Grid Controller of India Ltd.

Procedure

for

Activities of

CYBER SECURITY COORDINATION FORUM

[For GRID-Operation Sector]

Prepared in Compliance

to

Regulation 53 of
Central Electricity Regulatory Commission
(Indian Electricity Grid Code) Regulations, 2023

September, 2023

Contents

ACTIVITIES OF CYBER SECURITY COORDINATION FORUM

(GRID OPERATION SECTOR)

1. Background

1.1. This procedure is in accordance with *Regulation 53 of the Central Electricity Regulatory Commission (Indian Electricity Grid Code) Regulations, 2023 (hereinafter referred to as "IEGC, 2023")*.

1.2. In accordance with clause 53 (1) of the IEGC, 2023, a subcommittee at the regional level shall also be formed. The procedure therefore lays down the rules of procedure for carrying out the activities of Central and Regional Cyber Security Coordination Forums under the Grid Operation Sector as per the provisions stipulated in the aforementioned regulation of the IEGC, 2023.

The procedure will supplement the Information Security Management practices, policy and procedure of the utilities in accordance with the provisions detailed in the CEA (Cyber Security in Power Sector) Guidelines, 2021 and other relevant guidelines / directions issued from time totime by Central Government and statutory bodies like CEA, NCIIPC, CERT-IN etc.

The procedure will also strengthen the activity and role of relevant Sectoral CERTs in performing their functions and obligations.

2. Abbreviations

Abbreviations	**Description**
a) ARR	Annual Rate of Return
b) CEA	Central Electricity Authority
c) CERT	Computer Emergency Response Team
d) CERT-In	Indian Computer Emergency Response Team
e) CERT-GO	Computer Emergency Response Team – Grid Operation
f) CERT-MoP	Computer Emergency Response Team – Ministry of Power
g) CIGRE	International Council on Large Electric System
h) CISO	Chief Information Security Officer
i) CSCF-GO	Cyber Security Coordination Forum – Grid Operation
j) CSIRT	Computer Security Incident Response Team
k) CSK	Cyber Swachhta Kendra
l) IEEE	Institute of Electrical and Electronics Engineers
m) IEGC	Indian Electricity Grid Code

n) ISMS	Information Security Management System
o) ISO	International Organization for Standardization
p) IT	Information Technology
q) LDC	Load Despatch Centre
r) NCIIPC	National Critical Information Infrastructure Protection Centre
s) NLDC	National Load Dispatch Centre
t) NPC	National Power Committee
u) NPTI	National Power Training Institute
v) OT	Operational Technology
w) RLDC	Regional Load Dispatch Centre
x) RPC	Regional Power Committee
y) SCADA	Supervisory Control and Data Acquisition Systems
z) SLDC	State Load Dispatch Centre
aa) SOC	Security Operation Centre
bb) SOP	Standard Operating Procedures
cc) VA-PT	Vulnerability Assessment and Penetration Testing
dd) ISO Standards:	International Organization for Standards
ISO 27001	Information Security Management

3. Definitions

3.1. Grid-Controller of India Ltd. (Grid-India) means the wholly Government owned independent Company notified by Central Government under Section 26 and subsection (2) of Section 27 of the Act vide notification dated 19th December 2016. Grid-India is operating all five RLDCs and the NLDC w.e.f. 1st October, 2010;

3.2. Chief Information Security Officer: shall mean the designated employee of the Senior management level directly reporting to the 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.

3.3. 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.

3.4. Cyber Security Incident: shall mean any real or suspected adverse cyber security event that violates, explicitly or implicitly, the cyber security policy of the Responsible Entity resulting in unauthorized access, denial of service or disruption, unauthorized use of computer resources 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.

3.5. Security Architecture: shall mean a framework and guidance to implement and operate a system using the appropriate security controls with the goal of maintaining the system's quality attributes like confidentiality, integrity, availability, accountability and assurance

3.6. Vulnerability: shall mean intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.

3.7. Vulnerability Assessment: shall mean a process of identifying and quantifying vulnerabilities

3.8. Penetration Testing: shall mean simulated cyber-attack on a computer system to check for exploitable vulnerabilities.

3.9. CSIRT: Computer Security Incident Response Team that performs, coordinates and responds to security incidents that occur within a defined sector. CSIRT - Power: shall mean Computer Incident Response Team specifically set up for the power sector at Central Electricity Authority, which will function as an extended arm to Indian Computer Emergency Response Team (CERT-In).

The definitions indicated above are in accordance with the provisions available / defined in variousRules / Regulations / Guidelines such as Information Technology (Information Security Practicesand Procedures for Protected System) Rules, 2018; CEA (Cyber Security in Power Sector) Guidelines, 2021 etc.

Any amendment in the definitions / provisions of any such rules / regulations shall inter-alia be effective in the definitions indicated herein.

Words and expressions used in this procedure and not defined herein but defined in the IEGC,2023 orany other regulations / Guidelines / Directions specified by the Central Commission shall, unlessthe context otherwise requires, have the meanings assigned to them under the Act or other regulations specified by the Central Commission, as the case may be.

4. Scope & Applicability

These procedures are applicable for all activities related to formation, roles & responsibilities and activities of Cyber Security Coordination Forum -GO and Regional level sub-committees -GO to coordinate and deliberate on the cyber security challenges and gaps at appropriate level by National / Regional / State Load Despatch Centres and any other utility (if any) to be declared time to time by the concerned statutory bodies under CERT-Grid Operation.

5. Short title and commencement

There will be two (2) levels of Committees to be formed under the Head of Cyber Security Coordination Forum viz.

a) A Regional Level Sub-committee to be called as Regional Cyber Security Coordination Forum – Grid Operation (GO-xR-CSCF)

b) A Central Level committee to be called as Central Cyber Security Coordination Forum - Grid Operation (GO-CSCF)

6. Regional Cyber Security Coordination Forum

In order to ensure proper coordination, information sharing, sharing of best practices, harmonising the Cyber Security initiatives and preparedness of the Load Despatch Centres and to review the Cyber Security initiatives, incidences reported and actions taken to mitigate the risks, a Regional Coordination Forum shall be formed at the regional level (with LDCs as per the definition of Regional Entity of IEGC, 2023) with representations as detailed in subsequent section below.

6.1. Members

The sub-Committee of GO-x’R-CSCF shall consist of the following members:

a) Head of RLDC

b) CERT-GO Nodal or his authorised representative

c) Member Secretary RPC or his/her authorised representative

d) Heads of SLDCs or his/her authorised representative other than CISO.

e) Chief Information Security Officer of all SLDCs within the specific Region.

f) Cyber Security Nodal officer of RLDC

g) Representative of the NCIIPC

h) Any other member deemed necessary by the Forum for smooth coordination and monitoring

Members may invite stakeholder representatives from STUs and other utilities like Thermal, Hydro, RE, Transmission & Distribution sectors operating in the region as and when required.

The member convenor of the Sub-committee shall be the designated cyber security nodal officer of the concerned RLDC and the necessary Secretariat functions shall be housed at the respective RLDC.

The Chairperson of the Committee shall be Head of the RLDC.

[1] X denotes region

6.2. Roles and Responsibilities

6.2.1. Monitoring & Management of Cyber Security Challenges and Gaps

a) Monitoring of Cyber Security Challenges and Gaps on a Quarterly basis

i. Building a shared understanding of regulatory requirements. Adopting and reviewing a framework for Cyber Security Gap Analysis for Grid-Operation sector.

ii. Periodic review and assessment of compliance to provisions of CEA (Cyber Security in Power Sector) Guidelines, Guidelines, CERT- IN directions and other regulatory requirements of LDCs and other concerned agencies under CERT-GO towards cyber Security measures and controls including gaps from the adopted framework.

iii. Review of compliance to NCIIPC & CERT-IN advisories and action taken against the same.

iv. Review of VA-PT audit of IT & OT systems of LDC, schedules, observations and compliance thereof. Identification of common vulnerabilities across the LDCs and suggest necessary advisory.

v. Review of ISO27001 certification, continuation and activities related to the same.

vi. Gap analysis of Cyber Security Framework implementation of LDCs on an Annual basis

b) Monitoring and review of events and incidences reported / published on a Quarterly basis

i. Creating an information sharing platform for sharing IOCs/IOAs (Indication of Compromise / Indication of Attack), Malware information and/or events / incidences observed at any LDC.

ii. Review of actions taken against CSK Vulnerabilities reported and hand-holding if required.

iii. Review of events and incidences reported at any LDC and action taken thereof.

6.2.2. Harmonization & Capacity Building

a) Harmonization of cyber security practices in grid operation

i. Coordination in knowledge sharing and implementation of the best practices adopted across LDCs.

ii. Forming working groups for the formulation of recommendations towards adoption of the latest technology on cyber security, preparation of Standard Operating Procedure (SoP), implementation policy of Cyber Security Controls, study on specific tasks on cyber security and their implementations in Grid Operation and submission of reportsthereof.

iii. Review and verification of the SoPs, Cyber Crisis Management Plans, Emergency Preparedness Plan and Incidence Response mechanism of LDCs at least once a year.

iv. Identification of common issues on cyber security in grid operation and discussion on ways to mitigate them.

b) Organising Cyber Security Workshops, Table-top Exercises, Training & Awareness Sessions

i. Organising workshops and awareness sessions on Cyber Security Best practices and initiatives for all stakeholders including representation from Regional Entities, Vendor ecosystems and associated institutions. Such workshops shall be conducted at least twice a year.

ii. Conducting Cyber Security Table-top exercises, incidence management and response drills along with other activities at least once a year for assessment of preparedness to withstand cyber attacks

iii. Formulating training needs for LDC personnel, and course material and providing suggestions to designated institutions for Cyber Security related courses.

6.3. Meetings & Reports

The committee shall conduct periodic meetings on a Quarterly basis to discuss the following minimum agenda:

a) Progress review of the activities conducted towards the accomplishment of the roles and responsibilities assigned as per Para 6.2 above.

b) Action / compliance requirements and plan thereof towards the recommendations and resolutions of the Central level committee meetings as applicable.

c) Adequacy of resources and capacity building requirements at LDCs towards Cyber Security implementation and compliance.

d) Highlights of the Cyber Security activities, developments, technological upgradations, and major incidences reported across the globe, especially in the power sector and its probable impact including learnings / actionable insights thereof.

e) Major Cyber Security gap observed / reported in the LDCs and its mitigating actions.

f) Matters required to be escalated to a higher forum including that in the Central Level Cyber Security Coordination Forum.

g) Any other agenda which the committee feels suitable and applicable.

The committee may also conduct special meetings if required.

The meetings shall be organised by the concerned RLDC. The expenditure shall be met by respective RLDC from ARR/fees & charges. The minutes of the meeting shall be published and circulated among the members, central coordination forum and relevant statutory bodies.

An annual compendium of the activities, resolutions and observations of the Regional Level sub-Committee shall be published by the Secretariat for limited circulation.

7. Central Cyber Security Coordination Forum

In order to ensure Pan-India Coordination and implementation of Cyber Security Resilient Grid-Operation process and controls as well as to ensure harmonized cyber security practices, emergency response and governance, a Central Cyber Security Coordination Forum shall be formed with representations as detailed in subsequent section below.

7.1. Members

The Committee of GO-CSCF shall consist of the following members:

a) CISO-MoP

b) CERT-GO Nodal or his authorised representative

c) CISO Grid India

d) Deputy Director General NCIIPC or his/her authorised representative

e) Deputy Director General CERT-IN or his/her authorised representative

f) Heads of NLDC or his/her authorised representative other than CISO.

g) Representative of CEA/NPC & CSIRT-Power

h) Chairpersons of the Regional Sub-Committees.

i) Member convener of Regional Sub-Committees

j) Any other member deemed necessary by the Forum for smooth coordination and monitoring

Members may invite stakeholder representatives from CTU and other utilities in power sectors like Thermal, Hydro, RE, Transmission & Distribution as and when required.

The member convenor of the Coordination Forum shall be the CERT-GO Nodal and the necessary Secretariat functions shall be housed at GRID-INDIA.

CISO-MoP shall be the Chairperson of the Central Cyber Security Coordination Forum.

7.2. Roles and Responsibilities

7.2.1. Monitoring & Management of Cyber Security Challenges and Gaps

a) Review and Monitoring of challenges & gaps

i. Half-yearly review of compliance to all regulatory requirements and statutory obligations by LDCs. Analysis of Gap from adopted Framework.

ii. Review of available policies, regulatory provisions, guidelines, Cyber Security maturity framework and recommendations and providing necessary feedbacks to the designated agencies for upgradation / modification as deemed suitable.

iii. Coordination with the non-complying agencies /utilities / LDCs to address the root cause and provide technical as well as administrative guidance.

b) Incident response and emergency preparedness.

i. Discuss root cause, impacts and mitigating techniques of any latest cyberattack or cyber incidences reported nationally or internationally especially in power sector at large.

ii. Provide necessary feedback and alerts to the concerned agencies and senior management of LDCs regarding any such development and learnings thereof.

iii. To conduct cyber security mock-drill at least once in a year covering majority LDCs and its associated stake holders to assess the emergency response and preparedness of the LDCs and advise improvements thereof.

7.2.2. Planning, Development, Capacity Building & Coordination

a) Planning & Policy level guidance for Cyber Security initiatives at LDCs

i. Review and redressal of Policy level decisions, implementations and adoption of advanced platforms for Cyber Security enhancement at LDCs.

ii. Review and proliferation of appropriate Cyber Security Framework of LDCs along with review of its implementation thereof.

iii. Planning & Formulation of cyber risk evaluation and management methods through various measurable parameters and periodic assessment of Cyber Security Maturity of the LDCs accordingly.

iv. Endorsing and encouraging a unified harmonised cyber resilience plan for grid operation and hand-holding the LDCs towards implementation thereof.

v. Review of standard reference security architecture for IT, OT and associated systems for LDCs

vi. Recommendation for specific R&D activity in Cyber Security area pertaining to LDC functioning.

vii. Forming Working Groups to study adoption of various security standards/protocols; interface with stakeholders; themes related to products and services involved in integrated System Operation, Market Operation functions, reporting and exchange of information among LDCs and stake holders at large etc. and to suggest appropriate policy interventions to strengthen cyber security and resilience of LDCs.

b) Ensuring Capacity Building & Resource adequacy

i. Providing necessary guidance and feedback to the planners, decision makers and institutional heads for ensuring adequacy of resources, capacity building programmes and harmonisation of practices.

ii. Facilitate Senior Management Level Workshops, Table-top exercises, round-tables and brainstorming session on Cyber Security practices, developments and implementations on yearly basis.

iii. Providing necessary guidance and feedback to the appropriate agency / institution in framing appropriate training modules, courses and selection of certification mechanism for IT, OT & Cyber Security professionals of LDCs along with recommendation of appropriate incentive schemes thereof.

iv. Exploring emerging technologies and the best practices adopted in the field of cyber security by the industry leaders in international arena and creating opportunity to obtain exposure through participation in various National & International workshops, seminars, plenums etc. organised by global leaders.

v. Providing necessary feedback to the designated entity towards development and continuation of suitable certification mechanism like trusted vendor system etc. for third party devices and services towards supply chain risk management.

c) Coordination and handholding of LDCs towards building a robust integrated cyber secured grid operation practice

i. Establishing a trustworthy, mutually dependant and coordinated knowledge sharing platform for dissemination of findings, experiences, practices and concerns towards implementation of cyber security controls and providing necessary guidance / directions in mitigating the challenges.

ii. Review of risk assessment of the LDCs and providing necessary assistance for compliance of regulatory and statutory requirements.

7.3. Meetings & Reports

The committee shall conduct periodic meeting on Half-yearly basis to discuss the following minimum agenda:

a) Progress review of the activities conducted towards accomplishment of the roles and responsibilities assigned as per Para 7.2 above.

b) Progress review and monitoring of compliance to the recommendations of Empowered Committee on Cyber Security and other similar forums as deemed appropriate.

c) Review of recommendations and resolutions of the Regional level Sub-committee meetings and providing necessary endorsements / guidance / redressal thereof.

d) Adequacy of resources and Cyber Security maturity of the LDCs and Gap identified thereof.

e) Review of the prevailing policies, guidelines, regulations and taking appropriate actions towards mitigation of the challenges.

f) Matters required to be escalated to higher forum including that in Regional Power Committee, Empowered Committee on Cyber Security or as deemed appropriate.

g) Any other agenda which the committee feels suitable and applicable.

The committee may also conduct special meetings if required.

The meetings may be organised and funded by GRID-INDIA and shall be reimbursed against its fees & charges under applicable head.

An annual compendium of the activities, resolutions and observations of the Central Cyber Security Coordination Forum shall be published by the Committee Secretariat for limited circulation.

8. <u>Revision of Procedure</u>

As and when required, the procedure shall be reviewed and revised in consultation with stakeholders by CERT-GO with an intimation to the Commission.