



USAID
FROM THE AMERICAN PEOPLE

Regional Training Program on Cybersecurity

South Asia Regional Energy
Partnership (SAREP)

Regulations in Indian Power Sector
ANAND SHANKAR, POWERGRID



INDIA

India's electricity grid to be more future ready, insulated from cyber attacks soon: Union Power Minister

PTI

NEW DELHI: SEPTEMBER 01, 2022 18:01 IST
UPDATED: SEPTEMBER 01, 2022 18:01 IST

SHARE ARTICLE



Minister of State (Independent Charge), Power and New & Renewable Energy, K.K. Singh has in past admitted that there were cyber attacks on the national power grid. File | Photo Credit: Shiv Kumar Pushpalar

Electricity Amendment Bill, 2022 to make provisions for inspection of the national electricity grid for maintaining cyber hygiene in the network

India's power network will soon be more future-ready and insulated from cyber attacks with the provision of routine inspections and timely action under the

Govt releases guidelines for cybersecurity in power sector

The government on Thursday announced the release of guidelines for cybersecurity in the power sector for the first time, to create a secure cyber ecosystem

Topics
Power Sector | cybersecurity | Cyberattacks

Press Trust of India | New Delhi
Last Updated at October 7, 2021 21:04 IST

GOVERNMENT OF INDIA
MINISTRY OF POWER
LOK SABHA
UNSTARRED QUESTION NO.1916
ANSWERED ON 28.07.2022
ENERGY SUPPLY GRID

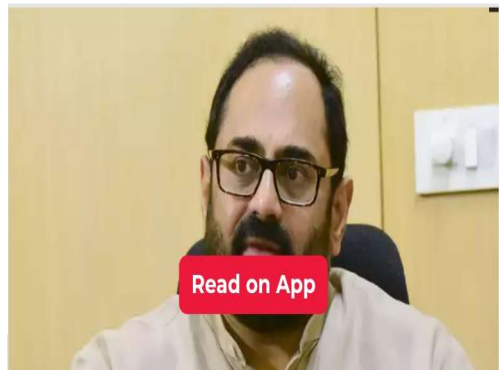
1916. DR. SUJAY RADHAKRISHNA VIKHEPATIL:
DR. HEENA GAVIT:
PROF. RITA BAHUGUNA JOSHI:
DR. SHRIKANT EKNATH SHINDE:
DR. KRISHNA PAL SINGH YADAV:

Will the Minister of POWER
be pleased to state:

- (a) whether the Government has conducted any study to identify the vulnerabilities of the energy supply grid in the country during the last three years and the current year;
- (b) if so, the details thereof and if not, the reasons therefor, State/UT-wise;
- (c) whether the Government has carried out any investigation in this regard along with the measures taken/being taken to ensure the safety of the powergrids from cyber-attacks in future; and



Follow rules or leave India: MoS Rajeev Chandrasekhar to VPN service providers



Recent Challenges

- Spurt in Cyber Incidents in Power Sector
 - Impacting several Load Despatch Centres, Generating Stations and Substations of other utilities.
- Directions of MoP for several compliances with long term impact
 - Board Level Reviews / Sensitisation Programs
 - Mandatory Audits, Equipment Testing, ISO 27001 Certification
 - CEA Regulations, Model Contractual Clauses, Trusted Vendors
 - Capacity Building, Replacement for Legacy Systems
 - Cyber Crisis Management Plans, Critical Information Infrastructure (CII) Identification, Grid Operations cyber sensitive
 - Reviews by MoP

ELECTRICITY GOVERNANCE ECOSYSTEM in INDIA

Updated as on 25-Jan-2021

Electricity Act 2003



Adopted on 2nd June 2003 and consolidates :

1. The Indian Electricity Act, 1910,
2. The Electricity (Supply) Act, 1948.
3. The Electricity Regulatory Commission Act, 1998.



Mandate preparation of following guiding documents :

1. National Electricity Policy & Tariff policy - (Section-3) - By Gol.
2. National Electricity Plan once in five year - (sec-3) - By CEA.
3. National policy of rural electrification - (sec 4&5).
4. Grid standards & technical standards - (sec-73) - By CEA
5. Grid code (Sec-79)-by CERC and state grid code (sec-86) -by SERC

Prepared by - P.K. Agarwal

Act, Policy & Rules



Central Government (Ministry of Power & MNRE)

1. Administration of the Electricity Act, 2003
2. Administration of Energy Conservation Act, 2001.
3. To undertake such amendments to these Acts.
4. Responsible for development of electrical energy in the country.
5. Make rules for carrying out the provisions of EA 2003 on behalf of Gol - Section 176.



Central Electricity Authority CEA - (Sec-70) Part - IX

1. Make consistent regulations - Sec-177
2. Advising the MoP on technical issues.
3. Data management/dissemination.
4. Preparation of technical standards.
5. Preparation of National Electricity Plan.



State Government (State Energy department)

1. Act as per of the Electricity Act, 2003
2. Administration of Energy Conservation in the state.
3. To undertake such actions as deemed fit in accordance with rules and policies.
4. Responsible for development of electrical energy in the state.
5. To make rules for carrying out the provisions of the Act. - Section 180

**Special Courts
Part - XV**
Notified by state Government for speedy trials of cases - Section



Appellate Tribunal For Electricity Section -110 Part - XI

To hear appeals against the orders of the adjudicating officer or the Commission.

Regulations



Central Commission - Section-76 Central Electricity Regulatory Commission -

1. To regulate and determine tariff of central generating company and inter state transmission system.
2. Issue license to inter state transmission licensee and electricity traders for inter-state operations.
3. Adjudicate upon disputes involving generating companies and transmission licensee.
4. To make consistent regulations - section 178.
5. Nomination of arbitrator - Section 158

Forum of Regulators

Consisting of the Chairperson of the Central Commission and Chairpersons of the State Commissions.
The Chairperson of the Central Commission is designated as Chairperson



State Commission - Section-82 Joint Commission - Section-83

1. To determine tariff generation, supply, transmission and wheeling of electricity, wholesale, bulk or retail within state.
2. Regulate electricity purchase and procurement process of distribution licensees.
3. Facilitate intra-State transmission and wheeling of electricity
4. To make consistent regulations. - Section 181

Implementation

Regional Power Committees - by central Government - Section 2 (55)

Facilitating the integrated operation of the power systems in that region



National Load Despatch Center (NLDC) - Section - 26 Power System Operation Corporation Ltd. (POSOCO)

Apex body for grid operation. Monitors & Schedules Interregional & Trans-National electricity exchange.



Regional Load Despatch Center (RLDC) - Section-27

1. Manged by central government company : POSOCO Ltd.
2. Optimum scheduling and despatch of electricity within region.
3. Monitors grid operation within region.
4. Keep accounts of electricity transmitted on regional grid.
5. Operates as per grid standard and grid code.

Central Advisory Committee : Constituted as per section 80

Central Transmission Utility Section - 38 Power Grid Corporation of India Ltd.

1. To discharge all functions related to planning and co-ordination relating to inter-State transmission system.
2. To ensure development of an efficient, co-ordinated and

State Transmission Utility Designated by State. Section - 39

1. To discharge all functions related to planning and co-ordination relating to intra-State transmission system.
2. To ensure development of an efficient, co-ordinated and economical system of intra-State transmission lines



State Load Despatch Center (SLDC) - Section-31

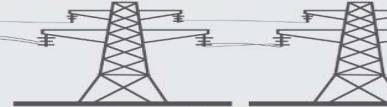
1. Manged by state government or it's company.
2. Optimum scheduling and despatch of electricity within state.
3. Monitors grid operation within state.
4. Keep accounts of electricity transmitted on state grid.
5. Operates as per grid standard and state grid code.

State Advisory Committee : Constituted as per section 87

Supply



Generation
Electricity Act-2003 Part III



Transmission (Licensed)
Electricity Act-2003 Part V



Distribution (Licensed)
Electricity Act-2003 Part VI



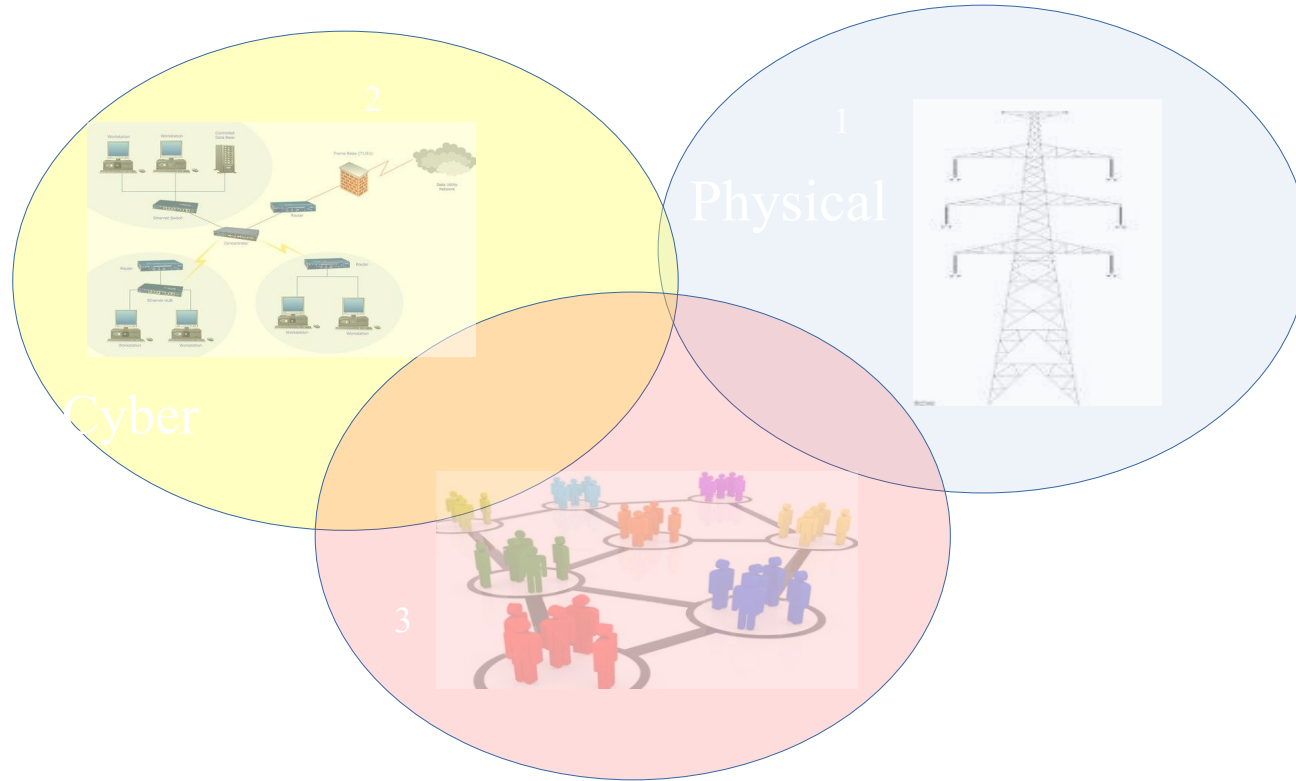
Consumption

← **Electricity Market** - Power Exchange, Electricity Traders (Licensed) - Part-IV →

Prepared by - P.K. Agarwal

Critical Information Infrastructure

Smart Ecosystem: Cyber-Physical-Social System



CI in Critical Infrastructure [CI] Sectors

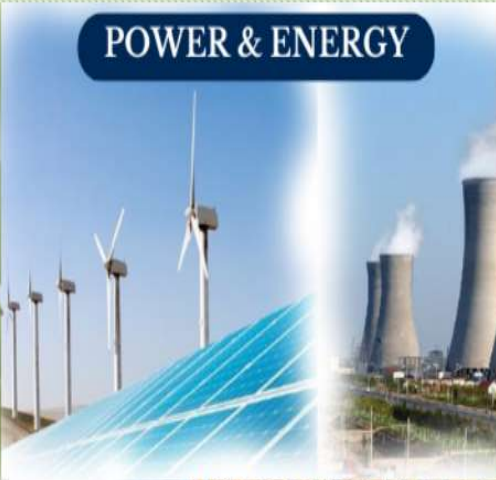
GOVERNMENT



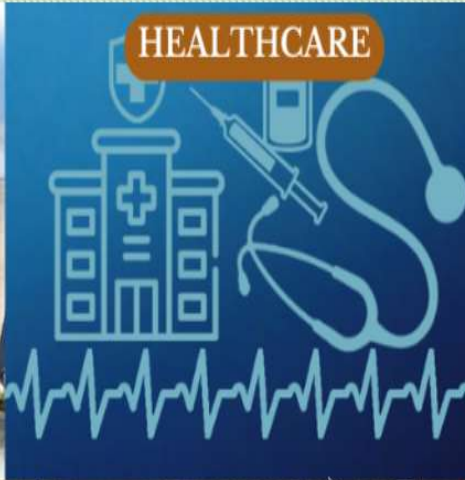
BANKING, FINANCIAL SERVICES & INSURANCE



POWER & ENERGY



HEALTHCARE



TRANSPORT



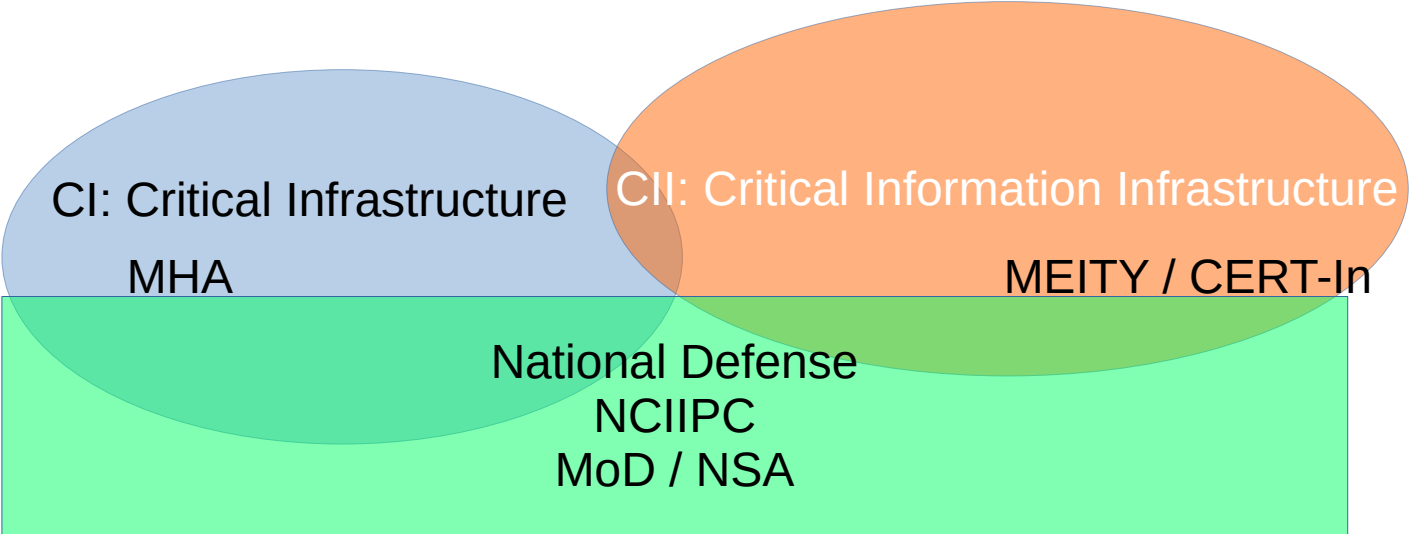
TELECOM

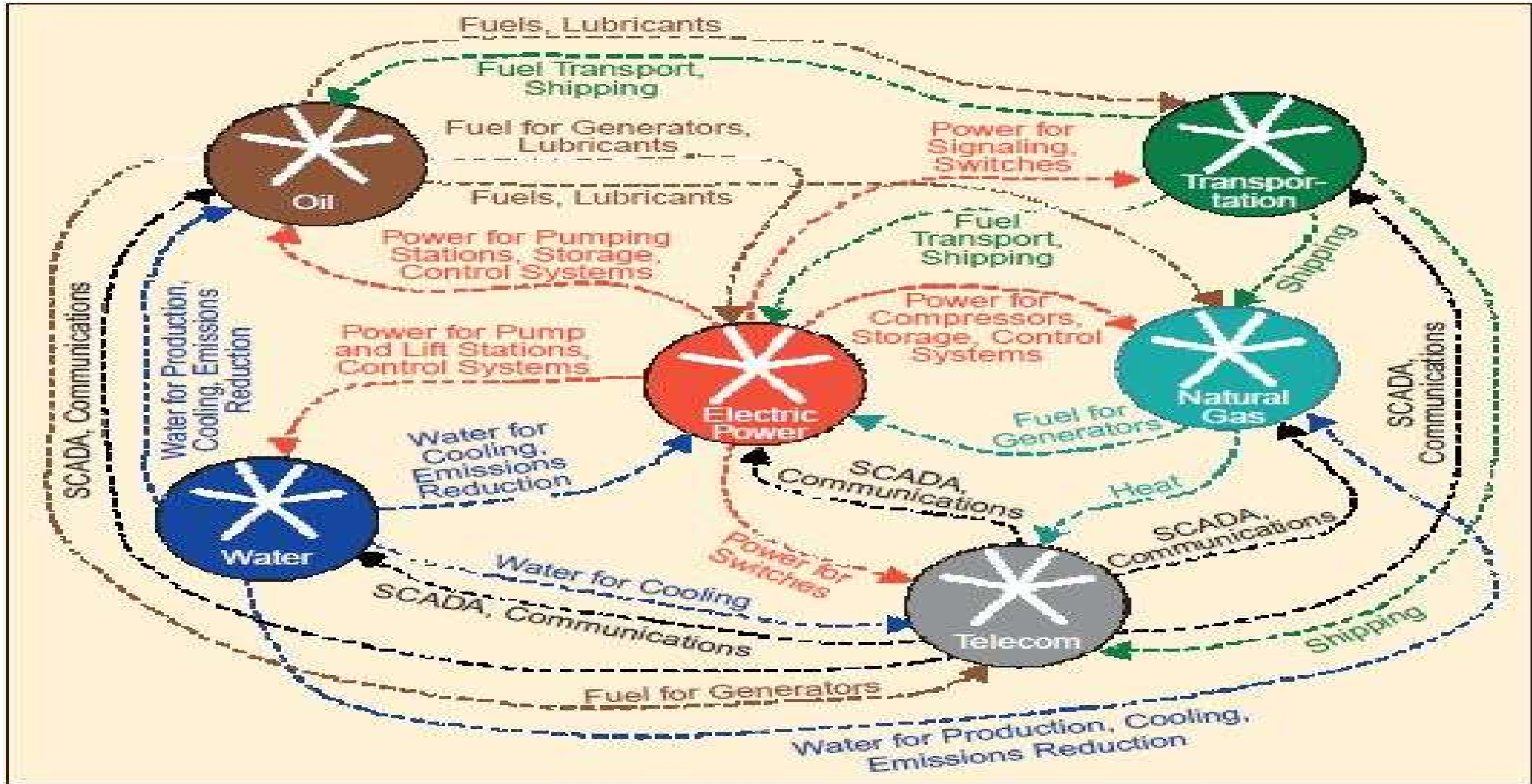


STRATEGIC AND PUBLIC ENTERPRISES



Critical Infrastructure & Critical Information Infrastructure





Rinaldi et al.: "Critical Infrastructure Interdependencies (Identifying, Understanding, and Analysing)." IEEE Control Systems Magazine 21 (2001): 12-25.

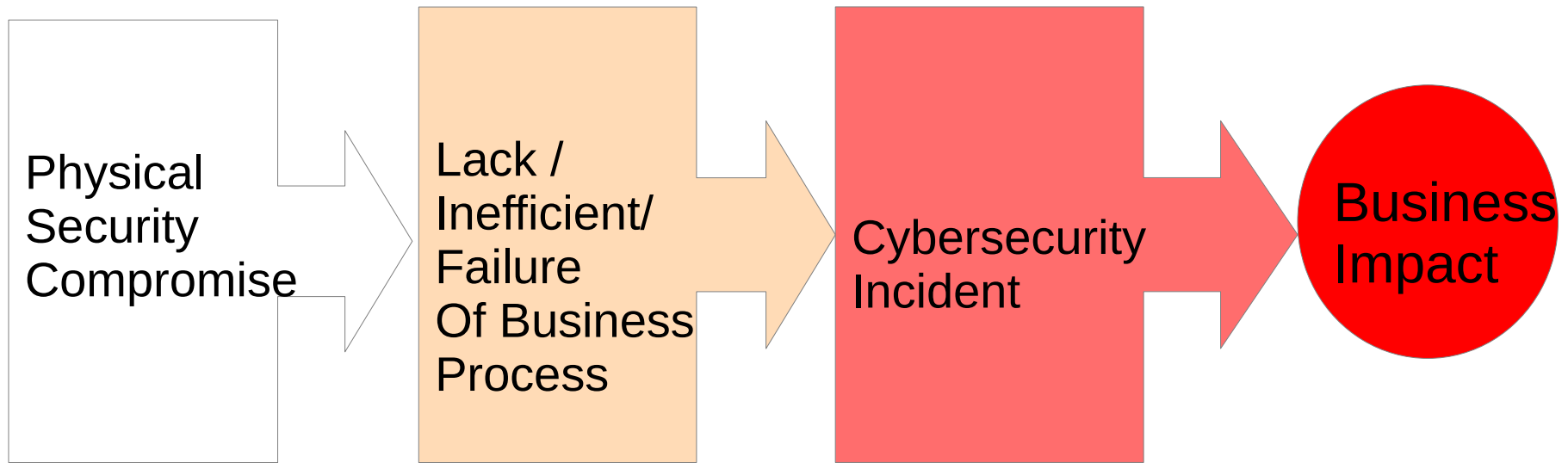
Key Drivers for Information (Cyber) Security

- **Information Technology Act 2000 (Amendment 2008)**
- Business critically dependent on underlying IT infrastructure
 - Critical Information Infrastructure
 - Debilitating Impact on **National Security**, **Economy**, **Public Health** and **Safety**.
- National Critical Information Infrastructure Protection Centre [NCIIPC] : Clause 70A
- Computer Emergency Response Team India : CERT-in : Clause 70B
- **Offences by Companies : Clause 85(1) : Due Diligence Requirement**
- **Due Diligence Rules under IT Act: Gazette Notification 11/04/2011**
 - **Implementation of Information Security Management System (ISO 27001)**

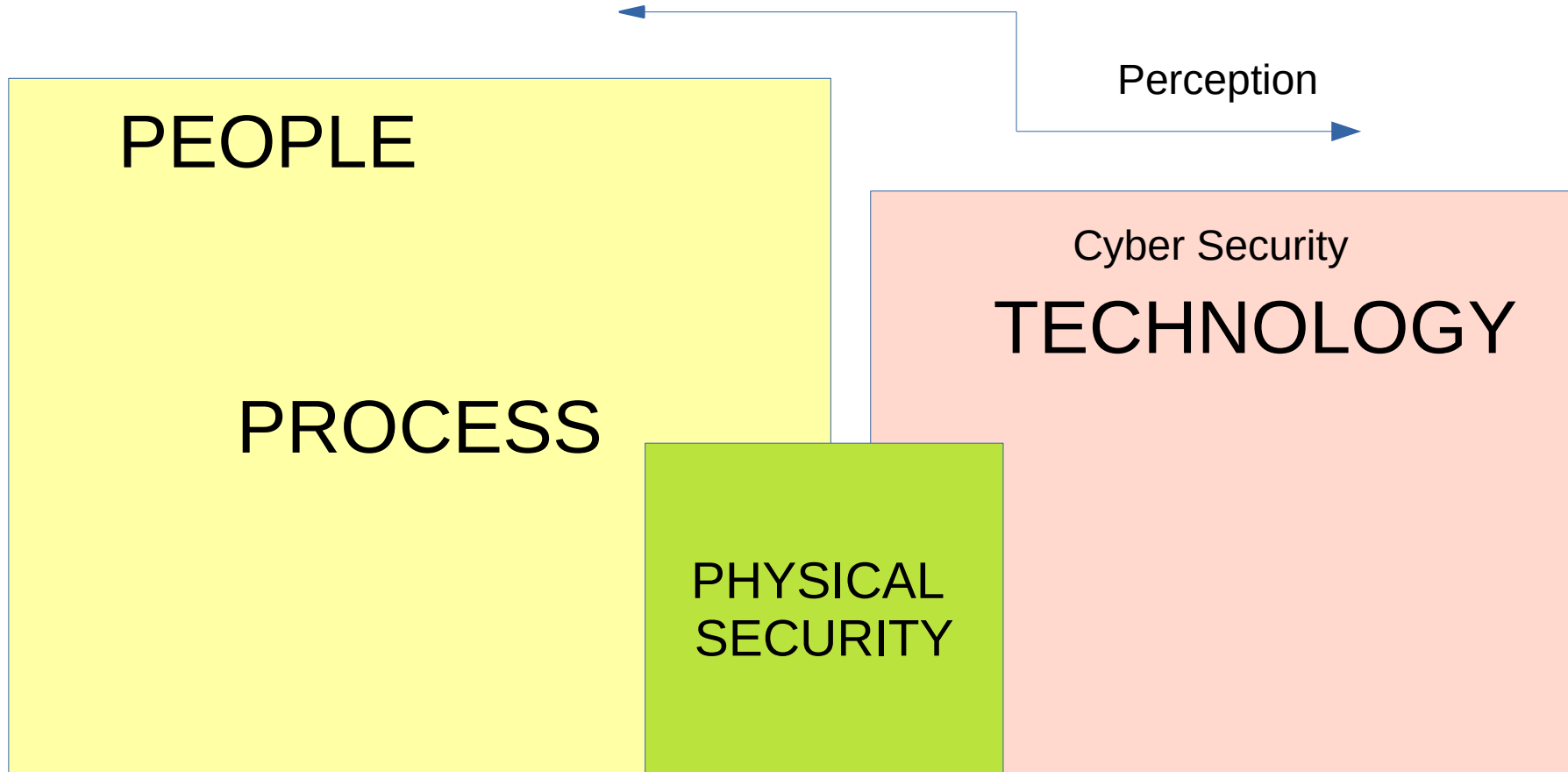
Key Drivers for Information (Cyber) Security

- Enterprise Risk Management: Companies Act 2013: Sec 134
- National Information Security Protection Guidelines, 2014
- **CERC Communication System Regulation, 2017**
- **Listing Obligations and Disclosure Requirements [LODR], 2018**
- **CEA Guidelines on Cybersecurity, 2021**
- **CERC Indian Electricity Grid Code, 2023: Chapter 9**
- **National Cybersecurity Reference Framework, 2023 (To be notified)**
- **Digital Privacy and Data Protection Act, 2023**
- **CSMS of Critical Sector Entity (Level 2 - Supplementary Technical Criteria – Power Sector)**

Cybersecurity Incident is Last in a chain of compromises



Standards and Systems driven Information Security Management System



Relevant Standards for Cybersecurity

- ISO 27000 Family of Standards :
 - ISO27001 Certification Standard
- IEC 62443 Family of Standards
 - Cybersecurity in Industrial Control Systems
- ISO 15408 : Common Criteria Testing
- IEC/ISO 20243 : Malicious and Tainted Components

Sectoral CERTs

Ministry of Power

CISO-MoP

CSIRT-POWER at CEA

Sectoral CERTs

CERT-Thermal

NTPC

CERT-Hydro

NHPC

CERT-Trans

POWERGRID

CERT-Distribution

CEA Distribution
Planning

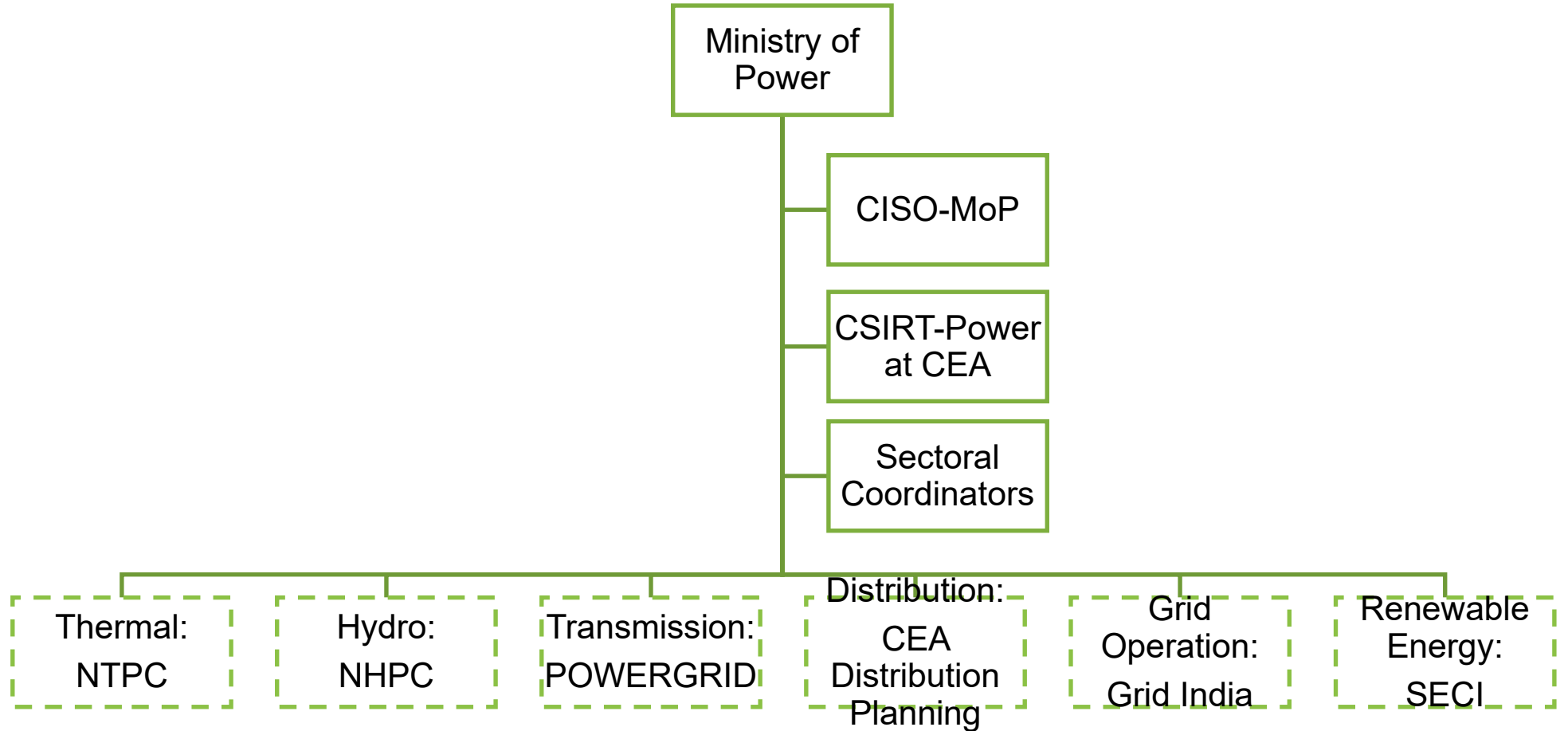
CERT-GO

Grid
India

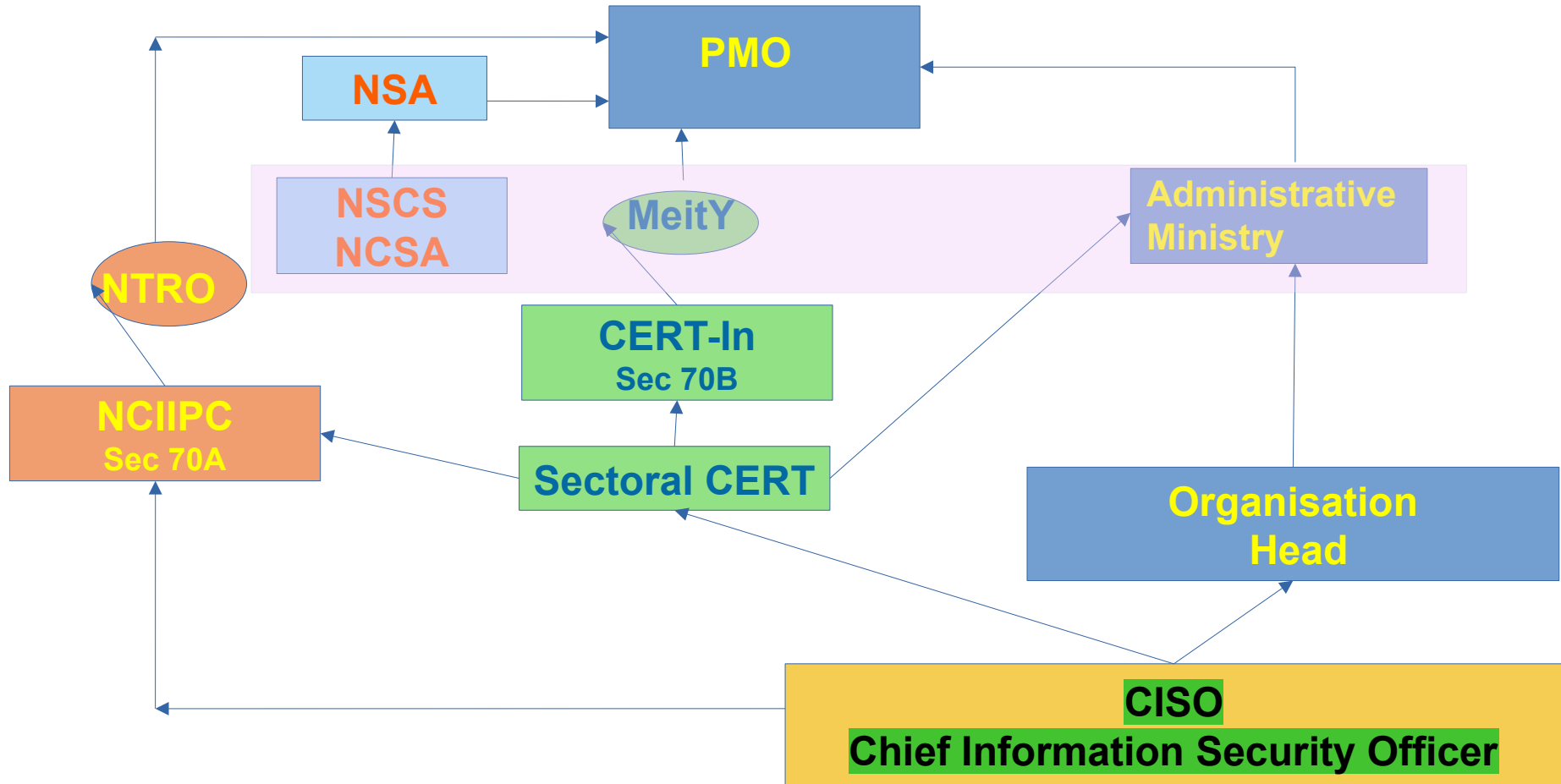
CERT-
RE

SECI

Sectoral CERTs




Cyber Security Monitoring & Reporting Framework



Sectoral Initiatives

- CISO and Alternate CISO Nomination
- Capacity Building : Training and Certification of people.
- Cyber Crisis Management Plan (CCMP)
- Critical Information Infrastructure (CII) Identification
- Monitoring of Internet Connected Traffic
- Cyber Security Policy Implementation - ISMS (ISO 27001) Implementation
- Cyber Security Audit / VAPT
- Mock Drills organised by CERT-In
- Cybersecurity as Board Agenda

Best Practices

- Enterprise Cyber Risk and Resilience Management
 - Organisational Governance
 - Regulatory and Legal Frameworks
 - Standards and Best Practice Guidelines
 - Communities of Practice
- 


Regulatory Challenges

- Driven by IT paradigms and practices
- OT insights and requirements need to be built in policy
- OT/IT identification and separation is blurry in many contexts
- Focus on Risk Assessment missing
- Binding requirements for OEMs/ SIs for compliance
 - Compliance to Inter-Operability Standards and Testing to reduce proprietary bindings.
 - Software and Hardware BoM
 - Service and Support
- Supply Chain compliance requirements need to span across Industry verticals.
- Identification of suitable tariff provisions

Security Process Requirements

- Cyber Security:
 - Nomination of CISO
 - Training & Awareness
 - Formation of Information Security Department
 - Implementation of Information Security Management System [ISO:27001]
 - Vulnerability Assessment and Penetration Testing
 - Incident Management and Response: CERT-In & NCIIPC Requirements
 - Compliance to CERT-In & NCIIPC Advisories: Patch Management
 - Identification of Information Assets, Risk Assessment & Mitigation
 - NCIIPC : Designate Protected CII Status

Organisational Challenges

- Information Security Department separate from Functional IT Departments
 - Skill Gap : In House vs Out Sourcing vs Trust
 - Functional gap between IT and Operations
 - Instrumentation to deploy patches
 - System to detect latest threat symptoms
 - Management Review Process
 - Upgrade of Legacy Infrastructure
 - Security as a Culture
- 

Critical Information Infrastructure

The Information Infrastructure of the Organisation, which when compromised debilitating impact on National Security, National Economy, Public safety and Public health is termed as Critical Information Infrastructure.

All Transmission utilities are required to identify their Critical Information Infrastructure in co-ordination with NCIIPC as per clause 70(1) of IT Act.

Process:

- Listing of all processes as per NCIIPC format
- Listing of Critical Processes which will be assessed by NCIIPC if it affects National Security, National Economy, Public Health and Public Safety.
- Organisation to submit inputs as per NCIIPC formats.
- Discuss with NCIIPC and conclude findings
- Getting approval from NCIIPC
- Declaration of CII by Ministry/ Administrative Department.
- Gazette notification from Administrative Ministry/Department to notify it as protected system.

Cyber Crisis Management Plan

- Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY) have developed Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism.
- This plan takes into consideration the crisis that occur due to cyber security incidents and breaches, and presents a broad based approach to deal with such crisis. CCMP is not only to respond cyber crisis/incidence but guide in building cyber resiliency at organisation & sector-level.
- The plan is updated periodically by CERT-In to take into account dynamic nature of Cyber Security threat landscape and emerging technologies.
- Each organization has to develop it's CCMP inline with model template published by CERT-In.

Requirements of Cyber Crisis Management Plan

This plan establishes strategic framework for dealing with Cyber incidents.

It describes types of cyber incidents, actions and responsibilities for a coordinated approach in order to prepare for rapid identification, information exchange, response, and remediation to mitigate & recover from malicious cyber related incidents impacting critical business functions and processes.

Key components of CCMP:

- Scope of plan
- Roles of CISO and employees
- Identification and priority of critical assets
- Mapping of critical roles to critical assets
- Incident response procedures
- Escalation matrix
- Mock drill scenarios
- Business Impact Analysis
- Contingency plan

CSK alerts/ CERT-In guidelines on Cyber security incident, analysis, reporting and closure.

- CERT-In guidelines:
 - Reporting of Cyber Incidents within **6hrs** is mandatory.
 - System clocks to be synchronised with standard time published by NPL / NIC
 - Logs to be maintained for 180 days on rolling basis
 - Designated Point of Contact.
- Penalty under Section 70B(7) of IT Act, 2000.
- CSK alerts:
 - Required updating and blocking to be done as per **advisories** issued by CERT-In/ NCIIPC/ MHA, etc.
 - Internal incident response mechanisms to be in place to identify and isolate impacted assets, if any.

CEA (Cyber security in Power sector) Guidelines, 2021

-
- The guidelines are divided into 14 articles which are:

Cyber Security Policy	Cyber Security Training
Appointment of CISO	Cyber Supply Chain Risk Management
Identification of Critical Information Infrastructure	Cyber Security Incident Report and Response Plan
Electronic Security Perimeter	Cyber Crisis Management Plan(C-CMP)
Cyber Security Requirements	Sabotage Reporting
Cyber Risk Assessment and Mitigation Plan	Security and Testing of Cyber Assets
Phasing out of Legacy System	Cyber Security Audit

CEA Guidelines on Cybersecurity, 2021

- Cyber Security Audit of IT and OT system by the CERT-In empanelled auditors. IT once in every six months and OT once every year.
- Critical Information Infrastructure (CIIs) to be identified in co-ordination with NCIIPC.
- Cyber Crisis Management Plan (CCMP) to be prepared and vetted by CERT-In
- Implementation of ISMS/ISO 27001.
- Cyber security mock drills to be conducted regularly
- Cyber Security training from the Training Institutes designated by CEA for all IT/OT personnel
- The guidelines present a window to the responsible entities for necessary preparations for compliance and feedback.

ISO 27019: Information Security Controls for Energy Utility Industry

Mandated as per CEA guidelines on
Cybersecurity



ISO27019 Controls

A.6 Organization of information security: A.6.1 Internal organization

1	Identification of risks related to external parties
---	---

2	Addressing security when dealing with customers
---	---

A.11 Physical and environmental security: A.11.1 Secure areas

3	Securing Control Centers
---	--------------------------

4	Securing equipment rooms
---	--------------------------

5	Securing peripheral sites
---	---------------------------

11.3 Security in premises of external parties

6	Securing in premises of other energy utilities organization
---	---

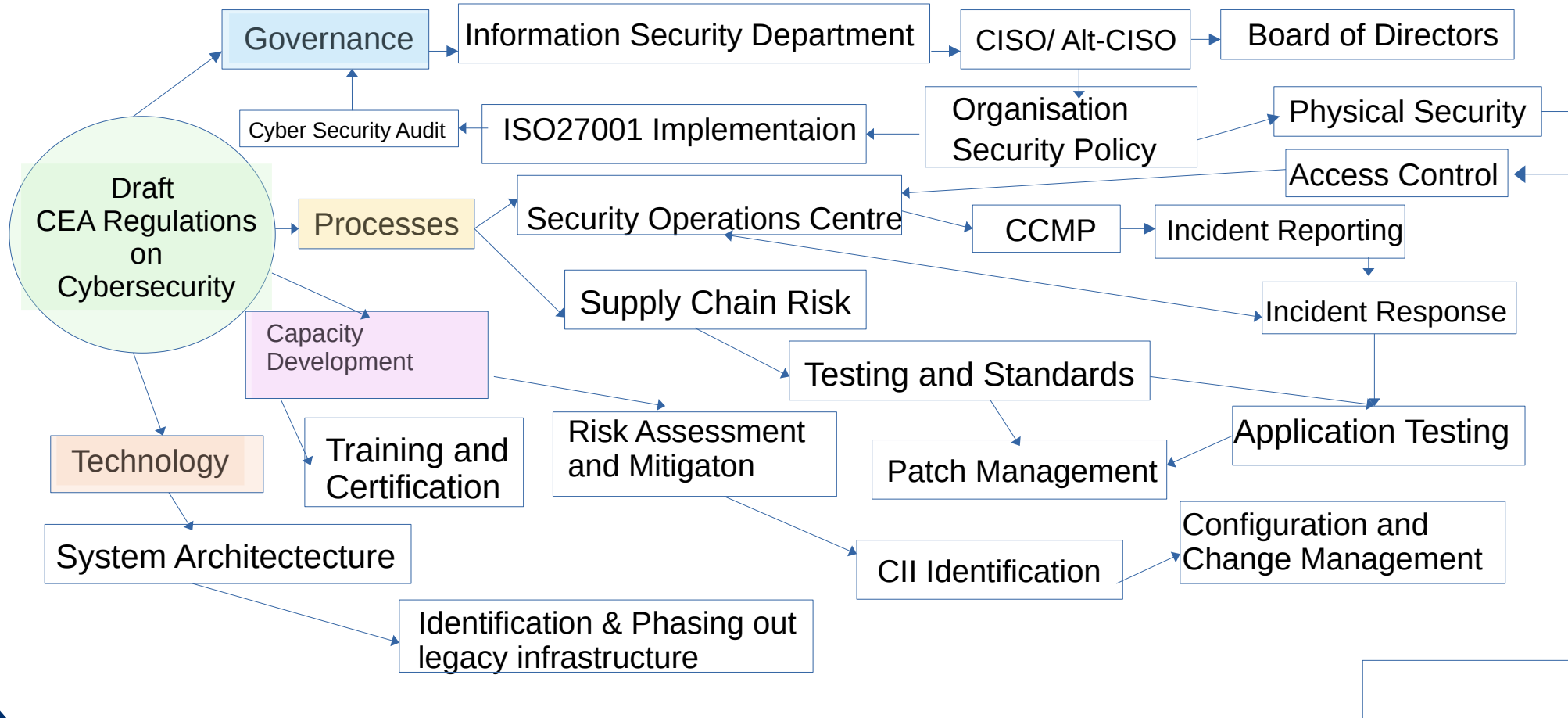
7	Equipment sited on customer's premises
---	--

8	Interconnected control and communication systems
---	--

ISO27019 Controls.. continued

A.12 Operations security: 12.8 ENR – Legacy systems	
9	Treatment of Legacy system
12.9 ENR – Safety functions	
10	Integrity of availability of safety functions
A.13 Communications security: A.13.1 Network security management	
11	Securing Process control data communication
12	Logical connection of external process control system
A.14 System acquisition, development and maintenance: A.14.2 Security in development and support processes	
13	Least Functionality
A.17 Information security aspects of business continuity management: A.17.2 Redundancies	
14	Emergency communications

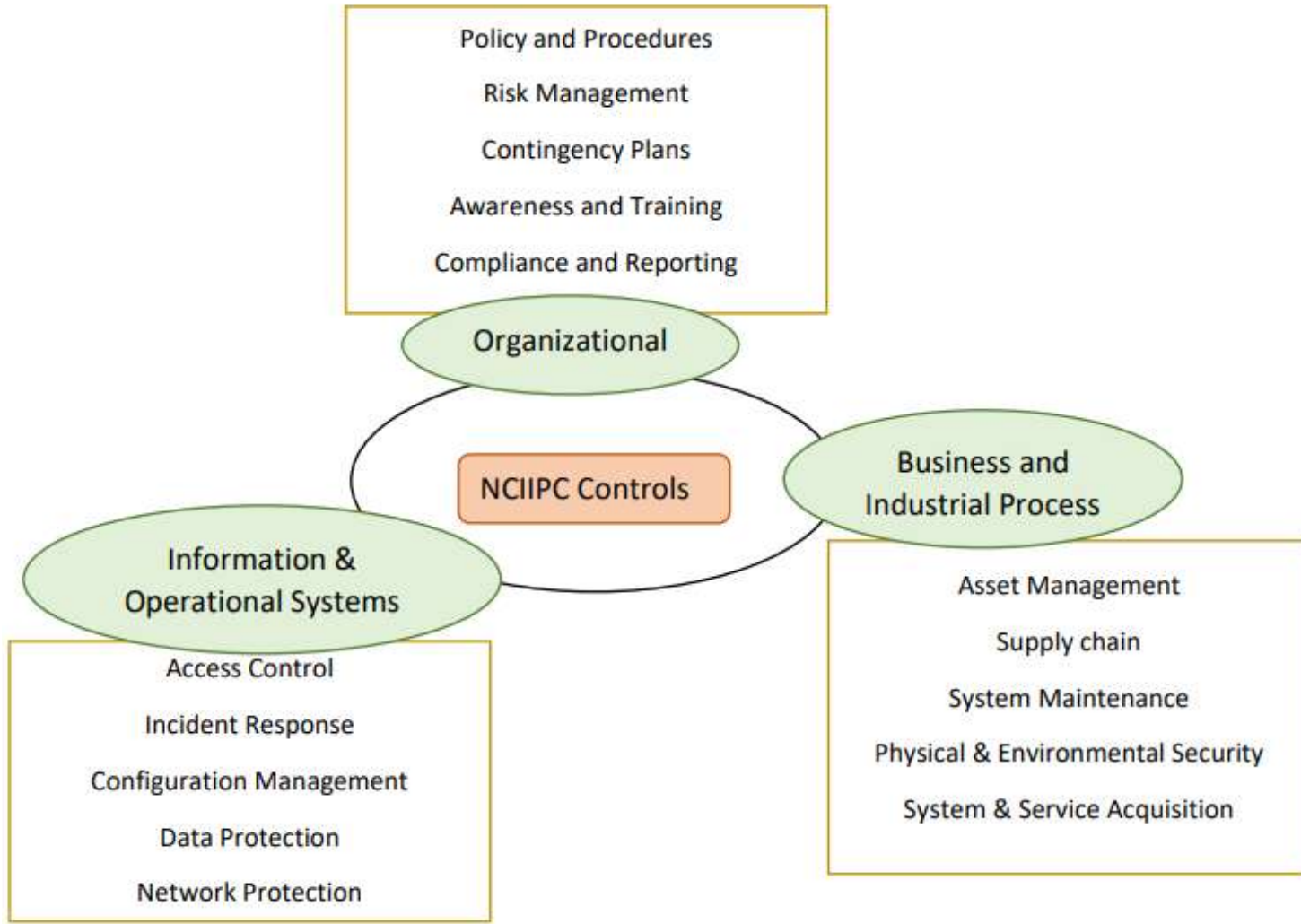
Draft CEA Regulations on Cybersecurity



NCIIPC Requirements

NCIIPC initiatives for CII

- Compliance to requirements of Protected Infrastructure as specified through Gazette Notification of 2018.
- National Cybersecurity Reference Framework (NCRF)
- Three Level hierarchy of controls to be implemented by CII.
 - L1 : Maps to ISO27001:2022
 - L2 : Domain specific controls for CII
 - L3 : Additional Technical Criteria
- Mapping of Job Roles with required Skills and accredited certification of skills



Information Security Practices and Procedures for “Protected Systems”

Clause 3 (1) & (2) :
Information Security Steering Committee

Information Security Practices and Procedures for “Protected Systems”

Clause 3 (3) The organisation having “Protected System” shall:

(a) nominate an officer as Chief Information Security Officer (CISO) with roles and responsibilities as per latest “Guidelines for Protection of Critical Information Infrastructure” and “Roles and Responsibilities of Chief Information Security Officers (CISOs) of Critical Sectors in India” released by NCIIPC;

- Most Power Sector utilities have a CISO as also required by CEA Guidelines.
- The roles and responsibilities are specified by NCIIPC and CERT-In.

(b) plan, establish, implement, operate, monitor, review, maintain and continually improve Information Security Management System (ISMS) of the “Protected System” as per latest “Guidelines for Protection of Critical Information Infrastructure” released by the National Critical Information Infrastructure Protection Centre or an industry accepted standard duly approved by the said National Critical Information Infrastructure Protection Centre;

- Most utility organisations are moving forward to achieve ISO27001 certification.

(c) ensure that the network architecture of “Protected System” shall be documented. Further, the organisation shall ensure that the “Protected System” is stable, resilient and scalable as per latest National Critical Information Infrastructure Protection Centre “Guidelines for Protection of Critical Information Infrastructure”. Any changes to network architecture shall be documented;

- Network Architecture is reviewed by NCIIPC as part of Risk Assessment of the identified CII.

(d) plan, develop, maintain the documentation of authorised personnel having access to “Protected System” and the same shall be reviewed at least once a year, or whenever required, or according to the Information Security Management System(ISMS) as suggested in clause(b);

- Standard part of Gazette Notification for protected systems

(e) plan, develop, maintain and review the documents of inventory of hardware and software related to “Protected System”;

- Software and Hardware Asset Inventory is to be maintained for CII entity

(f) ensure that Vulnerability/Threat/Risk (V/T/R) Analysis for the cyber security architecture of “Protected System” shall be carried out at least once a year. Further, Vulnerability/Threat/Risk (V/T/R) Analysis shall be initiated whenever there is significant change or upgrade in the system, under intimation to Information Security Steering Committee;

- VA-PT report compliance to be undertaken. Status is also required on annual basis for OT Assets as per CEA Guidelines.

(g) plan, establish, implement, operate, monitor, review, and continually improve Cyber Crisis Management Plan (CCMP) in close coordination with National Critical Information Infrastructure Protection Centre;

- Update for CCMP of the organisation to be reviewed as a process periodically.

(h) ensure conduct of internal and external Information Security audits periodically according to Information Security Management System(ISMS) as suggested in clause (b). The Standard Operating Procedure (SOP) released by National Critical Information Infrastructure Protection Centre (NCIIPC) for “Auditing of CII/Protected Systems by Private/Government Organisation” shall be strictly followed;

- The SOP is to be adhered to for CII entities

(i) plan, develop, maintain and review documented process for IT Security Service Level Agreements (SLAs). The same shall be strictly followed while designing the Service Level Agreements with service providers;

- SLAs are to be integral part of Service Contract for IT Security related assets.

(j) establish a Cyber Security Operation Center (C-SOC) using tools and technologies to implement preventive, detective and corrective controls to secure against advanced and emerging cyber threats. In addition, Cyber Security Operation Center is to be utilised for identifying unauthorized access to “Protected System”, and unusual and malicious activities on the “Protected System”, by analyzing the logs on regular basis. The records of unauthorised access, unusual and malicious activity, if any, shall be documented;

- SOC to be setup by CII entity and managed by organisations' ISD.

(k) establish a Network Operation Center (NOC) using tools and techniques to manage control and monitor the network(s) of “Protected System” for ensuring continuous network availability and performance;

- Organisation divisions to be equipped with a NOC

(I) plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, communication devices, servers, systems and services supporting “Protected System” and the logs shall be handled as per the Information Security Management System(ISMS) as suggested in clause (b).

- Necessary logs are to be kept for 180 days as CERT-In April 2022 Guidelines.

Information Security Practices and Procedures for “Protected Systems”

Clause 4:

Roles and Responsibilities of “Protected Systems”
towards NCIIPC

(1)	CISO shall maintain regular contact with NCIIPC
(2)	CISO shall share the details of following data of “Protected System”, whenever there is a change and incorporate inputs/ feedbacks suggested by NCIIPC
	CII and its dependencies/ ISSC/ ISMS / Network Architecture/ Authorised Personnel/ Inventory of HW and SW/ VTR Analysis/ CCMP/ Audit Reports and their Post-Audit compliances/ SLAs
(3)	Sharing of necessary Logs of SOC to help detect anomalies and generate Threat Intelligence on real time basis/ reports indicating unusual activities
(4)	Timely intimation of cyber incidents following SOP prescribed by NCIIPC

Privacy related Issues and Regulatory Developments

- Privacy Law in India is governed by Digital Personal Data Protection Act, 2023 (DPDP Act)
 - Resulted out of 9-Judge Constitutional Bench of Supreme Court ruling that privacy is a Fundamental Constitutional Right.
 - Roots of the case emerge from the Aadhar scheme of the Government.
- Digital Privacy being misused in cyber crime is a common experience.
- DPDP Act provide rights to the end user (Data Principal) for which organisations (Data Fiduciary) need to undertake technical measures for compliance requirements under the DPDP Act.
 - Data Protection Board of India
 - Data Protection Officer (DPO)

Privacy related Data Protection Requirements

- Organisations policy for identifying sensitive and personal data. Data Classification and implementation across all digital platforms and projects need to be ensured.
- Data Life Cycle Management practices need to be implemented.
 - Web applications requiring storage and processing of Data Principal's data, consent of Data Principal is necessary.
 - If a Data Principal requires that its data stored in the organisation be deleted, then it needs to be done along with its evidence.
 - Compliance along with evidence needs to be provided by Data Protection Officer.
 - Directives of Data Protection Board needs to be complied by Data Fiduciary
- Additional requirements for the data fiduciary if the data principal is covered under other jurisdictions of DGPR for eg, the compliance needs to be done.
- Requirements of Data Protection for Personal Data and Non-Personal Data
- Awareness/ Sensitisation and Training / certification is a strong and urgent requirement.



Thank You