

<<Name of Organisation>>

Standard Operating Procedure (SoP) for Cyber-Security

CONFIDENTIALITY CLAUSE

This document is the property of [redacted]. All ideas and information contained within the document is the intellectual property of [redacted]. These documents are not for general distribution and are meant for use solely by the person/persons to whom it is specifically issued to or shared with. [redacted] does not share this document with any third party or vendor unless specifically exempted by the competent authority. Copying or unauthorized distribution of these documents, in any form or means including electronic, mechanical, photocopying or otherwise is illegal.

CONTACT INFORMATION

For any question regarding this policy, please contact -
Email:

DOCUMENT CONTROL

Document Version Control Note	
Name of the Document	SoP for Cyber Security
Document Version Number	XX
Effective Date	XX.XX.XXXX
Approved By	XXXX
Document Classification	Restricted
Distribution List	CISO, ISMs, Nominated Members of <<Organization Name>>, Vendors / third parties and Service providers
Access Level	Read Only

REVISION HISTORY

Version	Release Date	Prepared By	Reviewed/ Approved By



Table of Contents

1	Introduction.....	5
2	Purpose	5
3	Scope and Applicability	5
4	Standard Operating Procedures (SoP) for Cyber-Security.....	6
5	Change, Review and Update	13
6	Standard Operating Procedure Templates	14



1 Introduction

<<Organisation Name>> handles critical IT and OT infrastructure which includes assets, applications, important data, information systems and processes for electricity transmission. <<Organisation Name>> infrastructure is classified as critical infrastructure by the Government and there are many periodic advisories issued by various government agencies. It is important to follow cyber security standard operating procedures in <<Organisation Name>> to protect critical infrastructure. It is important and mandatory for employees and associated vendors/ third-parties or any interested party to adhere to best industry practices and cyber security SOP to maintain standard operational method throughout <<Organisation Name>>.

2 Purpose

The main purpose of this SOP is to ensure mandatory cyber security practices and best industry practices are followed. This SOP is should be implemented for <<Organisation Name>>.

3 Scope and Applicability

The procedure written in this document is applicable to all <<Organisation Name>> employees, vendors/third parties/service provides and contractors as per applicability of cyber security procedures and recommendations by CISO. This SOP is applicable for <<Organisation Name>>.



4 Standard Operating Procedures (SoP) for Cyber-Security

Procedure for Organization is as follows:

Sr. No.	Activity	Responsible
1.	Define the security goals, objectives, scope, and boundaries of information security program <i>(Refer Annexure 5)</i>	Cyber Security Team
2	Define minimum baseline security standard applicable to all installed Cyber assets and evaluate the same periodically for any change/upgradation of base line. Ensure all new procurements of Cyber asset are in compliance with minimum base line identified. The Minimum base lines should be part of the standard specifications of all such procurement made by the constituents.	CISO
3.	Estimate budget and resources required to develop and maintain a resilient and robust cyber system	CISO
4.	Define information security measurement metrics and other key performance indicators. <i>(Refer Annexure 6)</i>	Cyber Security Team
5.	A formal process should be followed for creating, documenting, reviewing, updating, and implementing security policies, procedures, plans, guidelines and processes.	ISMs & Cyber Security Team
6.	Disseminate information security policies, procedures and guidelines to all concerned personnel including management, employees, contractors, sub-contractors and other stakeholders	CISO
7.	Define roles and responsibilities of the key personnel of the Organization for ensuring implementation of policies and guidelines of information security. <i>Please Refer Annexure-7 for Roles and Responsibilities of CISO</i>	CISO
8.	Enforce and oversee implementation of approved information security policies, procedures, plans, guidelines and ISMS as per ISO-27001.	CISO
9.	Ensure that information security considerations are integrated with IT and OT system planning, development & acquisition life cycle.	ISMs, <<Organisation>> Nominated members



Sr. No.	Activity	Responsible
10.	Identify Critical Information Infrastructure (CII) based on following parameters but not limited to: <ol style="list-style-type: none"> 1. Functionality: It may be viewed at two levels-Functional uniqueness and Functional Dependency. 2. Criticality Scale: It can involve factors such as the availability, delivery, access, and consummation of essential services. 3. Degree of Complementarities: It considers that how various systems in an organization are complementing each other. 4. Time duration: It is important because it may happen that not all systems are always critical and all circumstances and there may be time slots in which they are critical. 	CISO, ISMs, <<Organisation>> Nominated members
11.	Classify all documents as 'Top Secret', 'Confidential', 'Restricted' and 'Public'. A document which has been classified as 'Top Secret' is to be treated as the most critical document in <<Organisation>>. Also, the appropriate documents must be stored in a secure manner.	CISO, ISMs, <<Organisation>> Nominated members
12.	Implement Segregation of Duties (SoD) to reduce conflicts of duties and interests	ISMs, <<Organisation>> Nominated members
13.	Identify and allocate a dedicated team for asset and inventory management, with clear roles and responsibilities.	CISO and ISMs
14.	Periodically evaluate and review effectiveness of information security policies, procedures, standards, plans, guidelines and processes etc.	CISO
15.	Issue alerts and advisories with respect to new vulnerabilities/threats to all concerned personnel, departments, and inform other related organizations	CISO
16.	Perform Risk Assessment and based on analysis perform risk mitigation on regular basis.	CISO, ISMs and Cyber Security Team
17.	Document any non-compliance within a stipulated time frame as deemed fit by <<Organisation>>. A valid reason in the	ISMs and Cyber Security Team



Sr. No.	Activity	Responsible
	documentation for not complying with cyber security policies, plans, procedures, guidelines, standards, processes etc.	
18.	Approve any exception and noncompliance with justification and submit to the senior management.	CISO
19.	Share information related to critical information security incidents and breaches with associated reporting organizations.	CISO
20	Raise information security awareness among management, employees, contractors, subcontractors, and other stakeholders. Provide Cyber Security Training to all persons engaged in O&M of IT and OT Systems as per Article 8 of CEA (Cyber Security in Power Sector) guidelines 2021.	CISO
21.	Coordinate and ensure implementation of a Business Continuity Plan (BCP). Periodically conduct mock drills to evaluate the effectiveness of the Business Continuity Plan	CISO, ISMs, <<Organisation>> Nominated members
22.	Ensure compliance of information security by contractors/suppliers/sub-contractors etc.	ISMs, <<Organisation>> Nominated members
23.	Ensure all information systems with the Organization are adequately patched and updated. Evaluate compliance with respect to legal and regulatory requirements for information security.	ISMs, <<Organisation>> Nominated Members Nominated Members of Third parties, vendors or service providers
24.	Perform Cyber security audit bi-annually from CERT-In empaneled auditor and prepare Cyber security audit report along with recommendations for improving Cyber security and present to senior management.	ISMs and Cyber Security Team
25.	Ensure closure of reported audit observations	ISMs, <<Organisation>> Nominated members, Nominated Members of Third parties, vendors or service providers



Sr. No.	Activity	Responsible
26.	Send a copy of the audit report periodically to regulatory bodies and senior management as required.	CISO
27	Ensure that CEA (Cyber Security in Power Sector) guidelines 2021 and amendments thereof, if any is being followed by the Organization. <i>Please Refer Annexure -8 for the CEA (Cyber Security in Power Sector) guidelines 2021</i>	CISO

Procedure for Incident Response:

Sr. No.	Activity	Responsible
1.	Notify any suspicious event or incident to respective ISM or incident management team. Incident information may be received from the following sources: <ul style="list-style-type: none"> • Call • Email 	All User/Employees/ Contract employees/ Vendors
2.	<u>Incident Logging</u> Initiate Incident Management Process and log or record the incident when there is a disruption of any IT or OT services, or any suspicious incident reported by any user.	Incident Management Team
3.	<u>Classification</u> Classify the incident based on probable Impact and Urgency of the incident. Decide Priority for incident repose as per Impact-Urgency matrix.	Incident Management Team
4.	<u>Assign Ownership</u> Assign logical ownership to the Incident logged. The Assignment could be self or to any individual of team to have the incident resolved at the earliest.	Incident Management Team
5.	a. <u>Reporting to CERT-IN and Regulatory Authorities:</u> The incident to be reported to CERT-In within 6 hours of noticing such incidents or being brought to notice about such	Incident Management Team



Sr. No.	Activity	Responsible
	<p>incidents as per the directives of CERT-IN and CEA Guidelines.</p> <p>The incident also to be reported to respective Sectoral CERT and Regulatory Authorities</p> <p><i>Please Refer Annexure -9 for the directives of CERT-IN.</i></p> <p><i>Please Refer Annexure -10 for the CERT-IN incident report form.</i></p> <p>b. <u>Communicate/Inform Stakeholders</u></p> <p>Inform/Report users, interested parties, senior management and service providers about logged incident, its priority and assignee details. Periodically communicate status of incident with stakeholders-based on priority.</p>	
6.	<p><u>Matching the Incident</u> Match the incident against below parameters once the incident is assigned to the appropriate team.</p> <p><u>Parameters:</u></p> <ul style="list-style-type: none"> • Incident Records • Problem Records • Change Records • Known Error Database. <p>The incidents can be matched based on the symptoms of the incident recorded.</p>	Incident Management Team
7.	<p><u>Check whether resolution available from KEDB</u> The technical staff checks in the Knowledge database for any solution provided for similar Incidents.</p> <p>If solution exist move to step 9 else step 8.</p>	Incident Management Team
8.	<p><u>Investigation</u> Analyse and investigate incident in detail and to take up suitable measures to limit the spread of the incident ensuring the spread is limited on to the affected system. Search for best possible resolution. Suitable checklist to be referred for incident which are known and mitigation measures identified earlier.</p> <p>After determining that there is no resolution available, it is necessary to escalate functionally/hierarchically and transfer</p>	Incident Management Team and relevant IT and OT teams

Sr. No.	Activity	Responsible
	<p>the incident from existing line of support (L1 to L2 and then to L3).</p> <p>The relevant team to investigate and diagnose the issue and look for a work around. Evidences should be collected during investigation and preserved for future reference.</p>	
9.	<p><u>Provide Resolution</u></p> <p>The objective of the Incident Management is to restore services as soon as possible, hence it is important to provide a resolution. The resolution provided could either be a workaround / temporary fix or a permanent change (New/Update) for resolving the Incident.</p> <p>After resolution, status should be set to Resolved.</p>	Incident Management Team and relevant IT and OT teams
10.	<p><u>Review</u></p> <p>Based on the solution provided, it is necessary to know if the solution provided is effective or not. Based on the review of resolution and decisions taken, the following actions might be taken:</p> <ul style="list-style-type: none"> • Suspend an Incident Resolution • Cancel an Incident • Reopen an Incident • Close an Incident 	Incident Management Team
11.	<p><u>Close Incident Ticket</u></p> <p>Close incident only after review. Ensure that the resolution details are recorded correctly, and the incident is resolved.</p> <p>Before closure of ticket ensure sufficient monitoring time of the affected system and effectiveness of the deployed resolution.</p>	Incident Management Team
12.	<p><u>Communicate Closure</u></p> <p>Create a detailed RCA/Technical investigation report (TIR) for the incident and ensure the same is communicated to all relevant stake holders including Incident Management team members.</p> <p>Inform all users, interested parties, senior management and service providers about resolution.</p> <p>Track the resolution time and same to be taken up for improvement in future.</p> <p>Ensure learnings from Incident are shared with all stakeholders</p> <p><i>Refer Incident Report Form Annexure 2</i></p>	Incident Management Team



Procedure for Threat Advisory Compliance:

Sr. No.	Activity	Responsible
1.	Receive Threat advisories, assessment reports and recommendations from nodal agencies such as Cert In, Sectoral Cert, NCIIPC and other third-party advisors.	CISO
2.	E-Mail threat advisories, reports and recommendations to respective ISMs and internal nominated members of <<Organisation>> Please refer Annexure-3 & 4 for Nominated members of <<Organisation>> and Vendors/Third Parties.	CISO
3.	Receive and identify applicable threat advisories and record them in compliance tracker. Please refer Annexure-1 for Threat Advisory Compliance Tracker	ISMs, <<Organisation>> Nominated members
4.	Implement threat advisories and recommendations if applicable threat advisories to <<Organisation Name>> employees and record compliance in compliance tracker.	ISMs, <<Organisation>> Nominated members
5.	In case of Vendor specific advisories or recommendations or third-party dependencies then forward threat advisories, recommendations and reports to relevant Nominated Members of vendors/ third parties or service providers and record details in compliance tracker.	ISMs, <<Organisation>> Nominated members
6.	Implement received applicable threat advisories and recommendation received from ISM and <<Organisation>> Nominated Members within stipulated timeframe.	Nominated Members of Third parties, vendors or service providers
7.	Share compliance and evidence against received threat advisories and recommendations with ISM and <<Organisation>> Nominated members within stipulated timeframe.	Nominated Members of Third parties or vendors or service providers
8.	Forwarding compliance and evidences received from third parties or vendors or service providers to CISO and Record compliance in compliance tracker	ISMs, <<Organisation>> Nominated members
9.	Sending Consolidated Compliance to respective government agencies such as Cert-IN, Sectoral Cert, NCIIPC and other third-party advisors.	CISO



Sr. No.	Activity	Responsible
10.	Quarterly Review of status of compliance of threat advisories, compliance tracker and discuss issues and improvement opportunities with ISMs, nominated members of <<Organisation>>, Nominated Members of Vendors / Third parties / Service providers.	CISO
11.	Quarterly Reporting of status of compliance of threat advisories and discuss issues, if any with Higher Authority of <<Organisation>>	CISO

5 Change, Review and Update

This procedure shall be reviewed once every year unless the <<Organisation Name>> considers an earlier review necessary to ensure that this procedure remains current. Changes to this procedure shall be approved by CISO and senior management of <<Organisation Name>>.



6 Standard Operating Procedure Templates

S. No.	Document Name	Document
1.	Threat Advisory Compliance Tracker	 Threat Advisory Compliance Tracker.xl
2.	Incident Report	 Incident Reporting Form.docx
3.	Nominated Members of <<Organisation Name>>	 Nominated Members of Organisation Name
4.	Nominated Members of vendors / Third parties	 Nominated Members of vendors or Third parties
5.	Scope, Objectives & Goals of Information Security Program	 Annexure Scope Objective and Goals.docx
6.	Security measurement metrics and other Key Performance Indicators	 Security Measure Matrices and KPIs
7.	Roles and Responsibility of CISO (as per CERT-IN)	 Roles and Responsibilities of CISO
8.	CEA (Cyber Security in Power Sector) guidelines 2021.	 Guidelines_on_Cyber _Security_in_Power_Sector
9.	The directives of CERT-IN	 CERT-In Directives 28.4.22.pdf
10.	The CERT-IN incident report form.	 The CERT-IN incident report form.pdf



<<Organisation Logo>>										
Threat Advisory Compliance Tracker										
Sr. No.	Threat Advisory/ Assessment Report Name	Description	Date Received	Expected Compliance Date	Applicability	Compliance Status	Actual Compliance Date	Reason for Delay in Compliance (if any)	Evidences	Remarks
1					Yes/NO/Partial	Completed/In progress/Shared with Vendors for Compliance				
2										
3										
4										
5										
6										
7										
8										
9										
10										





Incident Reporting Form			
General Information			
Incident Report No.		Incident Priority	
Date and Time of Incident		Date and Time of Incident Resolution	
Reported By			
Place / Location of Incident			
Description of Incident			
Any Immediate Action Taken			
Permanent Resolution of the Incident			
Root Cause Analysis (if any)			
Recommendation			
Prepared By		Remarks	
Approved By		Approval Date	





Nominated Members of <<Organisation Name>> for Threat Advisory Compliance (Annexure-3)									
Sr. No.	Application / Infrastructure	Section	Name	Designation	Mobile		Email		Remarks
					Primary	Secondary	Primary	Secondary	
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									





Nominated Members of Vendors / Service Providers for Threat Advisory Compliance (Annexure-4)									
Sr. No.	Application No. /Infrastructure	Name	Designation and Company	Mobile Primary	Secondary	Email Primary	Secondary	Remarks	
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									





Annexure – 5

Scope & Applicability of Information Security Program

The Information Security Policies and SOP for Cyber Security applies to all information assets, IT and OT systems for <<Name of Organisation>>.

<<Name of Organisation>> employees, contractors, third party staff or any other partners who are directly or indirectly a part of <<Name of Organisation>> ecosystem and have access to <<Name of Organisation>> systems, processing facilities shall adhere to this policy and ensure compliance.

Goals of Information Security Program

The main goal of information security is to ensure:

- Confidentiality – The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity – Property of accuracy and completeness. Business critical information and systems remains accurate, error-free, and without omissions.
- Availability– Property of being accessible and usable upon demand by an authorized entity. i.e Authorized users have access to critical information and systems when required

Objectives of Information Security Program

<<Name of Organisation>> shall establish information security objectives at relevant functions, departments and levels. The information security objectives shall be measurable, consistent with the information security policy and consider applicable information security requirements, and results from risk assessment and risk treatment. These objectives shall be communicated and updated as appropriate.

The following key ISMS objectives are as follows:

- To ensure Confidentiality, Integrity and Availability of the information, IT and OT systems and processing facilities by establishing requisite controls.
- To create an information security culture, <<Name of Organisation>> should ensure information security awareness is spread amongst all interested parties.
- To ensure information security controls are considered during all stages of Service delivery
- To ensure established information security controls are followed.
- To ensure ongoing information security incident management.
- To comply with applicable legal, regulatory and contractual obligations.



- To ensure ongoing effectiveness of ISMS.

To meet the above information security objectives & goals, <<Name of Organisation>> shall establish, operate and maintain ISMS with defined scope and boundaries. The objectives need to be periodically reviewed and updated based on the information security requirements, results from risk assessment, risk treatment, recent incidents, audits or a change in policy/scope.

The established ISMS will be aligned with the requirements of the ISO 27001:2013 standard and leading practice guidelines, and follows the following guidelines to structure all ISMS related policies and procedures affected by the ISO 27001:2013 standard.

Standard Protocol

<<Organisation Name>> shall identify and document all applicable legal, statutory, regulatory and contractual requirements for maintaining information security of the organisation. <<Organisation Name>> must ensure compliance to each of the Laws and Acts relevant to its operations, wherever applicable. These will include but not limited to the Information Technology (IT) Act, CERT-IN guidelines or any other laws or acts applicable to the organization.

<<Organisation Name>> shall identify and protect its Intellectual Property Rights (IPRs). <<Organisation Name>> shall ensure that terms and conditions and license requirements of the copyrighted software or any other proprietary information used within the <<Organisation Name>> are complied with.

<<Organisation Name>> shall ensure that organizational important records relating to Information Security must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

<<Organisation Name>> shall ensure that data protection and privacy of personal information of the stakeholders must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. <<Organisation Name>> shall prevent any misuse of information processing facilities and systems. All information and systems must be used as per acceptable usage policy and guidelines. Disciplinary action may be taken for any wilful violation to the policies.

Cryptographic controls, wherever applicable, shall be used in compliance with all relevant agreements, laws, and regulations. <<Organisation Name>> management shall ensure that all security procedures are carried out correctly to achieve compliance with security policies and standards. Agreements with the third parties must specify the mandate for them to comply with the <<Organisation Name>> security policies and procedures.

<<Organisation Name>> shall ensure that periodic compliance review & reporting shall be conducted to verify that systems and process are compliant with the security policies and standards. Findings and recommendations in the report must be communicated to CISO for implementation. <<Organisation Name>> information processing resources must be reviewed by an independent third-party at least on an annual basis. The findings must be reported to senior management.

<<Organisation Name>> shall conduct internal and external information security audits by competent independent internal and external auditor respectively to ensure compliance with the information security policies, procedures, standards and guidelines. Formal procedures must be developed for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action. All corrective actions shall be documented and tracked to ensure continual improvement.

Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimize the risk of disruptions to organizational processes. Access to information systems audit tools must be protected to prevent any possible misuse or compromise.



Annexure - 6

Security Measurement Matrices and Key Performance Indicators

Security Measurement Matrices

- **Identify your data needs:** Once we know what questions are trying to answer, we will define SC data needs to establish what KPIs, metrics or data need to answer those questions.

Sr. No.	Metric	Description	Score / Value
1	Asset Capacity (AC)	The (remained) capacity of a cyber asset (after being attacked or compromised)	[0, 1]: 0 means not operational; 1 means fully operational
2	Average Length of Attack Paths (ALP)	The average effort to penetrate a network, or compromise a system/ service; evaluated by attack graph	n: the average length of potential attack paths
3	Compromised Host Percentage (CHP)	The percentage of compromised hosts in a network at time t	[0, 1]: 0 means no compromise; 1 means all compromised
4	Exploit Probability (EP)	How easy (or hard) to exploit a vulnerability? Could be measured by Common Vulnerability Scoring System (CVSS) exploitability sub-score	[0, 1]: 0 means hard to exploit; 1 means easy to be exploited
5	Impact Factor (IF)	The impact level of a vulnerability after being exploited, could be measured by Common Vulnerability Scoring System (CVSS) impact sub-score	[0, 1]: 0 means no impact; 1 means totally destroyed
6	Number of Attack Paths (NAP)	The number of potential attack paths in a network, could be evaluated based on attack graphs	n: the number of potential attack paths
7	Network Preparedness (NP)	Is a network ready to carry out a mission? E.g., all required services are supported by available cyber assets	[0, 1]: 0 means not ready; 1 means fully ready
8	Network Resilience (NR)	The percentage of compromised systems/services that can be replaced/recovered by	[0, 1]: 0 means cannot recover; 1 means can be fully recovered



		backup/alternative systems/services	
9	Operational Capacity (OC)	The (remained) operational capacity of a system/service (after being affected by a direct attack or indirect impact)	[0, 1]: 0 means not operational; 1 means fully operational
10	Resource Redundancy (RR)	Is there any redundant (backup) resources assigned or allocated for a critical task/operation?	0 or 1: 0 means no backup system; 1 means at least 1 backup system
11	Service Availability (SA)	The availability of a required service to support a particular mission, task, or operation	0 or 1: 0 means not available; 1 means service is available
12	Shortest Attack Path (SAP)	The minimal effort to penetrate a network, or compromise a system or service, evaluated by attack graphs	n: the shortest length of potential attack paths
13	Severity Score (SS)	The severity/risk of a vulnerability if it was successfully exploited, could be measured based on Common Vulnerability Scoring System (CVSS) score	[0, 1]: 0 means no risk; 1 means extremely high risk
14	Vulnerable Host Percentage (VHP)	The percentage of vulnerable hosts in a network	[0, 1]: 0 means no vulnerable host; 1 means all hosts are vulnerable

Illustrative list of key Performance

User access and account monitoring	Log collection, analysis and archiving	User awareness level
Number of data access requests	Data risks identified	Events by root cause
Data classification trends	Regulatory compliance level	Cost per Incident
Mean-Time-to-Detect & Mean-Time-to-Respond	Number of data breaches	Number of data security incidents
Cybersecurity Framework non-compliance level	National Information Assurance non-compliance level	Data Privacy Law non-compliance level
General Data Protection Regulation (GDPR) non-compliance level	ISO 27001:2013 non-compliance level	ISO 27701:2019 non-compliance level



Top policy violators (by individual or group)	Resource utilization	Incident handling efficiency
---	----------------------	------------------------------

Key Performance Indicators:

Sr. No.	Indicators	Descriptions
1	Level of preparedness	How many devices on your network are fully patched and up to date?
2	Unidentified devices on the internal network	Your employees bring their devices to work, and your organization may be using Internet of Things (IoT) devices that you're unaware of. These are huge risks for your organization as these devices are probably not secure. How many of these devices are on your network?
3	Intrusion attempts	How many times have bad actors tried to breach your networks?
4	Mean Time Between Failures (MTBF)	How much time exists between system or product failures when looking to determine reliability?
5	Mean Time to Detect (MTTD)	How long do security threats fly under the radar at your organization? MTTD measures how long it takes for your team to become aware of a potential security incident.
6	Mean Time to Acknowledge (MTTA)	What is the average time it takes you to begin working on an issue after receiving an alert?
7	Mean Time to Contain (MTTC)	How long does it take to contain identified attack vectors?
8	Mean Time to Resolve (MTTR)	How long does it take your team to respond to a threat once your team is aware of it?
9	Mean Time to Recovery (MTTR)	How long does it take your organization to recover from a product or system failure?
10	Days to patch	How long does it take your team to implement security patches? Cybercriminals often exploit lags between patch releases and implementation.
11	Cybersecurity awareness training results	Who has taken (and completed) training? Did they understand the material?
12	Number of cybersecurity incidents reported	Are users reporting cybersecurity issues to your team? That's a good sign because it means the employees and other stakeholders recognize issues. It also means your training is working.
13	Security ratings	Often the easiest way to communicate metrics to non-technical colleagues is through an easy-to-understand score. Security Score card's security ratings give your company an A-F letter grade on 10 security categories (network security, DNS health, patching cadence, cubit score, endpoint security, IP reputation, web application security, hacker chatter, leaked credentials, and social engineering). Based on these 10 factors, you're then assigned an overall grade, so you and your colleagues can see



		at a glance how secure your company is relative to the rest of your industry.
14	Access management	How many users have administrative access?
15	Security Policy compliance	How well are you tracking and documenting exceptions, configurations, and compliance controls?
16	Cybersecurity awareness training	How well are you maintaining documentation for your cybersecurity awareness training? Are you including all members of your organization, including senior executives?
17	Non-human traffic (NHT)	Are you seeing a normal amount of traffic on your website or is there an uptick that indicates a potential bot attack?
18	Virus infection monitoring	How often does your antivirus software scan common applications such as email clients, web browsers, and instant messaging software for known malware?
19	Phishing attack success	What is the percentage of phishing emails opened by end-users?
20	Cost per incident	How much does it cost to respond to and resolve an attack? How much money are you spending on staff overtime, investigation costs, employee productivity loss, and communication with customers?



INDIAN-COMPUTER EMERGENCY RESPONSE TEAM
Ministry of Electronics and IT
Government of India

No. 6(12)/2017-PDP-CERT-In

Dated: 14/03/2017

Ref: Ministry of Electronics and IT letter No. 1(1)/2017-CLES dated 13/2/2017

Sub: Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations

1. CISO to be appointed in each Ministry/Department/Organisation

- 1.1 With the rapid digitalisation of functions and processes of Government/Government organizations, the need for adopting secure cyber practices is becoming extremely important. A cyber breach can cause severe financial damage, bring the functioning of Government/Government organisation to standstill. It is therefore imperative, that every organisation involved in the use of Information Technology in the discharge of its functions must identify and document its Information Security (IS) requirements that arise from various sources including the following sources:
- (a) An assessment of risks (RA) to the organisation in the context of the organisation's business strategy and objectives; through which threats to an organisation's information assets are identified, vulnerabilities and likelihood of occurrence are evaluated and their potential impact is estimated;
 - (b) The legal, statutory, regulatory and contractual requirements that an organisation, its trading partners, contractors and service providers have to fulfil;
 - (c) The set of principles, objectives and business requirements for Information handling, processing, storing, communicating and archiving that are developed for Operations Support in an organisation.
- 1.2 Organisations must identify and implement an **Information Security Management System (ISMS)** that encompasses Cyber Security as well as physical and logical security controls for risk mitigation as appropriate, to protect the organisation from



business harm resulting from information security issues or cyber crises.

- 1.3 To ensure a structured mechanism, in accordance with best information security system practices, the Ministry of Electronics and IT has advised all Ministries/Departments to nominate a Chief Information Security Officer (CISO) for the Ministry/Department and also advise similar action to Chief Executives/Heads of Government organizations including PSUs/Autonomous Bodies/Attached Offices/ Statutory Bodies under their control. It shall be the responsibility of Secretary of the Ministry/Department (CEO/Head in case of organizations) to identify a member of senior management as a 'Chief Information Security Officer (CISO)' to establish a cyber security program, coordinate security policy compliance efforts across the organisation and interact regularly with CERT-In 'Point of Contact'.
- 1.4 The CISO must be given the mandate and resources to establish an Information Security program, coordinate security policy compliance efforts across the organisation and interact regularly with regulatory agencies such as CERT-In.
- 1.5 The CISO shall preferably report to the Secretary of the Ministry/Department (CEO/Head in case of organisations). If for some reason, that is not possible, CISO must report directly to next seniormost person in the Ministry/Department (CEO/Head in case of organisations)
- 1.6 The Ministry hereby issues a charter of roles and responsibilities for the CISOs so appointed. It shall be the duty of CISO to undertake the functions assigned herein with respect to cyber activities of his Ministry/Department/organization. The performance appraisal of the CISO may take these responsibilities into account while assessing the performance of the officer.

2. Roles and Responsibilities of CISOs

CISOs shall, inter alia, be responsible for the following:

- 2.1 Maintaining and updating the threat landscape for the organisation on a regular basis including staying up to date about the latest security threat environment and related technology developments.
- 2.2 Establishing a cyber security program and business continuity programme and for drafting of various security policies e.g., Information security policy, Data



governance and classification policy, Access control policy, Acceptable use of assets and asset management, Risk assessment and risk treatment methodology, Statement of Applicability, Risk management framework including third parties, Cryptography, Communications security, Information Security awareness programs for all personnel in the organisation and Incident management. This would also include:

- 2.2.1 Ensuring review of the Information Security Policy by internal and/or external subject matter experts to check for the adequacy and effectiveness of the ISMS programme
- 2.2.2 Reviewing and updating the cyber security policy documents.
- 2.2.3 Defining rules for secure and acceptable use of communication channels for the business requirements of the department/organization.
- 2.3 Developing and implementing a security architecture for the organisation by leveraging technology and understanding of threat landscape.
- 2.4 Establishing and reviewing the Risk Assessment methodology and selection of appropriate controls for risk mitigation by leveraging technology and an understanding of the threat landscape in the organisation.
- 2.5 Interacting with regulatory bodies and external agencies that could be of help to maintain information security for the organization, e.g. CERT-In
- 2.6 Ensuring that the following activities are carried out at regular intervals, either directly or through the deployment of subject matter experts:
 - 2.6.1 Log review, analysis and exception reporting
 - 2.6.2 **Vulnerability Assessment & Penetration Testing (VAPT)** of all websites, portals and IT systems, on a quarterly basis at a minimum; ensuring that websites are GIGW compliant
 - 2.6.3 **Web Application Security Assessment (WASA)** and white-listing of all web applications in use by the organisation, annually at a minimum
 - 2.6.4 **Software Development Lifecycle (SDLC) Audit and periodic Code Reviews** to ensure that applications continue to be secure
 - 2.6.5 **Information Security Audit** of IT Systems and controls, including site audits as appropriate, where online operations span multiple locations. The audit should ensure the following:
 - 2.6.5.1 No unsupported operating systems are in use in the department
 - 2.6.5.2 CISO prescribed hardening guidelines, patch management guidelines, anti virus / malware guidelines, no privilege access on endpoints, regular review of access privileges, acceptable configuration guidelines and procedures are properly



implemented;

- 2.6.5.3 Ensure defined principles of secure software development process is followed for all software applications and the same is reflected in contracts, if software development is outsourced;
- 2.6.5.4 Citizen / customer data privacy to be ensured in case if citizen / customer data is captured and maintained;
- 2.7 Periodic assessment / audits of third party service providers to assess risks to you organisation;
- 2.8 Certify that the time synchronisation of the Network Time Protocol in the organisation has been done with the National Physical Laboratory.
- 2.9 **Issuing and periodic review** of device hardening guidelines, patch management guidelines, anti-virus / malware guidelines, User Access Management guidelines, privilege access management guidelines, end point management guidelines, connectivity guidelines for Trading partners and external agencies, controls on mobile devices and wireless technology
- 2.10 **Authorising an Acceptable Use policy for software packages and freeware** in consonance with the organisation's risk/threat landscape, business objectives and Security Policy & Procedures
- 2.11 Adopting a suitable IT Governance framework for implementing supporting processes such as **Configuration Management, Change Management, Incident Management and Problem Management** etc. CISO should ensure that appropriate instructions are issued for adherence to processes within the organisation and that no authorised changes are carried out to online systems without specific Change Approval.
- 2.12 Ensuring that the IT infrastructure deployed for online operations is kept up to date as per policy and is always under maintenance and technical support so that security patches and bug fixes are regularly applied to protect the infrastructure from vulnerabilities.
- 2.13 Ensuring that clauses pertaining to Information Security are incorporated into contracts/agreements/MoUs with service providers.
- 2.14 Securing senior management approval for emergent/urgent procurements necessary to keep the infrastructure safe from attacks and exploits
- 2.15 Developing and Implementation of scenario-based **Incident Response plans to deal with Cyber crises, contingencies and disasters, attack on IT systems** etc. This



should include incident containment, assessment, root cause analysis, mitigation/prevention, continuous monitoring, forensics and reporting as required. This should include the following:

- 2.15.1 Ensuring that Incidents, especially repeat incidents are investigated and corrective action taken as identified through a comprehensive Root Cause Analysis (RCA)
- 2.15.2 Ensuring that information security incidents are reported to CERT-In
- 2.16 Coordination with stakeholders in all matters related to internal and external security and covering the following aspects:
 - 2.16.1 Assessing the adequacy of controls for Confidentiality, Integrity and Availability of all the Information Systems;
 - 2.16.2 Explaining exceptions, if any, to security policies and procedures along with the risk to business;
 - 2.16.3 Systematically identifying and managing security risks from an end-to-end perspective on a periodic basis;
 - 2.16.4 Assessment of the maturity and effectiveness of the security program;
 - 2.16.5 Steps proposed to remediate gaps identified, if any; and
 - 2.16.6 Impact of the incidents and breaches on the organisation from a business perspective.
- 2.17 Establishing a **Cyber Crisis Management Group** with the head of organisation (or his appointed representative) as its Chairman and to prepare a list of contact persons to be contacted during crisis e.g. internal: financial, personnel etc. and external: law enforcement agencies, CERT-In etc. complete with up-to-date contact details. CCMG should authorise a **Cyber Crisis Management Plan (CCMP)** outlining roles and responsibilities of organisational stakeholders. Implementing the CCMP, including security best practices and specific action points:
 - 2.17.1 Planning and executing periodic disaster recovery drills/simulation exercises in order to establish the adequacy of the Business Continuity Plan
 - 2.17.2 Ensuring that periodic tests are conducted to evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks as well as after any major incident
 - 2.17.3 Where the geographical spread of IT Systems and online operations spans multiple locations across the country, identifying personnel responsible for implementation of information security at the local level as well as for periodic reporting as required to the CISO.
- 2.18 Coordinating all matters related to security internally and externally while providing



regular reports to the head of the organisation covering the following aspects:

- 2.18.1 Assessing the adequacy of controls for confidentiality, integrity and availability of all the information systems;
- 2.18.2 Explaining exceptions, if any, to security policies and procedures along with the risk to business;
- 2.18.3 Systematically identify and manage security risks from an end to end perspective on a periodic basis;
- 2.18.4 Assessment of the maturity and effectiveness of the security program;
- 2.18.5 Steps proposed to remediate gaps identified, if any; and
- 2.18.6 Impact of the incidents and breaches on the organisation from a business perspective.
- 2.19 Develop and implement ICT disaster recovery and security incident management processes, which consists of following activities:
 - 2.19.1 To coordinate response to security incidents;
 - 2.19.2 To prepare evidence for legal action following an incident; and
 - 2.19.3 To comply with the security suggestions provided to them in incidents' analysis' reports;
 - 2.19.4 To analyze incidents in order to prevent their recurrence; and
 - 2.19.5 To report information about security incidents without delay to CERT-In.






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


०७/१०/२१
(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



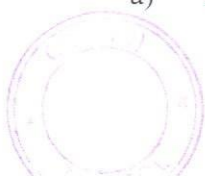
- without authorization, leading to harm to the power grid or its critical sub-sectoral elements Generation, Transmission and Distribution.
17. **Cyber Security Policy:** shall mean documented set of business rules and processes for protecting information, computer resources, networks, devices, Industrial 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 Edition1.0 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 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 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. IEC 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.



No. 20(3)/2022-CERT-In
Government of India
Ministry of Electronics and Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In)

Electronics Niketan,
6 CGO Complex,
New Delhi-110003

Dated: 28 April, 2022

Subject: Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Whereas, the Central Government in terms of the provisions of sub-section (1) of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) has appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette and as per provisions of sub-section (4) of section 70B of IT Act, 2000 The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security:-

- a) collection, analysis and dissemination of information on cyber incidents;
- b) forecast and alerts of cyber security incidents;
- c) emergency measures for handling cyber security incidents;
- d) coordination of cyber incidents response activities;
- e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- f) such other functions relating to cyber security as may be prescribed.

And whereas, "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" were notified and published vide notification dated 16.01.2014 by the Central Government in exercise of the powers conferred by clause (zf) of sub-section (2) of section 87 read with sub-section (5) of section 70B of the IT Act, 2000.



And whereas, as per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person for carrying out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000.

And whereas, various instances of cyber incidents and cyber security incidents have been and continue to be reported from time to time and in order to coordinate response activities as well as emergency measures with respect to cyber security incidents, the requisite information is either sometime not found available or readily not available with service providers/data centres/body corporate and the said primary information is essential to carry out the analysis, investigation and coordination as per the process of law.

And whereas, it is considered expedient in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence using computer resource or for handling of any cyber incident, that following directions are issued to augment and strengthen the cyber security in the country:

- (i) All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.
- (ii) Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.



- (iii) When required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents, the service provider/intermediary/data centre/body corporate is mandated to take action or provide information or any such assistance to CERT-In, which may contribute towards cyber security mitigation actions and enhanced cyber security situational awareness. The order / direction may include the format of the information that is required (up to and including near real-time), and a specified timeframe in which it is required, which should be adhered to and compliance provided to CERT-In, else it would be treated as non-compliance of this direction. The service providers, intermediaries, data centres, body corporate and Government organisations shall designate a Point of Contact to interface with CERT-In. The Information relating to a Point of Contact shall be sent to CERT-In in the format specified at Annexure II and shall be updated from time to time. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact.
- (iv) All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.
- (v) Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:
- a. Validated names of subscribers/customers hiring the services
 - b. Period of hire including dates
 - c. IPs allotted to / being used by the members
 - d. Email address and IP address and time stamp used at the time of registration / on-boarding
 - e. Purpose for hiring services
 - f. Validated address and contact numbers
 - g. Ownership pattern of the subscribers / customers hiring services



- (vi) The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years so as to ensure cyber security in the area of payments and financial markets for citizens while protecting their data, fundamental rights and economic freedom in view of the growth of virtual assets.

For the purpose of KYC, the Reserve Bank of India (RBI) Directions 2016 / Securities and Exchange Board of India (SEBI) circular dated April 24, 2020 / Department of Telecom (DoT) notice September 21, 2021 mandated procedures as amended from time to time may be referred to as per Annexure III.

With respect to transaction records, accurate information shall be maintained in such a way that individual transaction can be reconstructed along with the relevant elements comprising of, but not limited to, information relating to the identification of the relevant parties including IP addresses along with timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred.

And whereas, the meaning to the terms 'cyber incident' or 'cyber security incident' or 'computer resource' or other terms may be ascribed as defined in the IT Act, 2000 or "The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013" as the case may be.

And whereas, in case of any incident, the above-referred entities must furnish the details as called for by CERT-In. The failure to furnish the information or non-compliance with the *ibid.* directions, may invite punitive action under sub-section (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

This direction will become effective after 60 days from the date on which it is issued.



Annexure I

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In:

[Refer Rule 12(1)(a) of The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013]

- i. Targeted scanning/probing of critical networks/systems
- ii. Compromise of critical systems/information
- iii. Unauthorised access of IT systems/data
- iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- v. Malicious code attacks such as spreading of virus/worm/Trojan/Bots/Spyware/Ransomware/Cryptominers
- vi. Attack on servers such as Database, Mail and DNS and network devices such as Routers
- vii. Identity Theft, spoofing and phishing attacks
- viii. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- ix. Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
- x. Attacks on Application such as E-Governance, E-Commerce etc.
- xi. Data Breach
- xii. Data Leak
- xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
- xiv. Attacks or incident affecting Digital Payment systems
- xv. Attacks through Malicious mobile Apps
- xvi. Fake mobile Apps
- xvii. Unauthorised access to social media accounts
- xviii. Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
- xix. Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones



xx. Attacks or malicious/ suspicious activities affecting systems/
servers/software/ applications related to Artificial Intelligence and Machine
Learning

The incidents can be reported to CERT-In via email (incident@cert-in.org.in),
Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and
formats of reporting cyber security incidents is also published on the website of
CERT-In www.cert-in.org.in and will be updated from time to time.



Annexure II

Format for providing Point of Contact (PoC) information by Service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In

The Information relating to the Point of Contact shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified below and shall be updated from time to time:

Name	
Designation	
Organisation Name	
Office Address	
Email ID	
Mobile No.	
Office Phone	
Office Fax	



Annexure III

KYC Requirements

For the purpose of KYC, any of following Officially Valid Document (OVD) as a measure of identification procedure prescribed by the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016 / Securities and Exchange Board of India Clarification on Know Your Client (KYC) Process and Use of Technology for KYC vide Circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020 / The Department of Telecom File No: 800-12/2021- AS.II dated September 21, 2021 on Self-KYC (S-KYC) as an alternate process for issuing of new mobile connections to Local and Outstation category customers, shall be used and maintained:

- a. The passport,
- b. The driving license,
- c. Proof of possession of Aadhaar number,
- d. The Voter's Identity Card issued by the Election Commission of India,
- e. Job card issued by NREGA duly signed by an officer of the State Government and
- f. Letter issued by the National Population Register containing details of name and address.
- g. Validated phone number
- h. Trading account number and details, Bank account number and bank details

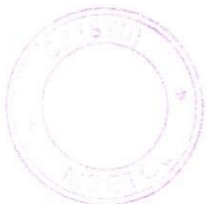
For the purpose of KYC for business entities (B2B), documents mentioned in the Customer Due Diligence (CDD) process prescribed in Reserve Bank of India Master Direction - Know Your Customer (KYC) Direction, 2016 as updated from time to time shall be used and maintained.



Form to report Incidents to CERT-In				
For official use only:			Incident Tracking Number : CERTIn-xxxxxx	
1. Contact Information for this Incident:				
Name:	Organization:	Title:		
Phone / Fax No:	Mobile:	Email:		
Address:				
2. Sector : (Please tick the appropriate choices)				
Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum	InfoTech Other _____	
3. Physical Location of Affected Computer/ Network and name of ISP.				
4. Date and Time Incident Occurred:				
Date:			Time:	
5. Is the affected system/network critical to the organization's mission? (Yes / No). Details.				
6. Information of Affected System:				
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model
7. Type of Incident:				
Phishing Network scanning /Probing Break-in/Root Compromise Virus/Malicious Code Website Defacement System Misuse	Spam Bot/Botnet Email Spoofing Denial of Service(DoS) Distributed Denial of Service(DDoS) User Account Compromise		Website Intrusion Social Engineering Technical Vulnerability IP Spoofing Other _____	
8. Description of Incident:				



9. Unusual behavior/symptoms (Tick the symptoms)				
System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Anomalies Suspicious probes Suspicious browsing New files Changes in file lengths or dates Attempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries Presence of new setuid or setgid files Changes in system directories and files Presence of cracking utilities Activity during non-working hours or holidays Other (Please specify)			
10. Has this problem been experienced earlier? If yes, details.				
12. Agencies notified?				
Law Enforcement	Private Agency	Affected Product Vendor	Other _____	
11. When and How was the incident detected:				
13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)				
Whether log being submitted		Mode of submission:		
OPTIONAL INFORMATION				
14. IP Address of Apparent or Suspected Source:				
Source IP address:		Other information available:		
15. Security Infrastructure in place:				
	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				



16. How Many Host(s) are Affected		
1 to 10	10 to 100	More than 100
17. Actions taken to mitigate the intrusion/attack:		
No action taken System Binaries checked	Log Files examined System(s) disconnected from network	Restored with a good backup Other _____
Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident		
Mail/Fax this Form to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax: +91-11-24368546 or email at: incident@cert-in.org.in		

