII	Critical Information Infrastructure
h)	CISO	Chief Information Security Officer
i)	CSK	Cyber Swachhta Kendra
j)	COTS	Commercial off-the Shelf
k)	ESP	Electronic Security perimeter
l)	ICS	Industrial Control Systems
m)	ICT	Information and Communications Technology
n)	IEC	International Electro Technical Commission
o)	ISAC	Information Sharing and Analysis Centre
p)	ISD	Information Security Division
q)	ISO	International Organization for Standardization
r)	ISMS	Information Security Management System
s)	IT	Information Technology
t)	FAT	Factory Acceptance Test
u)	NABL	National Accreditation Board for Testing and Calibration Laboratories
v)	NCIIPC	National Critical Information Infrastructure Protection Centre
w)	NLDC	National Load Dispatch Centre
x)	NPTI	National Power Training Institute
y)	NSCS	National Security Council Secretariat
z)	OEM	Original Equipment Manufacturer
aa)	OT	Operational Technology
bb)	RLDC	Regional Load Dispatch Centres
cc)	SAT	Site Acceptance Test
dd)	SERC	State Electricity Regulatory Commission
ee)	SCADA	Supervisory Control and Data Acquisition Systems
ff)	SIEM	Security Information and Event Management
gg)	SLA	Service Level Agreement
hh)	SLDC	State Load Dispatch Centre
ii)	QCI	Quality Council of India

CEA (Cyber Security in Power Sector) Guidelines, 2021

Article 1. Cyber Security Policy.

a. Cardinal Principles: The Responsible entity will strictly adhere to following cardinal principles while framing cyber security policy:

- i. There is hard isolation of their OT Systems from any internet facing IT system.
 - ii. May keep only one of their IT systems with internet facing at any of their site/location if required which is isolated from all OT zones and kept in a separate room under the security and control of CISO.
 - iii. Downloading/Uploading of any data/information from their internet facing IT system is done only through an identifiable whitelisted device followed by scanning of both for any vulnerability/malware as per the SOP laid down and for all such activities digital logs are maintained and retained under the custody of CISO for at least 6 months. The log shall be readily to carry out the forensic analysis if asked by investigation agency.
 - iv. List of whitelisted IP addresses for each firewall is maintained by CISO and each firewall is configured for allowing communication with the whitelisted IP addresses only.
 - v. Communication between OT equipment/systems is done through the secure channel preferably of POWERTEL through the fibre optic cable. Security configuration of the communication channel is also to be ensured.
 - vi. All ICT based equipment/system deployed in infrastructure/system mandatorily CII are sourced from the list of the “Trusted Sources” as and when drawn by MoP/CEA.
- b. The Responsible Entity shall be ISO/IEC 27001 certified (including sector specific controls as per ISO/IEC 27019).
 - c. The Responsible Entity shall have a Cyber Security Policy drawn upon the guidelines issued by NCIIPC.
 - d. The Responsible Entity shall ensure annual review of their Cyber Security Policy by subject matter expert and changes shall be made therein only after obtaining the due approval from Board of Directors.
 - e. The process of Access Management for all Cyber Assets owned or under control of the Responsible Entity shall be detailed in the Cyber Security Policy.
 - f. The Cyber Security Policy shall leverage state-of-art cyber security technologies and relevant processes at multiple layers to mitigate the cyber security risks.
 - g. The Responsible Entity shall be solely responsible to get Cyber Security Policy implemented through its Information Security Division (ISD).
 - h. The CISO shall record the reason(s) for exemption required, if any, in case, unable to comply with any of the provision(s) of the Cyber Security Policy. Any exception shall be allowed only after an approval of provisions of compensatory control(s) to mitigate residual cyber security risks.

- i. The CISO shall record the exemptions sought in statement of applicability controls, while getting the ISO 27001 certified. All exemptions and its justification need to be in conformance with Cyber Security Policy of the Responsible Entity.
- j. The Responsible Entity shall allocate sufficient Annual budget for enhancing cyber security posture, enhanced year over year.
- k. The Responsible Entity shall work in collaboration with other Industry Stakeholders as well as Academia to promote R&D activity in the domain of cyber security.
- l. The Responsible Entity shall ensure that cyber security issues are taken up as agenda items in their Board meetings once in every three months.

Article 2 Appointment of CISO.

- a) The Responsible Entity shall mandatorily appoint a CISO and shall confirm to qualification, if any, **laid** by Quality Council of India (QCI). In absence, the work of CISO shall be looked upon by Alternate CISO. In case qualification for appointment of Alternate CISO has been relaxed for reasons recorded thereof, Alternate CISO has to mandatorily acquire the minimum required cyber security skill sets within six months from the date of his appointment.
- b) The Responsible Entity shall regularly update details of CISO and Alternate CISO, with the Sectoral CERT, as well as on ISAC-Power Portal.
- c) Roles and Responsibility of CISOs shall be as laid by CERT-In and ring-fenced to ensure cyber security of the Cyber Assets of the Responsible Entity.

Article 3: Identification of Critical Information Infrastructure (CII).

- a) The Responsible Entity shall submit to NCIIPC through Sectoral CERT, details of Cyber Assets which uses a routable protocol to communicate outside the Electronic Security Perimeter drawn by the Responsible Entity or a routable protocol within a control centre and dial-up accessible Cyber Assets, within 30 days from the date of their commissioning in the System.
- b) The Responsible Entity shall submit details of Critical Business Processes and underlying information infrastructure along with mapped impact and Risk Profile to NCIIPC and shall get their CIIs identified in consultation with NCIIPC. The process of the notification/declaration by Appropriate Government shall follow thereafter.
- c) The Responsible Entity shall review their declared/notified CIIs at least once a year to examine changes if any in the functional dependencies, protocols and technologies or upon any change in security architecture. The Responsible Entity shall review their declared/notified CIIs once in every 6 months, in case if NCIIPC has directed them to constitute an Information Security Steering Committee.
- d) The Responsible Entity shall ensure that all cyber assets of their identified/notified CIIs are recorded in the asset register and considered for risk assessment as well as for finalization of controls in statement of applicability.

Article 4. Electronic Security Perimeter

- a) The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all Access Points to the perimeter(s).

- b) The Responsible Entity shall follow procedure of identifying “Electronic Security Perimeter” in case of distributed and/or hybrid information infrastructure, as per IEC 62443 / IS16335 (as amended from time to time).
- c) The Responsible Entity shall ensure that every Critical System resides within an Electronic Security Perimeter.
- d) The Responsible Entity shall perform a cyber-Vulnerability Assessment of each electronic Access Points to the Electronic Security Perimeter(s) at least once in every 6 (six) months and/or after any change in Security Architecture.
- e) The Responsible Entity shall ensure that all critical, high and medium vulnerabilities identified as a result of cyber Vulnerability Assessment shall be closed and verified for the effective closure.

Article 5. Cyber Security Requirements

- a) The Responsible Entity shall have an Information Security Division (ISD), headed by CISO.
- b) The Responsible Entity shall ensure that the ISD must be functional on 24x7x365 basis and is manned by sufficient numbers of Engineers having valid certificate of successful completion of course on cyber security of Power Sector from the Training Institutes designated by CEA.
- c) The Responsible Entity shall ensure that ISD
 - 1) has on-boarded Cyber Swachhta Kendra(CSK) of CERT-In, if they have public IPs.
 - 2) has timely acted upon the advisories, guidelines and directive of NCIIPC, CSK, CERT-In and Sectoral CERTs,
 - 3) has deployed an Intrusion Detection System and Intrusion Prevention System capable of identifying behavioural anomaly in both IT as well as OT Systems.
 - 4) shares reports on incident response and targeted malware samples with CERT-In,
 - 5) updates the firmware/software with the digitally signed OEM validated patches only.
 - 6) enables only those ports and services that are required for normal operations. In case of any emergency the procedure as laid in Access management be followed.
 - 7) maintains firewall logs for the last 6 months duration. Firewall logs shall be analysed and all critical and high severity comments shall be addressed for effective closure.
 - 8) retains document of FAT, SAT test results and report/ certificate of cyber tests carried out for compliance of Government Orders and Cyber Security Audit.*
 - 9) maintains all cyber logs and cyber forensic records of any incident for at least** 90 days.
 - * FAT, SAT must include comprehensive cyber security tests of the component/equipment/system to be delivered/delivered at site.
 - ** 90 days from date of the commissioning of the system/recovery from any incident, whichever is later.
- d) The Responsible Entity shall routinely audit and test security properties of the Critical System and must act upon, in case if any new vulnerabilities is identified through testing or by the equipment manufacturer.

- e) The Responsible Entity shall design a secure architecture for control system appropriate for their process control environment*.
- f) All State Load Dispatch Centres(SLDCs) shall comply with the directions issued by the National Load Dispatch Centre(NLDC) as well as Regional Load Dispatch Centres(RLDCs) U/s 29 (1) of the Electricity Act, 2003 to ensure stability and cyber security of grid operation and achieve efficiency in the grid operation. In case of any non-compliance, the Head of SLDC shall be responsible and shall be liable for Penalty as per the provision of CERC/SERC.

*There are so many different types of systems in existence and so many possible solutions, it is important that the selection process ensures that the level of protection is commensurate with the business risk and the Responsible Entity shall not rely on one single security measure for its defence. (*Reference IEC/TR62351-10 Edition 1.0 2012-10 Power systems management and associated information exchange –Data and communications security – Part 10: Security architecture guidelines*).

Article 6 Cyber Risk Assessment and Mitigation Plan

- a) The Responsible Entity shall document in their Cyber Security Policy a Cyber Risk Assessment and Mitigation Plans drawn upon the best practises being followed in the Power Sector, and the same shall be approved by Board of Directors.
- b) The Cyber Risk Assessment and Mitigation Plans shall clearly define the matrix for assessing the cyber risk of both IT and OT environment and risk acceptance criteria.
- c) The Cyber Risk Assessment Plan shall be capable to demonstrate that repeated cyber security risk assessment delivers consistent, valid and comparable results.
- d) The review of cyber risk assessment shall be carried out at least once in a Quarter. The actionable of risk treatment and mitigation shall be tracked in this review for their effectiveness.
- e) The CISO shall be responsible for implementation and regular review, on the basis of internal and external feedbacks, of the Cyber Risk Assessment and Mitigation Plans.

Article 7 Phasing out of Legacy System

- a) As the life cycle of the Power System Equipment/System is longer than that of IT Systems deployed therein, the Responsible Entity shall ensure that all IT technologies in the Power System Equipment/System should have the ability to be upgraded.
- b) The Responsible Entity shall ensure that the Information Security Division shall draw the list of all communicable equipments/systems nearing end life or are left without support from OEM. Thereafter CISO shall identify equipment/systems to be phased out from the list drawn, firm up their replacement plan and put up the replacement plan for approval before the Board of Directors.
- c) The CISO shall ensure that till equipments/systems nearing end life or left without support from OEM are not replaced, their cyber security is hardened and ensured through additional controls provisioned in consultation with the OEM or alternate Supplier(s)*.
*e.g. Use of CDAC developed AppSamvid and whitelisting of applications installed may be explored across all legacy systems.
- d) The Responsible Entity shall document in their Cyber Security Policy a Standard Operating Procedure for safe and secure disposal of outlived or legacy devices.

Article 8. Cyber Security Training.

- a) The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized physical access (unescorted or escorted) to their Critical Systems.
- b) The Responsible Entity shall review annually their cyber security training program and shall update it whenever necessary. Annual Review shall record evaluation of the effectiveness of the trainings held.
- c) The Responsible Entity shall ensure that Cyber Security training program designed for their IT as well as OT O&M Personnel must include following topics and as per their functional requirements and security concerns additional topics shall be added:
 - 1) User authentication and authorization.
 - 2) Cyber Security and Protection mechanisms of IT/OT/ICS Systems.
 - 3) Introduction to various standards i.e. ISO/IEC:15408, ISO/IEC:24748-1, ISO: 27001, ISO: 27002, ISO 27019, IS 16335, IEC/ISO:62443.
 - 4) Training on implementation of ISO/IEC 27001 and awareness on IEC 62443.
 - 5) Vulnerability Assessment in the Critical System.
 - 6) Monitoring and preserving of electronic logs of access of Critical Assets.
 - 7) Detecting cyber-attacks on SCADA and ICS systems
 - 8) The handling of Critical System during cyber crisis.
 - 9) Action plans and procedures to recover or re-establish normal functioning of Critical Assets and access thereto following a Cyber Security Incident.
 - 10) Hands on SCADA operation at any of the Regional Load Dispatch Centre.
 - 11) Handling of risks involved in the procurement of COTS Products.
- d) All Personnel engaged in O&M of IT & OT Systems shall mandatorily undergo courses on cyber security of Power Sector from any of the training institute designated by CEA, immediately within 90 days from the notification of CEA Guidelines on Cyber Security in Power Sector.
- e) The Responsible Entity shall ensure that none of their newly hired or the current Personnel have access to the Critical System, prior to the satisfactory completion of cyber security training programme from the Training Institutes designated in India, except in specified circumstances such as cyber crisis or an emergency.
- f) NPTI in consultation with CEA shall identify and design domain specific courses on Cyber Security for different target groups. The “Governing Board for PSO Training and Certification” shall approve the content, duration etc of these courses and shall review it Annually. NPTI shall conduct these courses at all of their branches on regular basis and shall maintain the list of the Participants successfully completing the course.

Article 9 Cyber Supply Chain Risk Management

- a) The Responsible Entity shall ensure that, as and when Ministry of Power, Government of India notifies the Model Contractual Clauses on cyber security, these clauses are included in their every Bid invited for procurement of any ICT based components/equipments/System to be used for Power System.
- b) The Responsible Entity shall ensure that all the Communicable Intelligent Equipments and the Service Level Agreements (SLAs) for their Critical Systems shall be sourced from the list of the “Trusted Sources” as and when drawn by MoP/CEA.

- c) The Responsible Entity shall ensure that, in case, for the any Communicable Intelligent Devices, if no Trusted Source has been identified, then the successful bidder in compliance with the provisions made in MoP order dated 2.7.2020 and any other relevant MoP order has got the product cyber tested for any kind of embedded malware/Trojan/cyber threat and for adherence to Indian Standards at the designated lab.
- d) The Responsible Entity shall ensure that the essential cyber security tests are carried out successfully during FAT, SAT as detailed in **Annexure A**. The equipment/System besides for functionality shall also be tested in the factory for vulnerabilities, design flaws, parts being counterfeit or tainted, so as to minimize problems during on-site-testing and installation. Cyber Security Conformance Testing are to be carried out in the designated Lab as listed in **Annexure-I of MoP Order No. 12/13/2020-T&R dt. 8th June, 2021(Order at Annexure-B)**.
- e) The Responsible Entity shall ensure that the Equipment/System supplied by the successful bidder shall accompany with a certificate^{§, #} obtained by OEM from a certification body accredited to assess devices and process for conformance to IEC 62443-4 standards during design and manufacture. The Responsible Entity shall accept the certificate submitted along with the supplied Equipment/System only if it's in line with the Testing Protocol as notified by Ministry of Power, Government of India, from time to time.
- f) The Responsible Entity in compliance to the requirement of Article 9(e) shall also accept, till the setting up of an adequate certification facility in the India, a digitally signed self-declaration of conformance to the IEC 62443-4 standards during design and manufacture of the equipment/system, if submitted by the OEM.
- g) The Responsible Entity shall dispose all unserviceable or obsolete Communicable Intelligent Devices as per the procedure laid in their Cyber Risk Assessment and Mitigation Plans which shall be in line with the prevailing best practices.

§ The National & International certification may be specified in the tender for critical systems/sub-systems being procured by the Responsible Entity.

Certification Schemes:

Embedded Device Security Assurance Certification is for an individual product,
System Security Assurance Certification is for a set of products in a system (possibly from different vendors)

Security Development Lifecycle Assurance Certification is for the development processes that a manufacturer uses for developing products.

Article 10 Cyber Security Incident Report and Response Plan

- a) The CISO of the Responsible Entity shall report in the formats prescribed by CERT-In, all Cyber Security Incidents, classified as reportable events.
- b) Root cause analysis for all reportable events shall be carried out and corrective action taken, so as to ensure that any re-occurrence of such event can be managed with ease.
- c) The Responsible Entity shall mandatorily define in their Cyber Security Policy, criteria(s) identified on the basis of impact analysis, for declaring the occurrence of

Cyber Security Incident(s) as a Cyber Crisis in the System owned or controlled by them.

- d) The Responsible Entity shall mandatorily designate an Officer along with his/her standby by name and designation and empower them to declare an occurrence of the incident(s) as “Cyber Crisis”. The contact details of these Officers shall be updated in the C-CMP within 15 days of changes if any due to transfer or superannuation etc.
- e) The CISO shall ensure that during any Cyber Security Incident, ISD monitors and minutely records every details of cyber security events and incidents in both IT as well as the OT System owned or controlled by the Responsible Entity.
- f) The CISO shall ensure that each cyber incident is handled strictly as per Cyber Security Incident Response Plan detailed in the latest C-CMP approved by the Board of Directors.
- g) The Responsible Entity shall ensure that the efficacy of the Cyber Security Incident Response Plan is tested annually through mock drill(s) carried out, if feasible, as simulation exercise(s) or as table top exercise(s) with wider participation of their employees, in consultation with CERT-In and sectoral CERT. In case if any shortcoming is observed in the Cyber Security Incident Response Plan suitable changes shall be made in it.
- h) The Responsible Entity shall ensure that the CISO compiles details of incident detection, incident handling, learnings from each incident and damage claims made if any and shall report to CERT-In as well as upload information on ISAC-Power Portal.

Article 11 Cyber Crisis Management Plan(C-CMP)

- a) The Responsible Entity shall prepare a Cyber Crisis Management Plan and submit to their sectoral-CERT for review with intimation to Ministry of Power/CISO-MoP. Responsible Entity shall update their C-CMP on the basis of comments made by sectoral-CERT and then submit for vetting to CERT-In. The C-CMP shall be updated once again to include the observations made by CERT-In before seeking approval of Board of Directors for implementation of C-CMP.
- b) The Responsible Entity shall ensure that the C-CMP is reviewed at least annually. The CISO shall ensure that all changes are made in C-CMP only with the due approval of Board of Directors and the changes made in C-CMP have been communicated through a verifiable means to all the concerned Personnel of the Responsible Entity.
- c) The CISOs shall be the custodian of all the cyber security related documents including Cyber Crisis Management Plan, Risk Treatment Plan, Statement of Applicability of controls, and compliance to regulator’s requirement.
- d) The CISO shall be accountable for ensuring enforcement of C-CMP by Information Security Division of the Responsible Entity, during a cyber-crisis, as and when declared by the designated Officer. (refer Article 10(d))

Article 12: Sabotage Reporting%

- a) The Responsible Entity shall incorporate procedure for identifying and reporting of sabotage in their Cyber Security Policy within 30 days from issue of the Guidelines, or grant of licence under the appropriate legal provisions to the Responsible Entity.
- b) The CISO shall be held liable for non-reporting of identified sabotage(s) as per procedure laid for identifying and reporting of sabotage in the Cyber Security Policy of the Responsible Entity.

- c) The CISO shall prepare a detailed report on disturbances or unusual occurrences, identified, suspected or determined to be caused by sabotage in the Critical System of the Responsible Entity, and shall submit the report to the Sectoral CERT as well as to CERT-In within 24 hours of its occurrence.
- d) The CISO shall submit to NCIIPC within 24 hours of occurrence the report on every sabotage classified as cyber incidents(s) on "Protected System".
- e) The CISO upon occurrence on every sabotage shall take custody of all log records as well as digital forensic records of affected Cyber Assets, Intrusion Detection System, Intrusion Protection System, SIEM and shall preserve them for at least 90 days and shall make them available as and when called upon for investigation by the concerned Agencies.

%Disturbances or unusual occurrences, suspected or determined to be caused by sabotage.

Sabotage e.g. can be a forced intrusion in un-manned/manned facility and taking control of operation of Critical System through a communicating device.

Article 13 Security and Testing of Cyber Assets

- a) The Responsible Entity shall ensure security of all in-service phase as well as standby Cyber Assets through regular firmware/Software updates and patching, Vulnerability management, Penetration testing (of combined installations), securing configuration, supplementing security controls. CISO shall maintain details of update version of each firmware and software and their certification if received from OEMs.
- b) The Responsible Entity shall carry out regularly Vulnerability Assessment of all Cyber Assets owned or under their control. If a Cyber Asset is found vulnerable to any exploits or upon any patch updates or major configuration changes, then further Penetration Testing may be carried out offline or in a suitably configured laboratory test-bed to determine other vulnerabilities that may have not been identified so far.
- c) The Responsible Entity shall specify security requirement and evaluation criteria during each phase of their procurement Process.
- d) The Responsible Entity shall ensure that all Cyber Assets being procured shall conform to the type tests as mentioned in the specification for type testing listed in the bid document. Type test reports of tests conducted in NABL accredited Labs or internationally accredited labs (with in last 5 years from the date of bid opening) shall be mandated to be submitted along with bid. In case, the submitted Type Test reports are not as per specification, the re-tests shall be conducted without any cost implication to the Responsible Entity.
- e) The Responsible Entity shall ensure that all Communicable devices are tested for communication protocol as per the ISO/IEC/IS standards listed in **MoP Order No. 12/13/2020-T&R dated 8th June, 2021(Annexure-B).**
- f) The Responsible Entity shall ensure that all Critical Systems designed with Open Source Software are adequately cyber secured.
- g) The Responsible Entity as a best practise upon any incidence of Cyber Security Breach shall carry out cyber security tests at any lab designated for cyber testing by Ministry of Power. These tests shall be similar to Pre Commissioning Security Test and those essential for carrying out Post Incident Forensics Analysis.

Article 14 Cyber Security Audit

- a) The Responsible Entity shall implement Information Security Management System (ISMS) covering all its Critical Systems.
- b) The Responsible Entity shall through a CERT-In Empanelled Cyber Security OT Auditor shall get their IT as well as OT System audited at least once in every 6 (six) months and shall close all critical and high vulnerabilities within a period of one month and medium as well as low non-conformity before the next audit. Effective closure of all non-conformities shall be verified during the next audit.
- c) The Cyber Security Audit shall be as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335 and other guidelines issued by appropriate Authority if any. These mentioned standards shall be current with all amendments if any and in case if any standard is superseded, the new standard shall be applicable. CISO shall ensure immediate closure of non-conformance, based on the criticality and by means all non-conformances are to be closed before the next audit.
- d) The Responsible Entity shall ensure that CISO has all the required systems and documents in place, as mandated by NSCS for base line cyber security audit.

FAT & SAT

1. During FAT stage, the customer has to verify all types test reports / certificates including Communication protocol and security conformance tests of the devices offered for FAT.
2. FAT of SCADA involves testing as a whole system in the integrated scale down set up. For SCADA, Indian standard IS 15953: 2011 “SCADA System for Power System Applications” provides definition and guidelines for the specification, performance analysis and application of SCADA systems for use in electrical utilities (for transmission & Distribution) including guidance on Tests and inspections.
3. The SAT will be done at customer site as per the SAT document mutually agreed by buyer and supplier. For SAT also, guidance from IS 15953: 2011 need to be applied.
4. IEC 61850-10-3 Communication Networks and Systems For Power Utility Automation- Functional testing of IEC 61850 systems (in draft stage - CDTR) covers testing of applications within substations covering
 - a. A methodical approach to the verification and validation of a substation solution
 - b. The use of IEC 61850 resources for testing in Edition 2.1
 - c. Recommended testing practices for different use cases
 - d. Definition of the process for testing of IEC 61850 based devices and systems using communications instead of hard wired system interfaces (ex. GOOSE and SV instead of hardwired interfaces)
 - e. Use cases related to protection and control functions verification and testing.

This standard may be used as a guidelines for FAT & SAT for Substation Automation System (SAS) based on IEC 61850.

Annexure - B**Annexure – 1****List of designated laboratories for cyber security conformance testing****Table -A. Field Equipment /Operational Technology (OT)**

Sl. No.	Equipment	Communication Protocol Conformance Standards	Protocol Security Conformance Standards	Designated Laboratories
1	Remote Terminal Units (RTUs) & PLCs with IEC communications protocols	IEC 60870-5 -101 / IEC 60870-5 -104 (Test Details Annexure 2)	IEC 60870-5- 7 Security extension & IEC 62351 series (specifically IEC 62351-100 parts 1 & 3) (Test Details Annexure-2	Central Power Research Institute (CPRI), Prof Sir C V Raman Road, Sadashivanagar P O, Bengaluru – 560080, Karnataka
2	Intelligent Electronic Equipment / Numerical Protection Relays / Bay Control Units / Bay Protection Units, Gateways, Transformer Tap controller/ changer, etc. with IEC 61850 communication protocol	IEC 61850 – 5 to IEC 61850 – 10 (Test Details Annexure 2)		CPRI
3	Smart meters with IEC 62056 communication protocols	IEC 62056 series / DLMS & IS 15959 series and IS 16444 series (Test details Annexure 2)	IEC 62056 series / DLMS & IS 15959 series and IS 16444 series (Test Details Annexure 2)	1. CPRI 2. Electrical Research and Development Association (ERDA), ERDA Road, GIDC, Makarpura, Vadodara - 390 010 Gujarat 3. Yadav Measurements Pvt. Ltd. (YMPL) 373-375, RIICO Bhamashah Industrial Area Kaladwas 313003 Udaipur – Rajasthan

Information Technology (IT) Equipment (Main / Backup / Disaster recovery (DR) Control Centre / Substation control centre IT equipment)

All IT products procured /supplied shall have a valid Certificate of Common Criteria as per ISO/IEC 15408 issued by signatories of the Common Criteria Recognition Agreement (CCRA) (www.commoncriteriaportal.org).

Import/procurement/supplied from vendors sourcing from prior reference countries, the Certificate for Common Criteria shall be from Government Laboratories in India according to the IC3S scheme operated by Ministry of Electronics and Information Technology, which is a signatory to CCRA.

<https://www.commoncriteria-india.gov.in/>

Details of tests for various identified products

Remote Terminal Units (RTUs) (Sl. No. 1 of Table – A of Annexure – 1)

Test protocol:

Utilities / manufacturers will submit the sample along with all the required technical documentation for taking up testing to the designated laboratory.

Reference standards

- 1) IEC 60870-5-101 & IEC 60870-5-104 as applicable
- 2) IEC 60870-5-7 Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)
- 3) IEC 62351-100-1 & IEC 62351-100-3 and other cross referenced standards.

Test cases

Extract from standard (IEC 62351-100-1)

The conformance test cases are divided into four clauses:

- Clause 5: Verification of configuration parameters. This clause contains the configuration parameters affecting the message contents and/or the protocol behaviour.
- Clause 6: Verification of communication. The goal of this clause is to verify that Device Under Test (DUT) is able to implement the security extension messages as described in IEC TS 60870-5-7.
- Clause 7: Verification of procedures. The goal of this clause is to verify that DUT is able to execute the security extension procedures as described in IEC TS 62351-5.
- Clause 8: Test result chart. This clause contains the results of the test cases listed in Clauses 6 and 7 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables. They are numbered; their numbering syntax is: Subclause number (where the Table is located) + test case number.

In the column ‘reference’ each test case has a direct reference to IEC TS 62351-5 or IEC TS 60870-5-7 where the clause under test is defined.

Test cases are mandatory depending on the description in the column ‘Required’. The following situations are possible:

M= Mandatory test case. The test is referencing a clause that is mandatory in IEC TS 62351-5 or IEC TS 60870-5-7.

Protocol Information Conformance Statement (PICS) x, x = Mandatory test case if the functionality is enabled in the PICS (by marking the applicable check box), with a reference to the section number of the PICS (x.x).

Conformance testing of security extension procedures

The security extension procedures can be summarized as follows:

- User management
- Update key maintenance
- Session key maintenance
- Challenge/Reply authentication
- Aggressive Mode authentication

Extract from standard (IEC 62351-100-3)

IEC 62351-3 defines the requirements related to the authentication/encryption protocol, procedures and methods to be implemented at TCP/IP (transport) level.

The conformance test cases are divided into three clauses:

- Clause 5: Verification of configuration parameters. This clause contains the parameters specified by the standards referencing IEC 62351-3 (see IEC 62351-3:2014/AMD1:2018, Clause 7) and affecting the protocol behaviour.
- Clause 6: Verification of IEC 62351-3 requirements. The goal of this clause is to verify that DUT is conformant to the requirements of the IEC 62351-3.
- Clause 7: Test result chart. This clause contains the results of the test cases listed in Clause 6 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables. They are numbered, their numbering syntax is: Subclause number (where the table is located) + test case number.

In the column 'Reference' each test case has a direct reference to IEC 62351-3 where the clause under test is defined. PICS or Protocol Implementation eXtra Information for Testing (PIXIT) could be found in the "Reference" column for some test cases whenever the execution of the test case shall take into account specific parameter values declared in the PICS or PIXIT of the DUT.

Test cases are mandatory depending on the description in the column 'Required'. The following situations are possible:

M = Mandatory test case. The test is referencing to a clause that is mandatory in IEC 62351-3.

PICS

or

PIXIT = Mandatory test case if the functionality is enabled in the PICS or PIXIT by marking the applicable check box or declaring the applicable value.

Intelligent Electronic Devices (IEDs) (Sl. No. 2 of Table – A of Annexure – 1)

Utilities / manufacturers will submit the sample along with all the required technical documentation for taking up testing to the designated laboratory.

Reference standards

IEC 61850 series

Specifically IEC 61850-5, IEC 61850-6, IEC 61850-7, IEC 61850-8, IEC 61850-9 and IEC 61850-10

Test cases

Communication protocol conformance as per IEC 61850 -10. This part of standard defines methods and abstract test cases for conformance testing of client, server and sampled values devices used in power utility automation systems, the methods and abstract test cases for conformance testing of engineering tools used in power utility automation systems, and the metrics to be measured within devices according to the requirements defined in IEC 61850-5. Further this part of standard specifies standard techniques for testing of conformance of client, server and sampled value devices and engineering tools, as well as specific measurement techniques to be applied when declaring performance parameters. The use of these techniques will enhance the ability of the system integrator to integrate IEDs easily, operate IEDs correctly, and support the applications as intended.

Smart Meters (Sl. No. 3 of Table – A of Annexure – 1)

Utilities / manufacturers will submit the sample along with all the required technical documentation for taking up testing to the designated laboratory.

IEC 62056 series of standards (Electricity metering data exchange – The DLMS/COSEM suite) specifies details of communication protocol requirements, conformance testing and security requirements. The Part 5-3 (DLMS/COSEM application layer) specifies the DLMS/COSEM application layer in terms of structure, services and protocols for DLMS/COSEM clients and servers, and defines rules to specify the DLMS/COSEM communication profiles. It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-6-2 using either logical name (LN) or short name (SN) referencing.

Clause 5 and sub clauses specifies security requirements. It cover security concepts, Identification and authentication, Cryptographic algorithms, Cryptographic keys – overview, Key used with symmetric key algorithms, Keys used with public key algorithms and Applying cryptographic protection.

Note: All above referred standards shall be latest with amendments if any at the time of submission of sample(s) for testing.

Testing Criteria

1) Supply from Trusted Sources

The sample size shall be as specified by CEA as per the approved criteria for Trusted Vendors

2) Supply from other than trusted vendors

The sample size shall be shall be 5% of the supply lot / ordered quantity (minimum one). The manufacturer shall submit request to the Nodal agency along with vendor's / manufacturer's certifications for supply chain management system practices and secure product development process implementations based on any one or more of standards ISO / IEC 27036, ISO / IEC 20243, IEC 62443 for verification.

After scrutiny of vendor's / manufacturer's certifications the supplier / utilities shall be asked to submit product to the designated laboratory for communication and cyber security conformance testing.

The supply lot shall stand rejected on failure to comply with the test requirements.

3) Supply from prior reference countries

The utility shall obtain prior permission from the Government of India for importing the product / system from prior reference countries.

The sample size shall be shall be 10 % of the supply lot / ordered quantity (minimum one). The manufacturer shall submit request to the Nodal agency along with vendor's / manufacturer's certifications for supply chain management system practices and secure product development process implementations based on any one or more of standards ISO / IEC 27036, ISO / IEC 20243, IEC 62443 for verification.

After scrutiny of vendor's / manufacturer's certifications the supplier / utilities shall be asked to submit product to the designated Government / Government controlled Autonomous laboratory for type tests (Annexure – 4) and communication & cyber security conformance testing.

The supply lot shall stand rejected on failure to comply with the test requirements.

Type Tests

Products imported from prior reference countries shall also undergo type testing as per following standards in addition to communication protocol and security conformance testing at the designated Government / Government controlled Autonomous laboratory:

Type test standards for RTUs

1. IEC 60870-1-2:1989 Telecontrol equipment and systems. Part 1: General considerations. Section Two: Guide for specifications.
2. IEC 60870-2-1:1995 Telecontrol equipment and systems - Part 2: Operating conditions - Section 1: Power supply and electromagnetic compatibility.
3. EC 60870-2-2:1996 Telecontrol equipment and systems - Part 2: Operating conditions -Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences).
4. IEC 60870-3:1989 Telecontrol equipment and systems. Part 3: Interfaces (electrical characteristics)

Type test standard for IEDs / Numerical Protection Relays / Bay controls units

1. IEC 61850-3: 2013, Ed. 2 Communication networks and systems for power utility automation – Part 3: General requirements.

Type test standards for Smart meters

1. IS 16444: 2015 AC static direct connected watthour smart meter class 1 and 2 – Specification.
2. IS 16444 Part 2: 2017 AC static transformer operated watthour and var - Hour smart meters, class 0.2 S, 0.5 S and 1.0 S: Part 2 specification transformer operated smart meters.

Note:

1. All above referred standards shall be latest with amendments if any at the time of submission of sample(s) for testing.
2. Type tests generally covers functionality, environmental, mechanical, EMI/ EMC and electrical safety related tests.