TAMIL NADU GENERATION AND DISTRIBUTION CORPORATION LIMITED

CYBER CRISIS MANAGEMENT PLAN (CCMP)

FOR

TANGEDCO

NOVEMBER, 2019

INDEX

1.0 PURPOSE

The purpose of this document is to create Cyber Crisis Management Plan (CCMP) for any unforeseen cyber incident i.e virus or malicious software code, cyber attack, etc., which may cause extensive damage to distribution sector critical information infrastructure of the **TAMIL NADU GENERATION AND DISTRIBUTION CORPORATION LIMITED (TANGEDCO)** is a distribution licenses in the area of **CHENNAI** in the state of TAMIL NADU, INDIA and has various Critical Cyber infrastructure to automate its business processes. In the IT dependent world, Cyber attacks that target the infrastructure or underlying economic well-being of **TAMIL NADU GENERATION AND DISTRIBUTION CORPORATION LIMITED** may severely affect available resources, and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences, or other related incidents capable of causing extensive damage to critical infrastructure of key assets. Large scale cyber incidents may overwhelm corporate resources and services by disrupting functioning of critical information systems and can have cascading effect on other utilities, states and country as a whole. Complications from disruptions of the large magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity.

The main Objectives of the document are -

a. To ensure that interruption or manipulations of critical functions / services in critical distribution sector are brief, infrequent, manageable and cause least possible damage.

b. To enable respective administrative Departments to draw-up their own contingency plans in line with Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism, equip themselves suitably to implement, supervise implementation and ensure compliance among all the organizational units within their domains.

c. To put in place a mechanisms to effectively deal with cyber security crisis and be able to pin point responsibilities and accountabilities right down to individual level.

2.0 SCOPE

The Cyber Crisis Management Plan for countering cyber attack in distribution sector includes the framework for identification of various Critical information infrastructures, cyber incident response co-ordination and steps to be taken for its mitigation. This Cyber Crisis Management Plan addresses the definitions and documentation of IT & Cyber security incident management procedures for such systems and services in **TANGEDCO**. The scope of this Cyber Crisis

Management Plan document is for Business, O&M, SCADA and IT Critical information infrastructure in distribution sector.

The field of cyber security is technology intensive and new vulnerabilities emerge with advancement in technologies giving rise to new types of incidents. As such, the plan of response to cyber security incidents need to be updated on regular basis, preferably once in a year.

3.0 CYBER CRISIS, POSSIBLE TARGETS AND IMPACTS

3.1 Physical threats

The different type of physical threats / crisis may be –

1. **External physical threats**:

   Flooding, lightning, earthquake, wind, tornado, hurricane, ice, fire, chemical.

2. **Internal Physical threats :**

   Fire, environmental failure, liquid leakage, electrical interruption

3. **Human Physical threats** :

   Theft, vandalism, sabotage, espionage, errors

3.2 Cyber Threats

3.2.1 Types of Cyber Security Incidents

Any real or suspected adverse event in relation to the security of computer systems or computer networks can be termed as a logical security breach. In other words, a logical security incident can be defined as network or host activity that potentially threatens the security of computer systems. Examples of such incidents could include activity such as:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

3.2.2 Nature of Cyber Crisis and Contingencies

Unlike physical attacks, cyber security incidents may be triggered on individual systems, simultaneously on multiple systems andnetworks in a single or multipleorganisations, states and entire nation from places within the country or anywhere outside the country. Physical crisis and cyber crisis may happen concurrently or follow each other.

Cyber crisis has unique features which are different from a physical crisis. In some cases, the severity of cyber crisis is high but confined to individuals or few organisations in a limited area. In other cases the severity may be low but widely spread to a larger area.

3.3 Security Requirements

The objectives of information security is preservation of

- **Confidentiality**: preventing the unauthorized access to information.
- **Integrity**: preventing the unauthorized modification or theft of information.
- **Availability**: preventing the denial of service and ensuring authorized access to information.
- **Non-repudiation or accountability**: preventing the denial of an action that took placeor the claim of an action that did not take place.

3.4 Nature of Cyber Crisis, Possible targets and Impact

The following provides the snapshots of nature of cyber security incidents which include attempts (either failed or successful) that can trigger a crisis at individual/organization, multiple organization, state and national level:-

Sl.No.	Type of Cyber Crisis	Possible Targets	Related impact
1.	Targetted Scanning, Probing and Reconnaissance of Networks and IT infrastructure	• Sensitive Government and Critical Information infrastructure. • Infrastructure at Data Centres and Network Operation Centres. • Routers, Switches, Database and DNS Servers.	• Pre-cursor to hacking and focussed attack leading to cyber crisis • Total / Partial disruption of e-Governance & Public services like electricity.

		• Web Portals	
2.	Large Scale defacement and semantic attacks on websites. A Website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website. Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated.	• High Profile Govt. / Nationals websites which are dissemination information / websites of Public utilities like Distribution Companies / Water Supply etc., • Key economic transaction websites such as banks / Financial Institutions (FI), online transactions etc.,	• Embarrassment to the public utility / loss of image, reputation etc., • Total / Partial disruption of public services / activities including electricity • Dissemination of false / misleading information. • Monetary loss to the distribution company etc.,
3.	**Malicious Code attacks** (Virus / worm / Trojans/Botnets) • Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus, worms, trojans, spyware, adware and Bots. • Sophisticated malware such as Stuxnet targeting Industrial Control Systems that are part of networks separated through 'airgap' from regular Internet facing networks	• Large & key national databases such as distribution company consumer data base, distribution plan information and any other sensitive information etc., • Large & Key economic data bases such as banks / FIs, Consumers, Data Centres, SCADA etc., • Private consumers / employees of Discom (Home / Corporate Organisations) • Supervisory Control and Data Acquisition systems (SCADA) and Centralized as well as distributed control systems of power, and other digital processes.	• Hanging of Computer systems • Partial or No response from Computer system • Total / partial break down of data access services. • Monetary loss, damage to reputation, loss of image etc • Total/partial corruption of data bases • Data Theft, Identity theft and possible espionage. • Total/partial disruption of services/activities in one or more critical sectors such as energy.
4.	**Malware affecting / Mobile devices** Malicious code and malicious applications	• Consumer / employees of Discoms using mobile apps with the affected operating system and connected computer	• Unauthorized disclosure of user's data and contact details

		(apps) affecting operating systems / platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile, Blackberry OS	systems.	• Misuse of devices resulting in excessive billing • Theft of sensitive user credentials
5.		**Large scale SPAM attacks** Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems. As a result, spamming could disrupt e-mail services, messaging systems and mobile phone communications.	• ISP networks • Large corporate networks • Key digital networks of distribution companies.	• Significant slowdown in network performance • Total/partial disruption of E-mail communication services • Severe drain on network resources. • Significant reduction in access to critical network services. • Increased possibility of virus/worm infection
6.		**Identity Theft Attacks**		
	6.1	**Large scale spoofing** • Spoofing is an attack aimed at 'Identity theft' • Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage	• High profile users in Government, Corporate and Key economic installations.	• Increased possibility of identity theft and root privileges compromise leading to penetration into sensitive IT systems and Databases • Loss of sensitive data, monetary loss and loss of image.
	6.2	**Phishing attacks** • Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds	• Key Government organisations and Government service providers including power Distribution organisations. • Key e-Governance entities including Banks	• Loss of sensitive personal data, monetary loss and loss of image and trust and • Financial frauds • Loss of user credentials

		• Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication • **Vishing attacks** Vishing is a combination of 'voice' and 'phishing'. It is the practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. It exploits the trust in landline telephone services and uses VoIP to trick the user. • SMShing attacks These are phishing attacks launched through SMS service via Mobile phones.	etc.,	• Monetary loss to Distribution company / consumers.
	6.3	**Social Engineering** Art of manipulating people into performing disclosure actions or divulging confidential information	• Individual users such as senior executives & officials, employees of Discoms • Network / System / Database Administrators	• Loss of sensitive personal Data and key information
7.		**Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks**	• Public utility services including power. • Critical Systems of Power Sector.	• Total/partial disruption of services for prolonged periods • Failed / aborted

		• Denial of Service (DoS) is an attempt to make a computer resource unavailable to its intended users • A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system. • DDoS attacks are launched through a Botnet which is a network of compromised computer systems called 'Bots' . • NTP based Distributed Reflected Denial of Service (DrDoS) Attacks.	• Supervisory Control and Data Acquisition (SCADA) System. • Web-based key economic targets such as control system of Discoms, Banks / FIs, Online transaction of bills etc.,	missions. • Possible damage to life and/or property • Monetary loss, damage to reputation, loss of image of Discoms etc
8.		**Domain Name Server (DNS) attacks** • Attacks on DNS Servers aim at denying resolution of a domain name into a IP address, reverse DNS queries or redirecting users and traffic to fake/malicious domains in some other country to disrupt internet and mail traffic in the country**.**	• Country Level Domain registry systems (NIXI ".IN" registry) • International gateway or ISP / Large Corporate server systems.	• Total/partial disruption of ".in" registry services. • Possible damage of / inaccessibility to domain registry database or resolution services. • Illegal diversion of Internet and mail traffic to some other countries. • Total / Partial disruption of internet traffic nationally / internationality. • Total / Partial break down of online economic activities. • Monetary loss, damage to reputation, loss of image etc

9.		**Application Level Attacks** • Exploitation of inherent vulnerabilities in the code of application software such as web / mail / databases	• e-Governance • e -commerce • Business and Banking Applications	• Data manipulation which may result in huge economic fallouts including monetary as well as business loss. • Disruption of services • Loss of sensitive data and loss of image & trust
10.		**Infrastructure attacks** • Attacks such as DoS, DDoS, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralised/Distributed Control System (DCS), Gateways of ISPs and Data Networks, Infection of Programmable Logic Control (PLC) systems by sophisticated malware such as Stuxnet, Reconnaissance and stealing of sensitive information through malware like Duqu, Nitro, Poison-Ivy (Remote Administration Tools) etc.,.	• Supervisory Control and Data Acquisition systems (SCADA) and Centralized as well as distributed control systems of power sector etc., • International gateways / ISPs of Discoms. • Undersea cables. • Data Networks	• Total/partial disruption of services/activities in one or more critical sectors such as energy, telecommunications, emergency restoration of supply etc., • Huge economic fallouts including monetary as well as business loss to Discoms.
11.		**Compound attacks** • By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber attack.	• Public utility services including power sector services. • Web based economic targets of Discoms. • Large & key national & economic databases. • Critical Systems of Discoms. • International gateway / ISPs	• Total/partial disruption of services/activities • Significant slow down in disaster/emergency response capabilities that can magnify the impact of a physical attack • Economic fallouts including monetary as well as business loss.

				• Damage to reputation, loss of image etc.
12.		**Router level attacks** • Routers are the traffic controllers of the Internet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication	• Gateway / ISP routers. • Routers of large & key economic targets such as bank / FI networks, corporate networks, etc., • ADSL / Wi-Fi Routers used offices / employees.	• Total/partial disruption of internet traffic nationally/internationa lly • Total/partial break down of online economic activities • Economic fallouts including monetary as well as business loss • Possession of Router's control by attackers and re-redirection to malicious websites through rogue DNS Server entries for conducting malicious activities
13.		**Attacks on Trusted infrastructure** Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks. Compromise of infrastructure of Certifying authority or key management systems of product / application owners may result in breakdown of trust of users and misuse of authentication mechanisms (i) Denial of Service attacks (ii) Rogue certificates	• SSL Servers • Certifying Authorities • Authentication infrastructures • Secure Communication Protocols and systems • Public Key Infrastructure	• Blocking of handshaking resulting in disruption of financial and authentication services • Large scale Man-in-the-middle attacks resulting in disclosure of sensitive data and user information • Redirection of users to fake websites with dubious authentication • Signing malicious code to make it appear as legitimate • Large scale cyber espionage

14.		**High Energy Radio Frequency Attacks** Use of physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including Wireless networks leading to attacks such as Denial of Service	• Wireless Networks ▪ Wi-Fi ▪ Wi-MAX • Mobile Networks • Satellite Network Communication Systems	• Disturbances or total disruption in the Wireless, Mobile and Satellite Networks • Appliances like, phones, Bluetooth and Microwave devices etc. • Some RF Jamming tools may use very high energy sufficient to even break down the electronics and make it to malfunction totally.
15.		**Cyber Espionageand Advanced Persistent Threats** Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware. The data from compromised system is siphoned off to remote locations. Common channel of attacks include spoofed/compromised email accounts of key officials, social networking sites and drive-by-download through watering hole websites.	• Sensitive Government Organisations including Power Sector Organisations.	• Disclosure of sensitive information • Data theft • Compromise of critical internal systems.
16.		**Client-Side attacks** Attacks on client side vulnerable software applications like MS office applications, Adobe Acrobat reader, JAVA, Browsers Plugins, etc usually via Sophisticated attack tool kits with various exploits available for compromising/rooting the client system.	• Individual users / employee of Discoms	• Data Leakage • User system as bot or launch pad for launching further attacks.

17.		**Attacks using Social / Network Sites (SNS)** Attacks targeting Social networking platform for various malicious activities such as identity theft, fake social accounts, fake news, misinformation, command & control for Botnets, drive-by-download etc.	• Individual users such as senior executives & officials / employees of Discoms / Power Departments.	• Loss of sensitive personal data, loss of image and trust. • Malware distribution.

3.5 Cyber Security – Level of concern

❖ Individual Organization

Perceptible change/variation in system performance and discovery of critical/non critical vulnerabilities/exploits and attacks that can affect normal operation of network and IT systems of individual organization may be any one or combination of the followings in any organization –

- Visible signs of viruses/ worms/ Bots/Malware/ Keyloggers/ Spyware
- Spam
- Identity theft (Phishing, spoofing, social engineering etc.)
- Web defacements
- Hacking of IT systems such as computers systems, Servers (Mail, Web, Database etc.) and Routers
- Application level attacks
- Denial of service attacks (DoS)
- Distributed Denial of Service (DDoS)

❖ Multiple Organization

Perceptible change/variation in network/ system performance and abnormal surge in network traffic affecting IT infrastructure of multiple organizations simultaneously due to:

- Large scale infection of viruses/worms/Bots/Malware/ Keyloggers/Spyware for malicious and espionage activities
- Focused attempts of network scanning and penetration
- DoS/DDoS attacks
- Attacks on Domain Name Servers, Mail Servers, Databases, Routers etc.
- Attacks on Web Servers resulting in defacement of websites on large scale
- Attack on the IT infrastructure of a Critical Information System

- **State/ Multiple State**

  Significant breakdown of supplies or services essential to the life of the citizens including but not limited to Financial, Government, Transport, Energy or Communication due to focused cyber attacks on infrastructure of critical sector and Government across a state or multiple states.

- **Nation**

  Cyber espionage on sensitive Government organizations or significant complete breakdown of supplies or services essential to the life of the citizens including but not limited to Financial, Government, National Defence, Transport, Energy or Communication due to focused cyber attacks on infrastructure of critical sector and Government across the nation.

4.0 CRITICAL INFORMATION INFRASTRUCTURE (CII)

Critical Information Infrastructure (CII) means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on National Security, Economy, Public Health or Safety. The most logical approach for identification of CII should be undertaken on the basis of identification of critical business processes as determined by the distribution company /entity and the information infrastructure supporting these critical business processes, may be identified as CII.

In order to continuously provide critical services and to avoid serious impact on the public services and socio-economic activities resulting from natural disasters, cyber-attacks or other causes, all stakeholders should protect critical infrastructure by reducing the risk of IT/OT outages as much as possible followed by prompt recovery of the same. The other purposes may include but not limited to the following:-

a. To ensure that interruption or manipulations of critical functions/services in critical systems are brief, infrequent and manageable and cause minimal damage.

b. To enable respective departments to draw-up their own contingency plans in line with Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism, equip themselves suitably to implement, supervise implementation and ensure compliance among all the organizational units within their domains.

c. To assist organizations to put in place mechanisms to effectively deal with cyber security crisis and be able to pin point responsibilities and accountabilities.

Each organization is responsible to identify and categorize CIIs within their infrastructures on the basis of Functionality, Criticality Scale, Degree of Complementarities Political, Economic, Social and Strategic Values, degree of dependence, sensitivity etc. The identification of critical infrastructure is a dynamic process and must be reviewed periodically by all stakeholders/Discoms to address changes in functional dependencies, technologies and protocols. CII identification is a part of organizational risk assessment which constitutes a holistic view of all risks to national/organizational security.

- **Functionality** is a dynamic concept which includes the set of functions, procedures and or capabilities associated with a system or with its constituent parts. It may be viewed at two levels- Functional Uniqueness and Functional Dependency.

- **Degree** of Complementarities is a distinguishing characteristic of the InformationInfrastructure is that it links other Information Infrastructure Systems together.Failure of one system has potential to shut down other Critical Information Infrastructure relatively quickly in a cascading manner.

- **Political, Economic, Social and Strategic** Values includes what is held important for political stability, economic prosperity, fraternity, unity and integrity of Nation.

- **Time Duration** has an important significance in the identification and categorization of CII. The same system may or may not be critical at different times / under different circumstances.

4.1 Identification of CII

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must collect system-related information, which are usually classified as follows:

- Details of Hardware
- Details of Software
- System interfaces (e.g., internal and external connectivity)/ Gateways
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity etc.

The initial thought process and initiative for Cyber Security may be directed towards computer and communication system in distribution Sector as follows:-

1. Information Technology for distribution system operation

    1.1 SCADA systems
    1.2 System Data Acquisition System/ Distribution Automation System (DAS)
    1.3 Outage Management System/ Distribution Management System of DISCOMs
    1.4 Advanced Metering Infrastructure (AMI)
    1.5 Integration of renewable sources and interconnection of storage batteries
    1.6 Communication with electric vehicles to manage charging etc.

2. Information Technology for other business functions

    2.1. Metering, Billing and Collections
    2.2. Consumer Web Portal/Apps
    2.3. Office IT / ERP

3. Communication Systems for coordination amongst operators and the above data exchange / processing nodes

    Additional information related to the operational environmental of the IT system and its data in distribution companies include, but is not limited to, the following:

    - The functional requirements of the IT system
    - Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
    - System security policies governing the IT system (organizational policies, statutory requirements, laws, industry practices)
    - System security architecture
    - Current network topology (e.g., network diagram)
    - Information storage protection that safeguards system and data availability, integrity, and confidentiality
    - Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
    - Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)

- Management controls used for the IT system (e.g., rules of behaviour, security planning)
- Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data centre policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

A tentative list of CII identified for distribution sector is as under-

1. Substation Automation system
2. Feeder Automation Systems
3. Outage Management System
4. Utility Enterprise Asset Management System
5. Advance Metering Infrastructure (AMI)/ Smart Metering/Prepaid metering
6. LT Power Management & Automation system
7. Smart RMUs
8. Smart auto re-closures
9. Smart Pole Mounted switchgear
10. RTUs
11. Feeder RTUs
12. Primary Switchgear with Protection Relays
13. SCADA System
14. Gateways
15. Human Machine Interface (HMI)
16. Protection Relays
17. Smart Metering field devices like DCU
18. Industrial PLCs
19. Industrial Firewalls
20. Industrial Networking Device (Ethernet switches, routers, Bridges)
21. Industrial GPS Devices
22. Industrial PCs
23. Smart Software and Analytic Solutions
24. Distribution Management Systems
25. Smart UPS
26. Energy Management System
27. Load Shedding/ Sharing Solutions
28. Drones used for line patrolling using wireless technology
29. Meter Testing/Calibration software
30. CCTV and its monitoring app/software

31. Configuration and Maintenance tool of all devices

The above list is a tentative list and may be updated by the utilities as per the identification of CII in their organization.

5.0 THREAT IDENTIFICATION AND ANALYSIS

A key part of the threat analysis is determining the threat actions associated with each threat-source. These factors govern the probability and impact of a given threat-source to exploit vulnerabilities. A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised.

Threat Types	Motivation for Threat	Threat Action
Intentional and Unintentional Human Threats		
Hacker, Cracker	Challenge Ego Rebellion Destruction of information	▪ Hacking ▪ Social Engineering ▪ System Intrusion, Breaking, ▪ Unauthorised System Access ▪ Computer Crime (e.g. Cyber Stalking)
Computer Criminal	Illegal Information Disclosure Monetary Gain Unauthorised Data Alteration	▪ Fraudulent Act (e.g. Replay, Impersonation, Interception etc.,) ▪ Information Bribery ▪ Spoofing ▪ System Intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	▪ Bomb / Terrorism ▪ Information Warfare ▪ System Attack (e.g. distributed denial of service) ▪ System penetration ▪ System tampering
Industrial Espionage	Competitive Advantage	▪ Economic Exploitation ▪ Information Theft
Governments, other Government interests	Economic Espionage	▪ Intrusion on personal privacy ▪ Social Engineering ▪ System Penetration ▪ Unauthorised system

		access (access to classified, proprietary, and / or technology-related information)
Poorly Trained Employee	Unintentional errors and omissions (e.g., data entry error, programming error)	▪ Incorrect information ▪ Computer abuse ▪ Input of falsified, corrupted data ▪ Malicious code (e.g.Virus, Logic Bomb, Trojan Horse)
Disgruntled Employee	Curiosity Ego Intelligence Monetary Gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	▪ Assault on an employee ▪ Blackmail ▪ Browsing of proprietary information ▪ Computer abuse ▪ Fraud and theft ▪ Information bribery ▪ Input of falsified, corrupted data ▪ Interception ▪ Malicious code (e.g.Virus, Logic Bomb, Trojan Horse) ▪ Sale of Personal Information ▪ System bugs ▪ System Intrusion ▪ Unauthorised system access sabotage
Negligent Employee	Curiosity Unintentional errors and omissions (e.g. data entry error, programming error)	▪ Browsing of proprietary information ▪ Computer abuse ▪ Input of falsified, corrupted data ▪ Malicious code (e.g.virus, logic bomb, Trojan horse) ▪ Unauthorised system access sabotage.
Dishonest Employee	Curiosity Ego Intelligence Monetary Gain Revenge Unintentionally errors and omissions (e.g. data	▪ Assault on an employee ▪ Blackmail ▪ Browsing of proprietary information ▪ Computer Abuse ▪ Fraud and theft ▪ Information bribery

	entry error, programming error)	▪ Input of falsified, corrupted data ▪ Interception ▪ Malicious code (e.g. virus, logic bomb, Trojan horse) ▪ Sale of Personal information ▪ System bugs ▪ System Intrusion ▪ System unauthorised system access sabotage
Terminated Employee	Ego Intelligence Monetary Gain Revenge	▪ Assault on an employe ▪ Blackmail ▪ Browsing of proprietary information ▪ Computer Abuse ▪ Fraud and Theft ▪ Information bribery ▪ Input of falsified, corrupted data ▪ Interception ▪ Malicious code (e.g., Virus, logic bomb, Trojan horse) ▪ Sale of Personal information ▪ System bugs ▪ System intrusion ▪ System unauthorised system access sabotage
Hardware Failures	N/A	▪ Routine wear and tear ▪ Human carelessness
Software Failures	N/A	▪ Software defect ▪ License expiration
Telecommunication Outages	N/A	▪ Extreme weather conditions ▪ Telecom provider configuration issues ▪ Telecom provider hardware issues

For each identified vulnerability, the probability that a threat-source would be able to exploit it, may be determined based on the using the criteria presented in the Tables below-

Likelihood Rating	Threat Description
High (1.0)	The Threat – source is in place, highly motivated and sufficiently capable. There are NO counter measures to prevent the threat from being exploited.
Moderate (0.5)	The threat-source exits, but counter measures are in place that will impede successful exercise of the vulnerability, or the threat-source lacks motivation or is only marginally capable of carrying out the threat.
Low (0.1)	The threat – source lacks motivation or capability, security controls are in place to prevent successful exploitation of the threat, or significantly impede threat capability.

- CISOs of States/UTs would analyse and compile the information/data regardingThreats and furnish the same to CERT-D within the Time line for reporting given in this Document, i.e , within 24 hours of cyber threats and also in the Quarterly report for all aspects within 1st week of next month.

6. BUILDING CYBER RESILIENCE

6.1 Cyber Resilience

Cyber resilience is defined as ability of organization or business process to anticipate, withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact of such cyber-attacks.

Resilience can be defined in various ways depending upon the area of application or the type of sector under consideration. Common aspects include preparing for, preventing, or otherwise resisting an adverse event; absorbing, withstanding, or maintaining essential functions in the face of the event; recovering from the event; and adapting to (changing processes, systems, or training based on) the event, its consequences, and its implications for the future.

6.2 Protection and Resilience of Organizations Infrastructure

The Discoms need to work towards following to build cyber resiliency by adopting the following:

- Identification of key information and technology assets that support the services of that organization.
- Implementation of controls to protect those assets from cyber attack
- Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption

- Development of processes to maintain and repeatedly carry out the protection and recovery activities
- Development of appropriate measures to drive these activities
- To develop a plan for protection of organization Infrastructure and its integration with business plan and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, cyber crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To closely interact with 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) by providing it the necessary and timely information.
- To ensure identification, prioritization, assessment, remediation, and protection of organization infrastructure and key resources based on the plan for organization Information Infrastructure
- To ensure compliance to global security best practices, business continuity management and cyber Cyber Crisis Management Plan by all entities within domain of organization/ department, to reduce the risk of disruption and improve the security posture.

6.3 Cyber Resilience Components & Control Matrix

Building cyber resilience begins with effective protection of five key components within any system (i.e. key information and technology assets) - the user identity, system processes, data and hardware & software platform along with network of connections between systems. These components are defined as follows:

Identity: The representation of a user or organization within a system.

System Processes: The actual programs running within the system that may be executing on behalf of user or at root level within the operating system.

Hardware & Software Platform: Typically this will be a physical manifestation of the system as hardware and software, but it may also be a virtualized platform residing on a cloud infrastructure or in the data centre.

Data: The data either physically stored or held in memory within the system.

Network: The communication link between systems and all the protocols for establishing and securing that communication. Commonly, the gateways on the network act as enforced barriers to

communication that may act as a boundary or filter to prevent some communications while enabling others such as network firewall.

The Network infrastructure security best practices are available at **"Appendix IV "** which brings out the actions to be taken for building network resiliency by the Discoms.

6.4 Security and Safety Team of Organisation

- Man all the gates
- Plan & conduct periodic mock drills
- Coordinate with other members of team for mock drill
- Bar entry of unauthorized persons and non-essential staff
- Permit, with minimum delay, the entry of all authorized personnel, vehicles etc.
- Testing of control equipment on periodic basis
- Any other responsibility as decided by Team leader, looking into the circumstances at the time of the cyber disaster
- Account for personnel
- Obtaining authorization to access damaged facilities
- Damage Assessment of electrical equipments
- Restoring electric facilities back to normal operating conditions
- Maintaining proper documentation of the available infrastructure
- Vendor coordination etc.

6.5 Cyber Security Mock Drills

6.5.1 Objective

- To enable the participating Discoms to assess their ability and preparedness to deal with cyber crisis situations.

- To enable participating Discoms to secure their IT networks & systems and resist cyber attacks by way of effective implementation of Information Security Management System (ISMS) and Sectoral Cyber Crisis Management Plans.

- To detect cyber attacks and determine appropriate response, mitigation and recovery actions.

Cyber security mock drills are to be conducted periodically to enable Discoms to assess their preparedness and resilience in dealing with cyber crisis. These drills shall help Discoms to learn how to anticipate threats, protect their infrastructure and platform, detect incidents, withstand impacts, recover from attacks and improve their security posture.

Cyber security drill is a confidence building and learning exercise based on simulated cyber security incident scenarios that resemble occurrence of a cyber security crisis. Cyber Security drills are intended to be a collaborative and coordinated exercise between CERT-In and organizations . A proper record of the mock drills should be available with the Discoms.

In addition, cyber security mock drills would also help in

- Promoting cross sector and critical infrastructure relationships / partnerships
- Identifying preparedness gaps
- Addressing gaps by improving processes, communication and information sharing
- Enhancing response to cyber incidents Reducing cyber risk
- Create awareness among the Discoms & CERT-In besides imparting training and education for responding to cyber security incidents.

After a period of maturity in the cyber security drills at participants end, Discoms may carry out mock drills on their own with necessary guidance from CERT-In, as may be required. The Discoms may approach CERT-In for conducting regular mock drills as per the guidance on CERT-In.

CISOs of States/UTs shall furnish the report on Mock drill within the Time line for reporting given in this Document, i.e , within 07 days of Mock drill and also in the Quarterly report for all aspects within 1st week of next month.

7. INCIDENT PREVENTION

7.1 Incident Prevention and Precautionary Measures

The Discoms should implement the following precautionary measures to prevent cyber security incidents:

- **Nomination of Cyber Management Group (CMG)**

  A team of senior officers of the organization **(Annexure A**) should be nominated as CMG having the main functions as-

  - Declaration of the disaster or Emergency after consultation with CISO.

  - Periodic status review of corrective & preventive action decided after an event.

- **Nomination of Chief Information Security Officers (CISO)**

  Discoms should nominate a Chief Information Security Officers(CISO) to coordinate the security related issues/implementation within the organization as well as coordination and interface with CERT-In and Intelligence Bureau. The main function of CISO would be

  - To create secure cyber ecosystem
  - To implement cyber security measures as per ISO 27001 framework and coordinate cyber security related issues
  - Define contingency plan / disaster recovery plan
  - Damage Assessment in case of a disaster
  - Declaration of the disaster or Emergency in absence of BCM Head
  - Communication to the CMG Head
  - Pre & Post Coordination with various teams i.e Recovery Team, Security & safety team, Administrative Team, Infrastructure Team
  - Monitoring the recovery process and communicate the same to CMG Head
  - Conduct periodic CMG training and deployment in the event of a disruptive situation requiring plan activation
  - Conduct periodic mock drills
  - Contact fire station
  - Prepare Recovery Test Plan etc.

- **Information Security Policy and Implementation of Best Practices**

  Every Discom should formulate Information Security Policy and identify appropriate information security management practices keeping in view their business needs. The identified practices should be implemented. The critical sectors should necessarily implement Information Security Management System (ISMS) Best Practices as per ISO 27001. The following steps should be taken into account while implementing the ISMS:

  - The Information Security Policy should clearly identify the three components namely process, technology and mitigation of incidents
  - Undertake comprehensive Risk Assessment of the Information Technology/Network assets
  - Implement appropriate security control measures such as those defined in the ISO 27001 which include Service Level Agreements with various service providers.

- **Business Continuity Plan (BCP)**

  Define Contingency Plan (Business Continuity Plan) to counteract interruptions to business operations/activities and protect critical operations/business processes from effect of major disaster.

- **Disaster Recovery Plan (DRP)**

  Establish Disaster Recovery (DR) Plans with adequate redundancy to take over the operation in case of the need.

- **Security of Information Infrastructure and Network**

  The Discoms should secure the entire IT infrastructure including the network by implementing appropriate hardening measures. Guidelines on "Important Security Controls for Effective Cyber Security and Continuous Security Policy Compliance" are given in**Appendix II.**

  - Security devices may be installed at all levels. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure should be secured by installing appropriate perimeter security devices such as firewalls, Intrusion Prevention System and anti-virus system. Configuration of these security devices should be checked at the time of installation as well as at the time of significant changes for the needed functionalities and security features.

  - The security mechanism should include appropriate devices and methods to log and monitor the events to detect network scanning, probing, reconnaissance and flooding attempts on the IT infrastructure. These attempts should be regularly reviewed and analyzed for initiating necessary preventive measures.

  - The remote monitoring and maintenance of the security devices should be strictly restricted to authorized persons only.

  - The software at network, system and application level should be regularly upgraded by applying/installing upgrades and updates

- **Network Traffic Scanning**

  The network traffic scanning technique provides visibility into the state of the network and identifies deviations from baselines that may indicate abnormal or suspicious behaviour. The traffic

patterns provides leads on the targeted ports such as 80,25,23 which gives leads to the attack targeted on the services like 'http', 'smtp', 'ftp' or spread of malicious code like 'Bots'. For example, if it is observed that suddenly there is rise of traffic on the port 25, associated with e-mail service; this may indicate that e-mail based worm is spreading at a high speed. A sudden traffic rise on the IRC ports may indicate surge in the 'Botnet activity'. The network traffic flows thus gives the exact portrait of the communications happening on the network, irrespective of their state whether a normal or an anomaly. Majority of attacks such as Distributed Denial of Service (DDoS), Worm, Spyware, Botnet detection, malicious scan of any nature etc. at the organisation level could thus be detected by analyzing network flow-data traffic. Industry solutions are available to collect and analyze network flow traffic on the gateway routers and switches. Network flow data DO NOT contain any content data and is totally non-intrusive on the network. The organisations may use network flow data for security analysis to detect attacks onto the networks

- **Isolation of critical networks**

  The critical sector organisations, Defence and sensitive organisations use separate physical networks for operations of critical infrastructure and performing their functions. The critical networks should be isolated from other production networks connected over Intranet/Internet. At no point of time the gap between critical network and production network over Intranet/ Internet be compromised. No transfer of data from a Intranet/Internet based network to a critical network or vice versa be allowed. In case required, it should be under strict control and thoroughly screened. There are malicious codes specifically designed to target critical infrastructure systems by means of spreading through systems connected over internet. Risk assessment and regular monitoring of critical networks is essential for security of critical infrastructure.

- **Implementation of Security Guidelines issued by Ministry of Home Affairs, Intelligence Bureau, respective Ministries and agencies like CERT-In**

  Discoms should implement Security Guidelines and advisories both with respect to cyber and physical security issued by Ministry of Home Affairs, CERT-In, CERT-D, MOP and other agencies from time to time.

- **Manpower Engagement in Cyber Security activities of organization**

(a) Screening and Background check

Background verification checks on all employees engaged in implementing and monitoring cyber security and cyber crisis management plan, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the requirements of task and responsibilities, the classification of the information to be accessed, and the perceived risks.

Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:

a. availability of satisfactory character references, e.g. one business and one personal
b. check (for completeness and accuracy) of the applicant's curriculum vitae
c. confirmation of claimed academic and professional qualifications
d. independent identity check (passport or similar document)
e. more detailed checks, such as credit checks or checks of criminal records

Information security management practices based on ISO 27001 standard provide guidance with regard to screening and background checks in respect of employees and other personnel. The organisation may consider following ISO 27001 best practices.

(b) Roles and responsibilities

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy. Security roles and responsibilities should include the requirement to:

a. implement and act in accordance with the organisation's information security policies.
b. protect assets from unauthorized access, disclosure, modification, destruction or interference.
c. execute particular security processes or activities.
d. ensure responsibility is assigned to the individual for

actions taken.

e. report security events or potential events or other security risks to the organisation.

Security roles and responsibilities should be defined and clearly communicated to job candidates during the pre-employment process. Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organisation's employment process, e.g. engaged via a third party organisation, should also be clearly defined and communicated.

- **Audit of IT infrastructure**

  - Discoms should undertake comprehensive security audit of the entire IT infrastructure including network and applications by independent auditingorganisations to discover the gaps with respect to best security practices and takeappropriate corrective actions. Apanel of IT security auditingorganisations who provide IT security audit is available on CERT-In website www.cert-in.org.in.

  - The audit of the system should be undertaken at least once in a year and also as and when any significant addition or alteration in respect of hardware, software, network resources, policies and configurations of systems and sub systems are affected.

  - Following the audit, compliance with the security policy should be documented in the annual report.

- **Assurance Framework**

  - **3rd Party Audit –** Discomsshould undertake comprehensive security audit of the entire IT infrastructure including network and applications by independent auditing organizations to discover the gaps with respect to best security practices and take appropriate corrective actions.

  - **Internal Audit –** Periodic internal audit shall be conducted at least once a year.

  - **VAPT –** Vulnerability Assessment and penetration testing shall be conducted for critical IT infrastructure and applications.

- **Internal testing –** Shall be conducted for any change or new purchase of infrastructure and application in respect of hardware, software, network resources, policies and configurations of systems and sub systems are affected.

- **Mock Drill –**Periodic mock drills shall be conducted to assess their preparedness and resilience in dealing with cyber crisis. These drills shall help organizations to learn how to anticipate threats, protect their infrastructure and platform, detect incidents, withstand impacts, recover from attacks and improve their security posture.

- **Internal Mock Drills –** can be conducted by creating an environment (Eg Staging server, Simulation Environment, Cluster etc).

- **External Mock Drill –** In coordination with sectoral CERT-In, NCIIPC etc

- **Security Training and Awareness**

  All employees of the Discoms and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function Awareness training should commence with a formal induction process designed to introduce the organisation's security policies and expectations before access to information or services is granted Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g.

  - Latest Technologies and threats
  - Implementation of Security Policy
  - Physical Security Procedures
  - Access Control Procedures
  - Use of Licensed Software Packages
  - Malicious code and Botnets and their prevention
  - Reporting and mitigation of incidents (as in the Format at Annexure-E ,F and G)
  - Cyber Crisis Management
  - Implementation of Information Security Guidelines

  The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills. Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role

and responsibility in event of violation of Standard Information Security guidelines.

- **Coordination and incidents information sharing**

  All Discoms should strive to improve coordination and communication with CERT-In, CERT-D, stakeholders, ministry/department and other designated agencies and should share all information pertaining to cyber security incidents(in the Format at Annexure-E ,F and G) with CERT-In and other designated agencies. Cyber Security exercises conducted by CERT-In may be used as a tool for improving the coordination and information sharing.

- **Deployment of Information Security Experts**

  Given the size of the problem and increasing threats of cyber terrorism, there is a need to deploy more experts in this field. A large number of security experts could be working on emerging vulnerabilities and effective defences. Periodic training may be provided to information security experts to update the skills with respect to latest technologies/threats and implementations.

7.2 ITSecurity Best Practices Compliance-Levels of Assurance

In order to assist Discoms to follow a roadmap for progressively achieving compliance and assurance w.r.t. IT security best practices, different levels of assurance have been conceived. Using these levels of assurance and the methods of verification, the Discoms can carry out self assessment with regard to their present status of compliance assurance and declare the same accordingly. It is expected that these levels of assurance will also help theorganizations in improving the maturity of their IT security management system as well as enhancing predictability and proactive nature of their system. Levels of Assurance are as under-

Sl.No.	Assurance Level	Description	Methods of verification
1.	Level 1 – Assurance of Systematic approach to IT security	Discom is aware of IT security best practices and has defined and documented its IT security plan, policies and procedures covering people, products, technology and processes. Evidence in the form of appropriate references to the IT security plan, policies and procedures exists.	▪ Questionnaire based check-list. ▪ Remote or on-site desk-top assessment of check-list response.

2.	Level 2 – Assurance of compliance to IT security best practices	Discom has implemented IT security best practices based on clear understanding of risks, threats & vulnerabilities and the compliance has been verified by a self-assessment process or by an independent third party auditing organisation.	▪ Self – assessment report or independent third party audit report.
3.	Level 3 – Assurance of an adequate IT security posture.	Discom has conducted IT security posture verification (by way of security testing of its IT infrastructure involving VA / PT, application security testing, code walkthroughs etc) by an independent third party auditing organization.	▪ Security testing of IT infrastructure involving VA/PT, application security testing, code walk throughs etc., and a report is available for the same.
	Level 3+ - Assurance of IT security crisis response & ability to resist cyber attacks.	Discom has participated in the cyber security drills to have its IT security crisis response & ability to resist cyber attacks tested and verified.	▪ Share cyber security drills results with CERT-In.
4.	Level 4 – Assurance of proactive IT security monitoring and mitigation of threats and vulnerabilities	Discom has implemented mechanisms for proactive IT security monitoring and mitigation of threats and vulnerabilities. These mechanisms allow for technology based monitoring and analysis of IT security incidents for proactive preventive actions (Ex. IPS / IDS, SIEM, flow based analysis etc.)	▪ Technology based monitoring and analysis (Ex. IPS / IDS, SIEM, flow based analysis etc) evidenced in terms of governance reports and management feedback.
	Level 4+ - Assurrance of proactive sharing and mitigation of IT security threats &	Discom has implemented mechanisms for proactive sharing mitigation of IT security threats & vulnerabilities by way of active collaboration with CERT-In, NCIIPC, ISACs etc.	▪ Collaboration with CERT-In, NCIIPC, ISACs etc., evidence in terms of communication trail.

	vulnerabilities. Level 4++ - Assurance of proactive prediction of residual IT security risks & attack paths and mitigation	Discom has implemented mechanisms for proactive prediction of residual IT security risks & attack paths and mitigation of IT Security threats and vulnerabilities.	▪ Attack path analysis.

7.3 Post Incident Activity

After restoring a system to normal operation, it is also important to perform the necessary follow up action. Actions may include evaluation of the damage caused, system refinement to prevent recurrence of the incident, security policies and procedures update and case investigation for subsequent prosecution.

Documentation of the entire incident cycle is also one of the critical parts of the Post Incident Activity since this forms a feed for the Preparation phase as can be understood from the incident lifecycle flow diagram. The Post-Incident Analysis Document should answer the following questions:

- Exact description of the incident - what happened, when and where?
- How was the incident dealt with and was the process and procedure followed adequate?
- What were the steps involved in each phase of the life cycle?
- What were the learning from the incident?
- What should be the corrective Action plan to be adopted?
- What additional tools, controls, process or procedures are required to prevent future occurrences of the incident?
- The Incident Report will be shared with CERT-In for future precaution and mitigation of similar attacks which in turn along with concerned agencies will improve the Incident response and coordination mechanism based on the Incident report. All critical organisations to implement infrastructure protection improvements resulting from postmortem reviews or other protection improvement mechanisms.
- Discoms should nominate an officer as Chief Information Security Officers(CISO) and intimate contact the details-such as Phone, fax nos, Mobile nos and Emails to CERT-D immediately, if not yet submitted.
- CISOs of States/UTs shall furnish the report (in the Format at Annexure-E,F and G) related to all these above within the Time line for reporting given

in this Document, i.e , within 07 days and also in the Quarterly report for all aspects within 1st week of next month.

8. CYBER CRISIS RECOGNITION, MITIGATION AND MANAGEMENT

8.1 Incident Recognition

Recognition of cyber crisis depends on clearly identifying the cyber incidents within the Distribution Sector/Discoms area of operation. The crisis arising out of cyber attacks may be categorized and prioritized from level 1 to Level 4. Each subsequent level will follow preceding one. No level other than level **1** will come in isolation.

Table : Cyber Security Emergency – Level of Concern

Threat Level	Condition
Level 1 Guarded Scope: Individual Organisation	Perceptible change/variation in system performance and discovery of critical/non critical vulnerabilities/exploits and attacks that can affect normal operation of network and IT systems of individual Discom such as: ➢ Targeted attacks and espionage activities. ➢ Identity theft (Phishing, spoofing, social engineering etc.) ➢ Web defacements and Application level attacks ➢ Visible signs of malicious programs (viruses/worms/ Bots/ malware/Keyloggers/Spyware/etc) ➢ Detection of new and advanced malware infections ➢ Attempts for exploitation of zero-day vulnerabilities ➢ Denial of service attacks (DoS) ➢ Distributed Denial of Service (DDoS) and Distributed Reflection Denial of Service (DrDoS) ➢ Hacking of IT systems such as computers systems, Servers (Mail, Web, Database etc) and Routers. ➢ Spam
Level 2 Elevated **Scope: Multiple Organisation**	Perceptible change/variation in network/ system performance and abnormal surge in network traffic affecting IT infrastructure of multiple organizations/ Discoms simultaneously due to: ➢ Targeted attacks and espionage ➢ Large scale infection of viruses/worms/ Bots/malware/ Key loggers/Spyware for malicious and espionage activities ➢ Detection of domain specific malwares like "stuxnet" targeting Industrial Control Systems ➢ Focused attempts of network scanning and penetration ➢ DDoS attacks and Distributed Reflection Denial of Service (DrDoS) ➢ Attacks on Domain Name Servers, Mail Servers, Databases,

	Routers etc. ➢ Large scale web-application attacks like backdooring and defacement. ➢ Attacks on Trust infrastructure ➢ Attack on the IT infrastructure of a Critical Information System ➢ Infection of computer systems and/or Programmable Logic Controllers (PLCs). ➢ Abnormal functioning of SCADA/ industrial Control Systems
Level 3 Heightened Scope: State/ Multiple States	Significant breakdown of supplies or services essential to the life of the citizens including but not limited to financial, Government, transport, energy or communication due to focused cyber attacks on infrastructure of critical sectorand Government across a state or multiple states.
Level 4 Serious Scope: Entire Nation	Cyber espionage on sensitive Government organisations or significant/complete breakdown of supplies or services essential to the life of the citizens including but not limited to financial, Government, national defence, transport, energy or communication dueto focused cyber attacks on infrastructure of critical sector and Government across the nation.

8.2 Strategic issues in cyber crisis management and business continuity

- Implementation of appropriate measures to reduce the likelihood of incidents occurring and/or reduce the potential effects of those incidents
- Taking due account of the resilience and mitigation measures
- Providing continuity for critical services during and following an incident
- Taking into account those activities that have not been identified as critical

The effectiveness of above actions depends on a range of factors such as:

- The maximum tolerable period of disruption of a critical activity
- The costs of implementing a strategy and
- Consequences of inaction

8.3 Incident Response and Mitigation

The steps necessary to mitigate crisis will vary with respect to nature and severity of crisis. The nature of crisis/contingency affecting the systems of individual organisation, multiple organisations, states and nation leading to crisis of different levels, authorities responsible for taking steps for mitigation along with agencies that support mitigation actions are outlines as under. Respective authorities responsible for

mitigation of a crisis will report the incident to the designated supporting organisations and also follow step-wise approach for mitigation vis-a-vis nature of crisis/contingency.

Nature and Severity of crisis, Authorities responsible and steps for Mitigation

Security Level of Crisis	Nature of Crisis	Authorities responsible and Steps for mitigation
Level 1 Response Scope : Individual Organisation	All Attacks	**Responsibility: Affected Organisation** **Steps to be taken by the Affected Organisations** • Notify incidents to respective Administrative Ministry / Department / Sectoral CERT • Monitor and detect anomalous behaviour and degradation of service in network and systems • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of ail the logs of affected systems and network devices, suspicious files, data, traffic. trends wherever applicable to CERT-ln / NTRO • Consult incident reports or vulnerability reports for specific advisories on the suspected behaviour as published by CERT-ln and implement those in the affected networks and systems • Segregate networks (LAN / WAN) and perimeter security devices and systems. Check for configuration vis-Prescribed against each attacks mentioned below • Change all user /root / administrator passwords in all systems and network devices • Install updated software patches on Operating System and all other system software running

		on computer servers and Personal computers in the network
	Web application Attacks	**Mitigation Steps - Specific to nature of cyber attacks/crisis** If possible, isolate affected server from Internet or disable the affected module in application. • Scan all files for web shells or any malicious footprint. • Take a copy of all the logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends • Identify the type of attack and vulnerability exploited • Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration • Report to CERT-In with webserver logs and dump of the vulnerable web application
	Virus / Worm / Spyware / Botnet Attacks	•Isolate affected systems/network segments fromInternet • Scan all files in the suspected systems, including emails for viruses • Clean the affected systems with the updated antivirus software • Install updated antivirus/anti-spyware on all systems (servers and Personal Computers)
	DoS/DDoS/NTP based DrDoS attacks	• Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends. • Identify the type of attack such as flooding of particular types of packets/ requests • Allocate traffic to unaffected available network paths, if possible, to continue the services

		• Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • Install updated software patches on all the network devices such as Routers, Firewalls, IDS, IPS and switches
	High Energy RF-based DoS attacks	• Use a network management solution capable of alerting on a based DoS Attacks degraded signal noise ratio or the increased noise levels in theairwaves. • Identify the other devices due to which RF interference occurs and physically remove them • Deploy IPS/IDS to detect rouge access points
	DNS Attacks	• Check for version updates at the DNS server and install latestsoftware patches • Implement spoofing countermeasures • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Adopt source IP address verification • Implement DNSSec
	Attack attempts / scans on Servers, Routers, Firewall, etc.,	• Check for effectiveness of filtering rules in the routers, firewalland IPS and reconfigure if required • Check the logs of these devices for source of attack
	Phishing Attacks	• Keep watch on phishing sites • Alert customers regarding the known phishing sites

		• Encourage customers to use anti-phishing enabled browsers • Shutdown phishing sites in coordination with concerned ISP and CERT-In
	Mail Server Attacks	• Deploy hot standby mail servers in physically separatednetworks and places which can be made operational when the main server is attacked • Disable all other ports and services on mail servers • Enforce strong password policy and encourage users to change passwords periodically
	Attacks on Critical Infrastructure and associated SCADA / Industrial Control Systems, through sophisticated malware such as Stuxnet / Duqu / Nitro / Flame	• Check for signs of infection in computer systems in general • Isolate infected systems from all networks immediately • Report the incident to local IR Team/ CERT-In at the earliest.Consult relevant advisories of CERT-In and follow specific measures suggested therein • Take a forensic image and send to local IR Team/CERT-In • Clean the affected systems with the updated antivirus software • Install updated antivirus/anti-spyware on all systems (servers and Personal Computers) • Examine the vectors of propagation of worms - Removal media, network shares and other sneaker net systems • Examine the critical SCADA/ industrial Control Systems/PLCs for abnormal functionality • Examine Critical systems of Industrial process for abnormal functionality • Examine network traffic towards malicious domains/websites/hosts that are

		identified as Command & Control • Trace the infected PLCs/Systems and isolate immediately • Review the security controls and processes to ensure isolation of critical networks from other infrastructure • Follow guidelines mentioned under Section 5.1 in respect of dealing with air gap for isolation of control systems from other networks **On report of the incident, CERT-in would take following supportive actions** • Analyse the information/logs received from affected organisations • Check for latest patches/updates from various sources including vendors (as per format in Annexure-B &C) • Consult the vendors and other sources (as per format in Annexure-B &C) to help the organisations in resolving the problems • Document the vulnerability information and disseminate • In case of phishing attacks, take appropriate action to block the phishing sites by interfacing with concerned organisations, ISPs and international CERTs • In case of Botnet attacks, locate Command & Control server and initiate action to disable the same in coordination with ISPs **On report of the incident, NTRO would take following supportive actions** • Carryout all response activities in respect of Law Enforcement and Security agencies, Space, Atomic Energy, Defence Research,

		Defence Production and their critical infrastructure
Level 2 Response Scope : Multiple Organisation	All attacks	**Responsibility :** **Respective Administrative Ministry / Department** **Steps to be taken by affected organisations** **General** •Notify incidents to respective administrative Ministry/Department • Monitor and detect anomalous behavior and degradation of service in network and systems • Take all logs (system application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In/ NTRO. • Consult incident reports or vulnerability reports for specific advisories on the suspected behaviour as published by CERT-In and implement those in the affected networks and systems • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration vis-a-vis ongoing attack. • Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks mentioned below • Change all user/root/administrator passwords in all systems and network devices If possible, isolate affected server fromInternet or disable theattacks
	Web application	

	attacks	affected module in application. Scan all files for webshells or any malicious footprint. Take a copy of all the logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends Identify the type of attack and vulnerability exploited Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration • Report to CERT-In with webserver logs and dump of the vulnerable webapplication
	Virus /Worm /Spyware/Botnet attacks	• Isolate affected systems/network segments from LAN/Internet • Scan all files in the suspected systems, including emails for viruses • Install Antivirus/anti-spyware updates • Clean the affected systems with the updated antivirus software • Block the infection/attack vectors through IPS/Firew
	DoS/DDoS/NTP/Based DrDoS attacks	• Shift critical services to alternate channels • Incase of IP based attacks, shift hosting of affecteddifferent ISPs • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP • Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends • Install updated patches on the

		network devices.
	High Energy RF-based DoS attacks	• Use a network management solution capable of alerting on a degraded signal noise ratio orthe increased noise levels in the airwaves. • Identify the other devices due to which RF interference occurs and physically remove them. • Relocate the Access Points incase of Wireless Networks
	DNS Attack	• Change the preferred DNS server • Implement Source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827) • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Run separate DELEGATED and RESOLVING name servers • Disable Recursion on DNS server authoritative for the zone • Restrict zone transfers to slave name servers and other authorized software • Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server. • Check for version updates at the DNS server and install latest patches • Implement split DNS architecture • Implement anycast technology on DNS server
	Attacks on Servers, Router, Firewall, etc.,	• Check for the effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required • Replace compromised systems with trusted ones • Check for version updates/patches and install latest patches for

		routers, firewall and IPS • Check the logs of these devices for source of attack •Activate hot standby mail servers and direct mail traffic appropriately
	Mail Server Attacks	• Examine incoming emails for social engineering attempts/spoofing through header/content analysis
	Advanced Targeted Attacks	• Report suspicious emails with attachments and headers to Administrator/ local IRTeam/CERT-In • Identify the target entities and sensitize them about the targeted attacks • Isolate systems found to be connecting to suspicious domains/hosts after preserving volatile data and create forensic images for further analysis • Based on analysis of incident, apply appropriate security controls such as patching the targeted application, updating antivirus signatures to detectthe crafted malware and detecting connections to call back domains/hosts through perimeter devices • Regularly monitor events and traffic at host/network level to detect malicious activities and report any suspicious activitiesto local IR Team/CERT-In
	Attacks on critical Infrastructure and associated SCADA / Industrial Control Systems, through sophisticated malware	•Check for signs of infection in computer systems in general •Isolate infected systems from all networks immediately •Report the incident to local IR Team/ CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein •Take a forensic image and send to local IR Team/CERT-In

	such as Stuxnet/Duqu/Nitro	• Clean the affected systems with the updated antivirus software • Install updated Antivirus/anti-spyware on all systems (servers and Personal Computers) • Examine the vectors of propagation of worms - Removal media, network shares and other sneakernet systems. • Examine the critical SCADA/industrial Control Systems/PLCs for abnormal functionality • Examine Critical systems of Industrial process for abnormal functionality • Examine network traffic towards malicious domains/websites/hosts that are identified as Command & Control • Trace the infected PLCs/Systems and isolate immediately • Review the security controls and processes to ensure isolation of critical networks from other infrastructure • Follow guidelines mentioned under Section 5.1 in respect of dealing with air gap for isolation of control systems from other networks • Regularly track network connections and probing attempts in normal situations
	Compromise of trust infrastructure Certifying Authority, Authentication mechanism, compromise of key	In case of report of compromise or circulation of rogue certificate: • Immediately report the incident to concerned Ministry/Department and CERT-In • Revoke the compromised keys • Announce revocation notification at the earliest • Review the network/system security posture • Deploy appropriate mechanism to check and certify correctness of cryptographic functions

	management.	• Generate fresh keys/certificates • Conduct appropriate awareness campaign to notify all users • Providers of App stores will need to pay special attention to implementation of trust and security functions in order to avoid serious impact on the user trust **On report of the incident, CERT-In would take following supportive actions** • Analyse and correlate the information/ logs received from affected organisations • Check for latest patches/updates of system software, network devices and antivirus signatures from vendors and other sources(as per format in Annexure-B &C) • Consult the vendors and other sources (as per format in Annexure-B &C) to help the organisations in resolving the problems • Contact the concerned CERTs or ISPs from where the attacks are originating for blocking in case of DoS/DDoS attacks • Document the resultant vulnerability, prepare vulnerability notes and disseminate to cyber community **On report of the incident, NTRO would take following supportive actions** • Carryout all response activities in respect of Law Enforcement and Security agencies, Space, Atomic Energy, Defence Research, Defence Production and their critical infrastructure

		On report of the incident, MHA would take following supportive actions • MHA to assist CERT-In, DoT, MoD and NTRO by providing all intelligence inputs and facilitating monitoring of networks • MHA would provide physical security protection as deemed necessary **On report of the incident, DoT would take following supportive actions** • To coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In, NTRO, MoD, MHA and other government agencies **On report of the incident, R&AW would take following supportive actions** • R&AW to assist CERT-In, MoD and NTRO by providing all external intelligence inputs.
Level 3 Response Scope : State / Multiple States	All Attacks	**Responsibility:** **Respective Administrative Ministry/ Department** • Notify the incidents to National Crisis Management Committee (NCMC) • Depending up on the situation request for the meeting of NCMC **Steps to be taken by affected Organisations** Notify incidents to respective administrative Ministry/Department Implement the Contingency Plan

		Deploy onsite response team on 24X7 basis • Limit the access to systems and networks from outside in consultation with concerned ISPs • Enable hot stand-by systems/servers with alternate Traffic paths • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration visa-vis ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks in level 1 &2 • Carry out file integrity checks on all the systems • Restore systems from trusted backups and validate the systems and networks before connecting to Internet. • Change all user/root/administrator passwords in all systems and network devices **Actions to be undertaken by CERT-In** • Analyse the on-going attacks/traffic and seek assistance from Vendors and other CERTs if required • Work closely with affected organisations, ISPs and other agencies to provide all necessary help to mitigate the incident Advise appropriate measures to isolate systems/networks at organisations/ regions

Level 4 Response Scope : Entire Nation	All Attacks	**Responsibility: Respective Administrative Ministry/ Department** Notify the incidents to NCMC Request for the meeting of NCMC **Steps to be taken by affected Organisations** Carry out all the steps indicated in level 3 Implement directives of NCMC, respective administrative Ministry/ Department Implement specific advisories and instructions issued by CERT-In, NTRO and other designated agencies

8.3 Media Management

A media forms a vital link between those responding to crisis situation and the outside world. Besides this, media also can help in educating all concerns about crisis prevention and preparedness. It is recognized that unbiased and comprehensive media coverage can effectively aid the crisis response & resolution process and also enhance public confidence in the ability of organisations to respond to crisis. Accordingly media management is a crucial issue in terms of pre-incidents as well as post incident information flow. In order to make best possible use of this vital link, it is necessary that media is given clear information and regular updates to enable them to perceive right picture and proportion of the crisis. In this context, it is also necessary for the organisations responding to cyber security incidents to identify responsible person of suitable level that has access to correct & updated information and is adequately trained for proper & consistent communication and avoid contradiction at all times.

Appendix –I

Information Security Management System (ISMS)

(a) Information Security and Management

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organisation are met.

An Information Security Management System (ISMS) is a systematic approach to managing sensitive information of an organization (Discom) so that it remains secure. The adoption of an information security management system is a strategic decision for an organization. It encompasses people, processes and IT systems.

(b) Information Security Standards

International Organisation for Standardization (ISO) has published the following standards to enable organisations to establish and implement ISMS effectively:

ISO 27001 - Information Security Management Systems - Requirements
ISO 27002 - Code of Practice for Information Security Management

These standards codify industry experience and security best practices, and are applicable to all types of organisations, irrespective of their size or business.

(c) National Cyber security Policy, 2013

In light of the growth of IT sector in the country, the National Cyber Security Policy of India 2013 was announced by Indian Government in 2013 yet its actual implementation is still missing. As a result fields like e-governance and e-commerce are still risky and may require cyber insurance in the near future. Its important features include:

- To build secure and resilient cyber space
- Creating a secure cyber ecosystem, generate trust in IT transactions.
- Creation of National Critical Information Infrastructure Protection Center (NCIIPC)
- Indigenous technological solutions
- Testing of ICT products and certifying them/ Validated products etc.

Countering cyber crimes is a coordinated effort on the part of several agencies in the Ministry of Home Affairs and in the Ministry of Electronics and Information Technology. The law enforcement agencies such as the CBI, IB , state police organizations and other specialised organizations such as Indian Computer Emergency Response Team (CERT-In) are the main organizations to tackle cyber crimes.

Appendix –II

Important Security Controls for Effective Cyber Security and Continuous Security Policy Compliance

"Establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms.

Securing our Nation against cyber attacks has become one of the highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks. Furthermore, for those external attacks that are successful, defenses must be capable of thwarting, detecting, and responding to follow-on attacks on internal networks as attackers spread inside a compromised network.

Security Controls for Effective Cyber Security and Continuous Security Policy Compliance

- Inventory of authorized and unauthorized hardware.
- Inventory of authorized and unauthorized software.
- Secure configurations for hardware and software for which such configurations are available.
- Secure configurations of network devices, such as firewalls and routers. Boundary defense.
- Maintenance and analysis of complete security audit logs.
- Application software security.
- Controlled use of administrative privileges.
- Controlled access based on need to know.
- Continuous vulnerability testing and remediation.
- Dormant account monitoring and control.
- Anti-malware defenses.
- Limitation and control of ports, protocols and services.
- Wireless device control.
- Data-leakage protection.
- Secure network engineering.
- Red-team exercises.
- Incident-response capability.
- Assured data backups.
- Security-skills assessment and training to fill gaps.

In general, Discoms should examine all twenty control areas against their current status and develop a Discom specific plan to implement the controls. Organizations with limited information security programs may choose to address certain aspects of the controls in order to make rapid progress and to build momentum within their information security program.

Insider Threats vs. Outsider Threats

A quick review of the critical controls may focus on outsider threats and may, therefore, not fully deal with insider attacks. In reality, the insider threat is well covered in these controls in two ways. First, specific controls such as network segmentation, control of administrative rights, enforcement of need to know, data leakage protection, and effective incident response all directly address the key ways that insider threats can be mitigated. Second, the insider and outsider threats are merging as outsiders are more and more easily penetrating the security perimeters and becoming "insiders." All of the controls that limit unauthorized access within the organization work effectively to mitigate both insider and outsider threats. It is important to note that these controls are meant to deal with multiple kinds of computer attackers, including but not limited to malicious internal employees and contractors, independent individual external actors, organized crime groups, terrorists, and nation state actors, as well as mixes of these different threats.

Periodic and Continual Testing of Controls

Each control included in this document describes a series of tests that Discoms can conduct on a periodic or, in some cases, continual basis to ensure that appropriate defenses are in place.

Appendix –III

Organisational Cyber Crisis Management Plans (CCMP)

1 Identify a member of senior management as a **'Chief Information SecurityOfficer (CISO)'** to coordinate security policy compliance efforts across the Discoms and interact regularly with CERT-In and sectoral 'Point of Contact'

2 Establish a Crisis Management Group, on the lines of Sectoral Crisis Management Committee, with head of Discom as its Chairman

3 Prepare a list of CII and contact persons complete with up-to-date contact details

4 Prepare an Discom level CMP on the lines of CMP of CERT-D/ CERT-In, outlining roles, responsibilities of various stakeholders, coordination process etc.

5 Implement the CMP, including security best practices and specific action points as outlined below:

- Prepare a **Security plan** and implement Security control measures as per **ISO27001 standard** and other guidelines/standards as appropriate

- Carry out **periodic IT security risk assessments** and determine acceptable level of risks, consistent with business impact assessment and criticality of business functions

- Develop and implement a **business continuity strategy** and **contingency plan** for IT systems

- Develop and implement **ICT disaster recovery** and **security incident management processes**

- **Periodically test and evaluate** the adequacy and effectiveness of technicalsecurity control measures, especially after each significant change to the ITapplications/systems/networks and it can include:

  i. Penetration testing (both announced and unannounced)
  ii. Vulnerability assessment
  iii. Application security testing
  iv. Web security testing
  v. Carry out **audit of information infrastructure** on an annual basis and when there is a major upgradation/change in IT infrastructure, by an independent IT security auditor (Ref. to list of CERT-In empanelled IT security auditing organizations on

CERT-In web site at http://www.cert-in.org.in)

6 Report to CERT-In cyber security incidents as and when they occur and status of cyber security periodically and take part in cyber security mock drills

7 Participate in the cyber security drills to be conducted by CERT-In on a regular basis **Cyber Resilience Control Matrix**

Component	Protect	Detect	Contain	Recover
Identity	• Controlled access based on need-to-know • Enforce Strong password Policy • Multi Factor Authentication • Usage of Digital Certificates	• Maintenance and Analysis of Complete security events and audit logs • Privilege escalation monitoring and alerting	• Minimize the invalid logon counts • Revocation of digital certificates • Change access contra on all devices • Continuous account monitoring and deactivating the dormant accounts	• Offline recovery procedures for logging into accounts • Alternative indicators
System Process	• Effective Security Patch Updating Mechanism on applications etc., • Following Best Security practices during software development Lifecycle • Secure Configuration • Malware defences	• Forensic Memory Analysis • File Integrity Checking • Malware Analysis	• Policy based restrictions on process actions • Reconfiguration of settings • Usage of Sandbox Security Mechanism	• Assured Data backups • Clustering • Recovery Time • Objectives (RTO) for system and support • Manual / automated takeover to activate alternative IT Provision • Use of Unstaffed sites as opposed to staffed sites
Hardware and Software platform	• Asset Inventory (asset classification and	• Continuous vulnerability testing and remediation	• Remote Wipe on failed logins • Code Integrity Checks to help	• Baseline remote image deployment

	management) • Supply chain protections • Regular review of configuration files : OS / middleware • Boot process integrity check	• Tamper detection mechanism • Platform Security Assessment (Review of System architecture / operating system configuration / Security Management controls / system configuration	prevent malicious code from being injected into system files or into the kernel at load / run time	• Usage of virtual environment • Assured Back-up and replication • Replacing Compromised files with clean versions
Data	• Database access control : Regular review of access privileges to users of the database / use of biometric technology • Data Encryption while in-process, handling, storage or transit • Data masking (for sensitive information)	• Monitoring Data flow to detect data leakage • Forensic disk imaging and analysis • Monitoring remote access • Database integrity checking	• Application restriction monitoring • Data Leakage prevention (System designed to detect potential data leakage while in-process, handling, storage or transit • Access control on database	• Assured Data back-ups and physical segregation of back-up • Storage replication Mirroring / Cloning • Database reprocessing (Going back to a known point of database Activity before the problem occurred and reprocessing work from that point forward)
Network	• Limitation and control of ports, protocols and services • Wireless Device Control	• Centralised network log analysis for wired & wireless networks	• Isolation of trusted • Networks from untrusted networks. • Denial of	• Alternate network routing • Alternative Cloud communicati

	• Following Best Practices for Secure configuration of network devices	• Honey-net • Network Scanning and Analysis	service offload to ISP and Cloud • Reconfiguration of impacted network devices • Modify access control (all user / root / administrator passwords) in all systems and network devices	ons • Usage of devices in cluster mode / load balancing mode

Appendix –IV

Network infrastructure Security Best Practices

ICT network infrastructure protection is necessary to achieve the objective of any organization including Distribution companies . Network infrastructure must provide secure, available, and reliable data. It is required to follow security best practices to reduce the' vulnerabilities and protect the network infrastructure from cyber attacks and operational challenges. The first step towards network security is to secure the infrastructure itself. This includes actions like passwords, securing device access etc, something applicable to all layers and subsets of the network.

The following are the key areas of baseline security:

1. Network infrastructure Edge Security.
2. Infrastructure device access protection.
3. Routing infrastructure Security.
4. Device resiliency and survivability.
5. Monitoring, Analysis and Correlation,
6. Network policy enforcement,
7. Switching infrastructure security,
8. Threat Control and Containment
9. Endpoints Security
10. Secure Third-Party Connectivity

Best practices for network infrastructure security:

1. Secure the Network Infrastructure Edge:

Network Infrastructure edge like the Internet edge which provides connectivity to the internet and that acts as the gateway for the organisation to the rest of the cyberspace and WAN edge of infrastructure provides geographically remote users with access to the organization network and services are important to consider when designing secure network infrastructure. At the edge, data usually flow from one trust zone to another trust zone, which exposes network to the threats also failure of network infrastructure edge can impact availability of the network. The availability and overall security of the infrastructure edge is the key for business continuity.

Following are good practices to be followed by the Discoms to secure the network infrastructure edge:

Isolate and Encrypt WAN Traffic: Segment organization WAN traffic from other traffic on the WAN to enable the confidentiality and integrity of data. This may be achieved through a dedicated point-to-point link, a corporate managed VPN, a client-originated VPN or a service provider-managed MPLS service. If data loss and data manipulation are possible threat on WAN traffic, data in-transit over the WAN may be encrypted.

Authenticate WAN Access: Access to the organization WAN should include strong authentication mechanism to prevent unauthorized access to the network and data.

Threat Detection and Mitigation: Intrusion prevention and network telemetry to identify and mitigate threats. IPS based global correlation, reputation-based filtering, botnet and malware blocking solutions.

Edge Protection: Traffic filtering, routing security, firewall integration, and IP spoofing protection to discard anomalous traffic flows, prevent unauthorized access and block illegitimate traffic.

Network Foundation Protection: Device hardening, control and management plane protection throughout the entire infrastructure to maximize availability and resiliency.

Secure Mobility: Always-on VPN protection for PC-based and smartphone mobile users.

Persistent and consistent policy enforcement independent of user location. Enforcement of Client Firewall Policies. Optimal gateway selection to ensure best connectivity. Integration with web security and malware threat defense systems deployed at the enterprise premises.

Enhanced Availability and Resiliency: Hardened devices and high-availability design to ensure optimal service availability. Design leverages redundant systems, stateful failover, and topological redundancy.

2. Protect Infrastructure Device Access

It is critical to secure the access to the network infrastructure devices like router, firewall, and switches to protect the network infrastructure. Uncontrolled or unmanaged access to the infrastructure devices can lead to serious network security compromise and operational glitches.

Restrict device accessibility: Limit the accessible ports and restrict the permitted communicators and the permitted methods of access.

Present legal notification: Display legal notice developed in conjunction with company legal counsel for interactive sessions.

Authenticate access: Ensure access is only granted to authenticated users/ groups and services.

Authorize actions: Restrict the actions and views permitted by any particular user, group, or service.

Ensure the confidentiality of data: Protect locally stored sensitive data from viewing and copying. Consider the vulnerability of data in transit over a communication channel to sniffing, session hijacking and man-in-the-middle (MITM) attacks.

Log and account for all access: Record who accessed the device, what occurred and when for auditing purposes.

Password Protection: Passwords should generally be maintained and controlled by a centralized Authentication, Authorization and Accounting (AAA) server.

3. Routing infrastructure Security

Routing is one of the most important parts of the infrastructure that keeps a network running, and as such, it is absolutely critical to take the necessary measures to secure it. There are different ways routing can be compromised, from the injection of illegitimate updates to DoS specially designed to disrupt routing. Attacks may target the router devices, the peering sessions, and/or the routing information.

Restrict routing protocol membership: Limit routing sessions to trusted peers, validates origin, and integrity of routing updates. Many dynamic routing protocol, particularly interior gateway protocols, implement automatic peer discovery mechanisms that facilitate the deployment and setup of routers. By default, these mechanisms operate under the assumption that all peers are to be trusted, making it possible to establish peering sessions from bogus routers and to inject false routing data. It is required to enable features designed to restrict routing sessions to trusted peers and that help validate the origin and integrity of routing updates.

Control route propagation: Enforce route filters to ensure only valid routing information is propagated. Control routing information exchange between routing peers and between redistributing processes. Route filtering is important tool to secure the routing infrastructure. Most routing protocols allow the configuration of route filters that prevent specific routes from being propagated throughout the network. In terms of security/ these filters are useful because they help ensure that only legitimate networks are advertised; and networks that are not supposed to be propagated are never advertised.

Log status changes: Log the status changes of adjacency or neighbour sessions. Frequent neighbour status changes (up or down) and resets are common symptoms of network connectivity and network stability problems that should be investigated. These symptoms may also indicate ongoing attacks against the routing infrastructure. Logging the status changes of neighbour sessions is a good practice that helps identify such problems and that facilitates troubleshooting. In most routing protocols, status change message logging is enabled by default. When enabled, every time a router

session goes down, up, or experiences a reset, the router generates a log message. If syslog is enabled, the message is forwarded to the syslog server; otherwise is kept in the router's internal buffer.

4. Network Device Resiliency and Survivability

Network devices in distribution sector may be subject to attacks designed to affect the network availability for critical functions of Discoms. Possible attacks include Distributed DoS, DoS, flood attacks, reconnaissance and unauthorized access. Following are the recommended best practices for preserving the resiliency and survivability of the network in distribution sector:

Disable unnecessary services and ports: Devices are having list of services turned on in default installation. Services and port not required by the environment must be disable to reduce the attack surface.

Implement Infrastructure protection Access Control List (ACLs): Infrastructure ACLs (iACLs) are designed to explicitly permit authorized control and management traffic bound to the infrastructure equipment such as routers and switches, while denying any other traffic directed to the infrastructure address space. ACLs shields the network infrastructure from internal and external attacks.

Port security consideration-Access based on MAC address: An attacker can mount attacks such as DoS attack against infrastructure devices by using MAC flooding to cause MAC address table exhaustion. This type of attack can be addressed with a feature called Port Security. Port Security helps mitigate attacks by restricting the MAC addresses that are allowed to send traffic on a particular port. Once Port Security is enabled on a port, only packets with a permitted source MAC address are allowed to pass through the port.

Redundancy to survive the failure or overloading of the device: Networks are built out of numerous hardware and software components that may fail or that may be subject to attacks. Implementing redundant designs helps eliminate single points-of-failure, improving the availability of the network and making it more resistant to attacks. Different ways of implementing redundancy varies from deploying simple backup interfaces up to building complete redundant topologies.

5. Monitoring, Analysis and Correlation

Monitoring of the network events, central correlation and analysis capabilities, troubleshooting and identifying security incidents and threats in the networks of Discoms is vital part of the network infrastructure security. It is critical to have visibility and awareness into what is occurring on the network at any given time. Collecting, trending and correlating logging, flow and event information help identify the presence of security threats, compromises and data leak. Network telemetry offers extensive and useful detection capabilities that can be coupled with dedicated analysis systems to collect,

trend, and correlate observed activity.

Monitoring, Analysis and correlation solution helps in:

- Identify the presence of security threats, compromises and data leak
- Confirm security compromises
- Reduce false positives
- Reduce volume of event information
- Determine the severity of an incident
- Reduce incident response times

6. Network Policy Enforcement

Network policy enforcement in Discoms is primarily concerned with ensuring that traffic entering the distribution network conforms to the network policy, including the IP address range and traffic types. Anomalous packets should be discarded as close to the edge of the network as possible, thereby minimizing the risk of exposure. Key steps to implementing baseline network policy enforcement are:

Access Edge Filtering: Network Security Baseline is focused on securing the network infrastructure itself, the control and management planes. Access edge filtering in this context is implemented to enforce policy on what traffic is permitted to be directed towards the network infrastructure devices themselves.

IP Spoofing Protection: Spoofing protection involves discarding traffic that has an invalid source address. Network security baseline includes source IP spoofing protection based on RFC 2827 ingress traffic filtering.

7. Switching Infrastructure Security

Networks uses switches to connect computers, printers and servers within a building or campus or area of operation of Discoms. A switch serves as a controller, enabling networked devices to talk to each other efficiently. Switching security in distribution sector is concerned with ensuring the availability of the Layer-2 switching network. Securing and preserving the switching infrastructure is key requirement for network infrastructure security.

Restrict broadcast domains: Segment broadcast domains into multiple IP subnets or VLANs using a hierarchical design instead of one large broadcast domain. The use of hierarchical design principles provides the foundation for implementing scalable and reliable LANs.

Port Security consideration: Configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port.This enables individual ports to detect, prevent and log attempts by unauthorized devices to communicate through the switch.

Implement VLAN best practices

- Always use a dedicated VLAN ID for all trunk ports
- Disable all unused ports and put them in an unused VLAN
- not use VLAN 1 for anything
- Explicitly Configure trunking on infrastructure ports
- Use all tagged mode for the native VLAN on trunks
- Set the default port status to disable

8 Threat Control and Containment

Detection and mitigation capabilities at network infrastructure are available on security appliances like firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS), Email and Web security appliances etc. Threat control and containment solution should be deployed to protect network infrastructure of the distribution companies. It is recommended to have following capabilities and features in selected threat control and containment solution in Discoms-

Complete visibility: Infrastructure-wide intelligence provides an accurate vision of network topologies, attack paths and extent of the damage.

Adaptive response to real-time threats: Source threats are dynamically identified and blocked in real-time.

Consistent policy enforcement coverage: Mitigation and containment actions may be enforced at different places in the network for defense-in-depth.

Minimize effects of attacks: Response actions may be immediately triggered as soon as an attack is detected, thereby minimizing damage.

Common policy and security management: Acommon policy and security management platform simplifies control and administration and reduces operational expense.

9. Endpoints Security

Network endpoints are defined as any systems that connect to the network and communicate with other entities over the network infrastructure such as servers, desktop computers, laptops, printers, handheld devices and IP phones. The vulnerability of any particular endpoint can impact the security and availability of an entire enterprise. Common threats to these endpoints include malware, adware, spyware, viruses, worms, botnets and E-Mail spam. Thus, endpoint security is a critical element of an integrated, defense-in-depth approach to protecting both clients and servers themselves and the network to which they connect. The first step in properly securing the endpoints requires end-user awareness and the adoption of the appropriate technical controls like antimalware software, Host based firewall, Host-based IPS/IDS, Patch and

update policy enforcement.

10. Secure Third-Party Connectivity

The ability of IT to communicate and collaborate with control center, data center, customers and employees anytime and anywhere is a requirement for Discoms. Network infrastructure must be protected from the threat due to third-part connectivity. Organization must ensure data confidentiality and integrity through a range of VPN options and PKI for strong, scalable authentication. Following are key points to consider for securing third-party connectivity.

Secure WAN/Internet Connectivity: Data confidentiality and integrity through a range of VPN options and PKI for strong, scalable authentication.

Granular Access Control: Extranet edge firewall and filtering rules should provide granular access control to necessary resources of the network to the third-party site.
Some of other best practices and control for cyber security are as under-

- Inventory of authorized and unauthorized hardware & software.
- Secure configurations of network devices, such as firewalls, routers and critical infrastructure.
- Maintenance and analysis of complete security audit logs.
- Secure coding practices for application
- Controlled use of administrative privileges and access management
- Dormant account monitoring and control.
- Anti-malware defenses.
- Limitation and control of ports, protocols and services.
- Wireless device control.
- Data-leakage protection.
- Secure network engineering.
- Assured data backups periodically.
- Security-skills assessment and training to fill gaps.
- Secure E-Governance - Encourage usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
- Develop a dynamic legal and regulatory framework to address social media challenges and statutory regulations and acts.

Appendix –V

Data Centre Guidelines

With the rapid advances taking place in technology such as cloud computing, social media, big data, context aware computing, etc; government, businesses and users are demanding secure, continuous, reliable operation in the data center which provide high availability and peak performance, 7 days a week, 365 days a year.

Data Centre for Energy Management has a defined data center as a special facility that performs one or more of the following functions:

- A data center physically houses various equipment, such as computers, servers (e.g., web servers, application servers, database servers), switches , routers, data storage devices, load balancers, wire cages or closets, vaults, racks and related equipment.

- Data centers store, manage, process and exchange digital data and information.

- Provide application services or management for various data processing, such as web hosting internet, intranet, telecommunication and information technology.

Further, a Data Recovery Centre also to be maintained at place away from the location of Data Centre, to store backup of data and information of data centre.

Other terms used to describe data centers include: Computer center, data centre, datacenter, data storage and hosting facility, data processing center, computer room, server room, server farm, data farm, data warehouse, co-location facility, co-located server hosting facility, corporate data center, managed data centers, internet service provider (ISP), application service provider (ASP), full service provider (FSP), wireless application service provider (WASP), telecommunications carriers, etc . The details of control room(s) shall be maintained by CGM as per format at Annexure-I.

While designing data center particular emphasis on the following factors should be kept in mind:

- Adequate facility space (present and future)
- Power (operational and backup)
- Cooling (general and rack-specific)
- Cabling pathways Equipment racks
- Cabling system (components and design)

The data centre structures also need to be protected from physical damage by considering the risks from Fire Risk, Water Risk, Smoke Risk, Power Supply Risk, Air-Conditioning Risk, Dust Risk, Unauthorized Access Risk, Explosion Risk, etc., to ensure availability:

Some of the other points that need to be considered for availability are:

- Security systems such as burglar alarms, access control, video surveillance, building security, security personnel, security lighting, central building controls systems, etc.
- Green IT and Energy efficiency
- Short response times for upgrades and extensions
- Low latencies to meet the growing requirements in terms of internet presence
- Restoration process for back up from Data Recovery centre and network connectivity etc.

Annexure – A :

DISTRIBITION CRISIS MANAGEMENT GROUP(DCMG)

1. **Computer Emergency Response Team For Distribution (CERT –D)**
   Chief Engineer, Distribution Planning and Development (DP&D) Division,
   Address : Central Electricity Authority, 6th floor, Sewa Bhawan, R.K Puram, New Delhi-66
   Contact no :Tele fax-011-2610 2793, Ph-011-2673 2661
   Email-cedpd-cea@gov.in,

2. CISO-MOP and for Coordination Information Sharing and Analysis Centre (ISAC)-Power also-
   Chief Engineer, Information Technology (IT) Division,
   Address : Central Electricity Authority, 3rd floor, Sewa Bhawan, R.K Puram, New Delhi-66
   Contact no :Tele fax-011-2610 2793, Ph-011-2673 2661
   Email-itcea@nic.in

3. Name of **CISO** :
   CHIEF ENGINEER / INFORMATION TECHNOLOGY,
   TAMIL NADU GENERATION AND DISTRIBUTION CORPORATION LIMITED,
   X FLOOR, NPKRR MAALIGAI,
   NO.144, ANNA SALAI,
   CHENNAI-600 002.

4. Name of Officers for **CMG**
   CHIEF ENGINEER / INFORMATION TECHNOLOGY,
   TAMIL NADU GENERATION AND DISTRIBUTION CORPORATION LIMITED,
   X FLOOR, NPKRR MAALIGAI,
   NO.144, ANNA SALAI,
   CHENNAI-600 002.

Annexure B : Key Vendor Contact Details

Vendor	Contact Person	Contact Number / Mobile	Off Business Hours Contact
<Software Solution Provide >	<Name & Designation>	Contact No. And email ID	Contact No. And email ID
<Hardware Solution Provider>	<Name & Designation>	Contact No. And email ID	Contact No. And email ID
<LAN Solution Provider >	<Name & Designation>	Contact No. And email ID	Contact No. And email ID
<WAN Solution Provider>	<Name & Designation>	Contact No. And email ID	Contact No. And email ID
Firewall and Antivirus	<Name & Designation>	Contact No. And email ID	Contact No. And email ID

Annexure C : IT Vendor Escalation Matrix

Vendor Name	Service Providing for	Escalation 1	Escalation 2	Escalation 3

Annexure D : Incident Management Process

Incident Response

Activity	Authority/ Responsibility
The personnel who detected the incident shall immediately bring it to the notice of the Crisis Management Group.(CMG)	Users & CMG
The CMG shall intimate the facts and impacts of incident to CISOusing the Incident Reporting Form (Refer to Annexure-E,F)	CMG
The CMG shall, in consultation with the concerned Head of Department, analyze the impact of the incident, then document and send it to the CISO using the Incident Management Form (Refer to Annexure-H)	CMG
The CMG Team shall maintain the log of all incidents. By using Incident tracker (Refer Annexure-G)	CMG
The CMG Team shall categorize all incidents based on the nature of each incident. The CMG may take assistance from domain experts to classify the incidents.	CMG
The CISO, in consultation with IT Team shall prepare the corrective action plan for the Incident and present it to Crisis Management Group (CMG) for approval.	CISO & CMG

Activity	Authority/ Responsibility
Level One Escalation Level One is the initial level for all incidents. The contact must be available 24x7x365 and therefore represents a role rather than an individual. The contacts at this level must have the ability to call to action engineers and to escalate to management as required, to resolve all categories and severity of incidents. All reports must be sent to the CISO every week.	User & CMG
Level Two Escalation Level Two represents senior management with authority to take actions that fall outside the standard operating policies of the concerned organizations. Escalation to Level Two is appropriate in cases where Level-One interactions have been unsuccessful in resolving an operational issue within the stipulated time schedule.	CMG

Annexure-E: Incident Reporting Form

Incident Reporting Form	
Incident Ref.#	Date : Time :
Location / Office :	Department
Name of the Employee	Email / Contact No.
Facts of the Incident	
Impact of the Incident	
Signature of Employee	

Annexure-F: Incident Response Form

Incident Response Form

From:

To:

Incident Ref # :				Incident Date:	
				Incident Time:	
No #	Location	Date of Reporting	Details	Risk and Impact Analysis	
Location / Office :			Date of Reporting from the Location / Office :		
Facts of the incident					
Discussed with IT Team					
Cause of the Incident					
Corrective Action Plan for incident management (with time schedule)					
#	Corrective Action	Responsibility	Start Date	Date of Completion	Cost Incurred
Preventive Action Plan:					
#	Actions Required	Test Results	List of Departments Informed		
Signature: IT Head / Designated Authority				Date :	

Annexure – G: Incident Tracker

Incident Tracker								
Issue No.	Incident Reporting Date	Problem Description	Problem Identification	Problem Resolution	Status	Issue Resolved Date	Challenges faced	Remarks

Annexure-H : Incide

Name of Reportee	
Date of Filing Incident	
Record Number	
Filed by CISO	

Type of Incident - Physical Incident (P) - Logical Incident (L)	
Scope of Incident - What did happen - Which asset(s) have been compromised? - What is the damage done ?	
Time of Incident - When was it detected ? - When was it reported ? - When action was taken ?	
Authorities (Name, Designation, Dept, Signature) - Reportee - Manager of Reportee, if applicable - CISO (acknowledgement and follow up)	
Analysis & Compliance - What was the root cause of the incident - What are the lessons learned ? - What are the actions taken ?	

Date Signature

CISO

Annexure I :

Control Room Details of Discoms / Power Departments

Primary Contact		
Name	Designation & Address	Contact Details
Alternate Contact		
Contact Details	<Name & Designation>	Contact No. and email ID

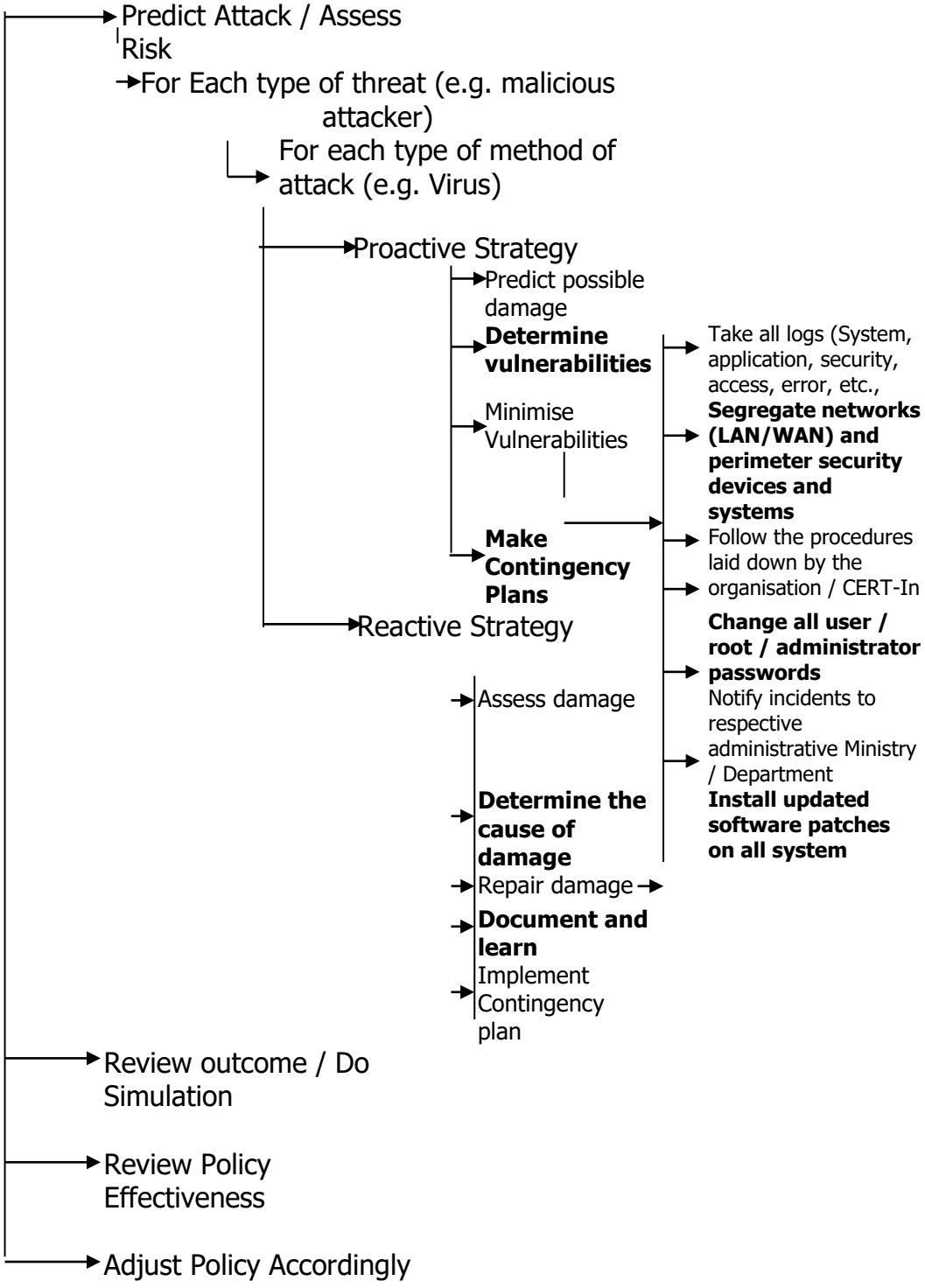
~~**References : Cyber Crisis Management Plan for Countering Attacks and Cyber Terrorism, Govt. of India, Ministry of Electronics and Information Technology, DEITY, CERT-In**~~

Annexure J

FLOW DIAGRAM FOR IDENTIFICATION OF THREATS AND ACTION REQUIRED BY UTILITIES

Security Strategy

A methodology for defining
Security policies and controls



GLOSSARY

AMI -	Automatic Meter Infrastructure
AMR -	Automatic Meter Reading
AP -	Access Point
BCP -	Business Continuity Plan
BIS -	Bureau of Indian Standard
BPCS-	Basic Process Control System
CA -	Certification Authority
CDA-	Critical Digital Asset
CII -	Critical information Infrastructure
CIP-	Critical Information Protection
CERT-	Computer Emergency Response Team
CERT In –	Indian Computer Emergency Response Team
CMP-	Crisis Management Plan
CSIRT -	Computer Security Incident Response Team
DAS –	Data Acquisition System
DC-	Data Center
DCS -	Distributed Control System
DDoS-	Distributed Denial of Service
DISCOM –	Distribution Company
DMS –	Distribution Management System
DMZ	Demilitarized zone
DNS	Domain Name System
DNSSec –	Domain Name System Security Extension
DoS -	Denial of Service
DRC-	Disaster Recovery Center
DRP -	Disaster Recovery Planning
EAP-	Electronic Access Point
e-mail -	Electronic Mail
EMS –	Energy Management System
FTP-	File Transfer Protocol
GIS -	Geographic Information System
HIPS-	Host Intrusion Prevention system
HMI-	Human Machine Interface
IEGC –	Indian Electricity Grid Code
ICS-	Industrial Control System
ICT –	Information and Communication Technology
IDS –	Intrusion Detection System
IPS –	Intrusion Prevention System
IPSec –	Internet Protocol Security
IP -	Internet Protocol
ISAC -	Information Sharing and Analysis Centre

ISD - International Security Department
ISMS- Information Security Management System
ISO - International Organisation for Standardization
ISP - Internet Service Provider
LAN - Local Area Network
LDC – Load Dispatch Centers
MSS – Management Security Service
NCIIPC - National Critical Information Infrastructure Protection Center
NAC- Network Access Control
NBA- Network Behavior Analysis
NCMC- National Crisis Management Committee
NIXI - National Internet Exchange of India
OEM- Original Equipment Manufacturer
OT- Operational Technology
PKI - Public Key Infrastructure
RF- Radio Frequency
RTO- Recovery Time Objective
RPO- Recovery Point Objective
SCADA - Supervisory Control and Data Acquisition
SIEM- Security Information and Event Management
SLA- Service Level agreement
SOD- Segregation of Duties
SOP - Standard Operating Procedures
SIEM - Security Information and Event Management
R-APDRP – Restructured Accelerated Power Development and Reform Program
SRS – Specific System Requirement
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
URL - Uniform Resource Locator
VAPT - Vulnerability Assessment and Penetration Testing
VOIP- Voice over Internet Protocol
VLAN- Virtual Local Area Network
VPN- Virtual Private Network
VTR- Vulnerability, Threat & risk
WAN - Wide Area Network
www- World Wide Web