CYBER SECURITY IN POWER SYSTEM

"There are only two types of companies: Those that have been hacked and those that will be hacked." Robert S. Mueller, III, Director FBI made this famous quote but almost by the time he made the quote it was out of date - it should be "There are only two types of companies: Those that have been hacked and those that don't know they have been hacked."

Cyber Security

- Cyber security refers to the protection of the networks, hardware, and software from attacks, damage, or unauthorized access and rejection of services.
- It basic involves:
- Identify Infrastructure
- Assess/Evaluate Vulnerabilities/Threats/Risks
- Implement Security Controls
- Verify Implementation of Security Controls
- Ensure Compliance to Audit

Cyber Security Initiatives in India

- 17.10.2000: Information Technology Act,2000 (No. 21 of 2000) - IT Act ,notified.This was amended in 2008. It is the primary law in India dealing with Cyber Crime and electronic commerce.
- 10.01.2014:National Critical Information Infrastructure Protection centre (NCIIPC) was created by Government of India under section 70 A of IT Act.
- Two important documents of NCIIPC:

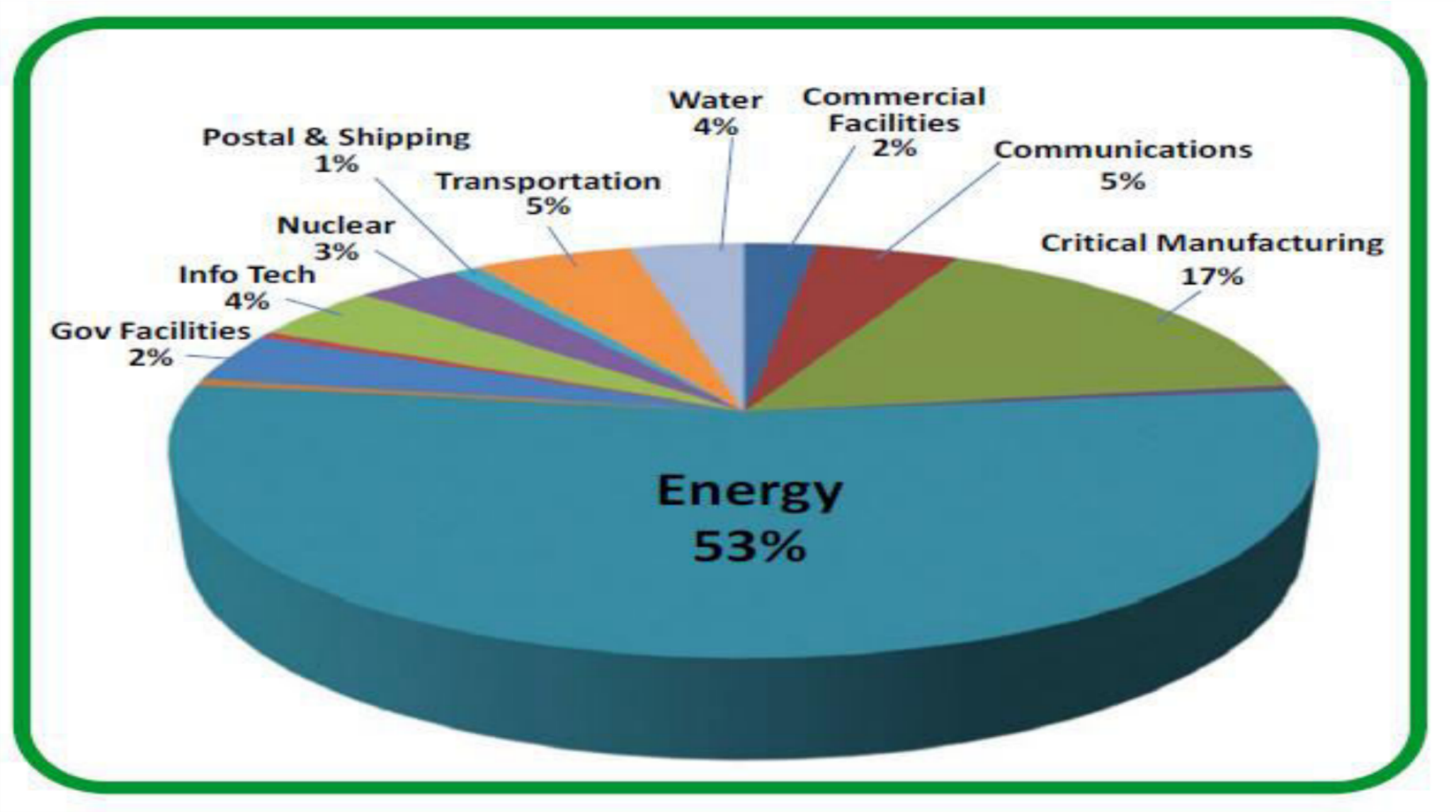
1. Guidelines for protection of critical Infrastructure (CII)
2. Framework for evaluation of Cyber Security

- Computer Emergency response Teams (CERT-In) under section 70(B) and sector specific CERTs constituted
- As per Rule 12(1) (a) of IT Rules 2013, it is mandatory to report specific cyber security incidents to CERT-In.
- ISGF Documentation: ISGF has prepared a framework for laying down procedures for securing India’s Smart Grid from cyber-attacks.
- ISO: 27001: The Government of India, under the Information Technology Act, 2000 and the Rules therein for Reasonable Security Practices published in 2011, require all organisations to implement ISO:27001 as the recommended Information Security Management System for legal compliance.

CYBER SECURITY IN POWER SECTOR

- INDIAN ELECTRICITY GRID CODE CLAUSE 4.6.5 – ALL UTILITIES SHALL HAVE DYDER SEDURITY FRAWEWORK TO IDEYTIFY THE DRITIDAL DYDER ASSET AYD PROTEDT THEW SO AS TO SUPPORT RELIADLE OPERATIOY OF THE GRID.
- IS-16335 :2015 POWER CONTROL SYSTEMS-SECURITY REQUIREMENT IT SPECIFIES REQUIREMENT FOR IDENTIFICATION AND PROTECTION OF CRITICAL ASSETS FOR ALL ENTITIES INVOLVED IN GENERATION, TRANSMISSION , DISTRIBUTION AND TRADING OF ELECTRIC POWER .
- CERC (COMMUNICATION SYSTEM FOR INTER-STATE TRANSMISSION OF ELECTRICITY) REGULATIONS, 2016.
- CEA SHALL FORMULATE AND NOTIFY TECHNICAL STANDARDS, CYBER SECURITY REQUIREMENTS, PROTOCOL FOR THE COMMUNICATION SYSTEM FOR POWER SECTOR WITHIN THE COUNTRY INCLUDING THE GRID INTEGRATION WITH THE GRID OF THE NEIGHBOURING DOUYTRIES.
- 13. CYBER SECURITY: (I) COMMUNICATION INFRASTRUCTURE SHALL BE PLANNED, DESIGNED AND EXECUTED TO ADDRESS THE NETWORK SECURITY NEEDS AS PER STANDARD SPECIFIED BY CEA.

Utility as target of Cyber attack



AREAS VULNERABLE TO CYBER ATTACKS

- **HARDWARE LAYER:** EMBEDDED COMPONENTS SUCH AS PROGRAMMABLE LOGIC CONTROLLERS (PLCS) AND REMOTE TERMINAL UNITS (RTUS) ARE HARDWARE MODULES EXECUTING SOFTWARE REQUIRED FOR INFORMATION COMMUNICATION AND CONTROL.

- **FIRMWARE LAYER:** THE FIRMWARE RESIDES BETWEEN THE HARDWARE AND SOFTWARE. IT INCLUDES DATA AND INSTRUCTIONS ABLE TO CONTROL THE HARDWARE.

- **SOFTWARE LAYER:** POWER CONTROL SYSTEMS EMPLOY A VARIETY OF SOFTWARE PLATFORMS AND APPLICATIONS, AND VULNERABILITIES IN THE SOFTWARE BASE MAY RANGE FROM SIMPLE CODING ERRORS TO POOR IMPLEMENTATION OF ACCESS CONTROL MECHANISMS.

- **NETWORK LAYER**: VULNERABILITIES CAN BE INTRODUCED INTO THE POWER CONTROL SYSTEM NETWORK IN DIFFERENT WAYS NAMELY THE FIREWALLS, MODEMS, FIELDBUS NETWORK, COMMUNICATIONS SYSTEMS AND ROUTERS, REMOTE ACCESS POINTS AND PROTOCOLS AND CONTROL NETWORK.

- **PROCESS LAYER:** ALL THE AFOREMENTIONED POWER CONTROL SYSTEM LAYERS INTERACT TO IMPLEMENT THE TARGET POWER CONTROL SYSTEM PROCESSES.

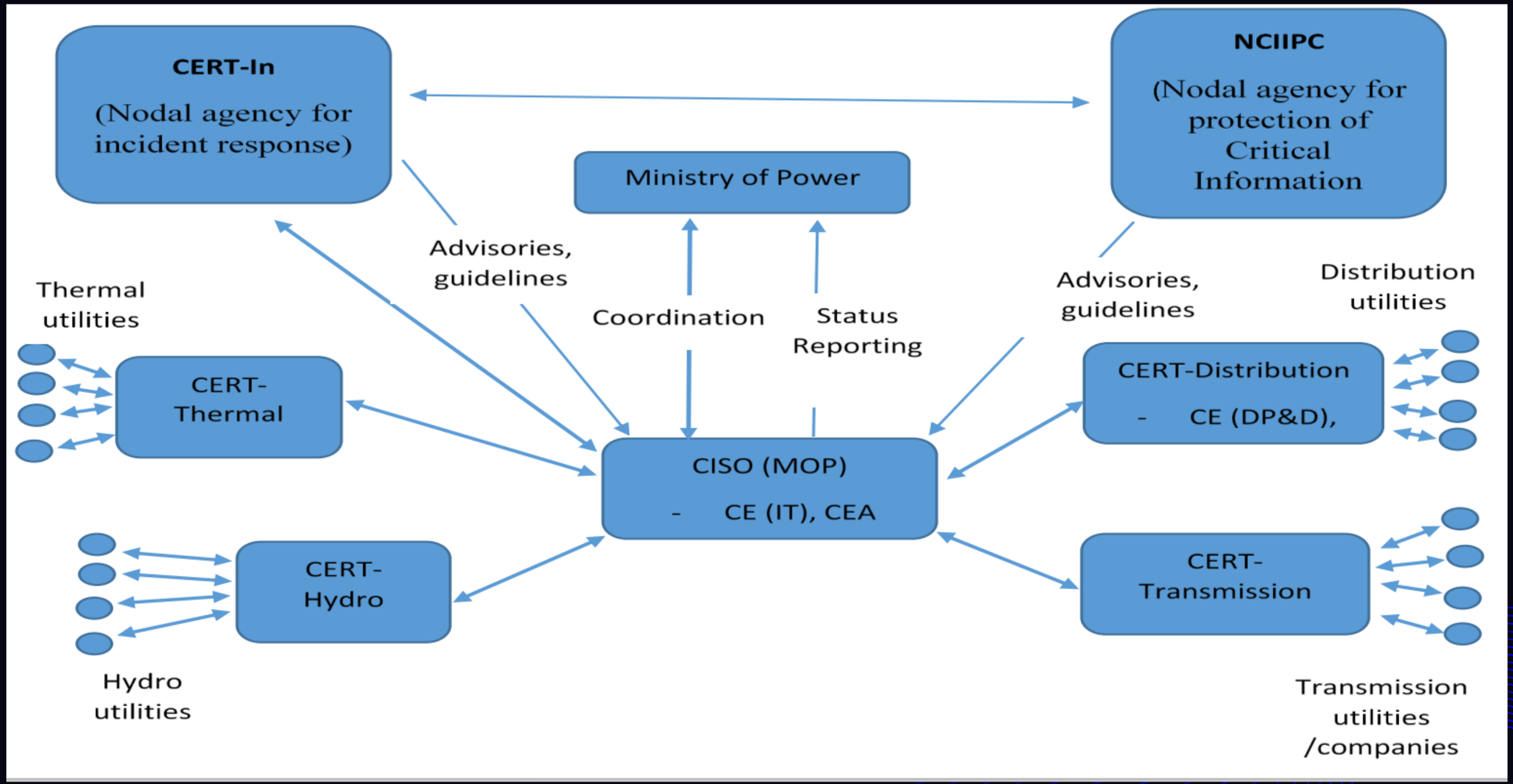
Issues in Cyber security

- To frame a cyber-security program to facilitate development of Cyber Security Standards
- create a platform for sharing cyber security incidents
- strengthening of the cyber security system in power generation, transmission, and distribution sectors.
- There are six areas, which need to be addressed for cyber security:

1. Vulnerability assessment in order to categorize the devices in terms of high risk and general vulnerabilities.
2. Vulnerability assessment area, extended to attacks from an insider, attack on the computer monitoring and controlling devices, attack on the SCADA network, and programming of malware into the control system devices.
3. Prepare framework for testing of equipment.
4. Asset mapping of all critical infrastructure equipment and periodic monitoring of these equipment for cyber security compliance.
5. Provide a complete monitoring solution to report on malicious connections.
6. Auditing and conformance procedure.

- Formulate provisions in regards to bidding to incorporate provisions for acceptance of technical standards and testing certificate of other countries

ORGANIZATION STRUCTURE FOR CYBER SECURITY IN POWER SYSTEM



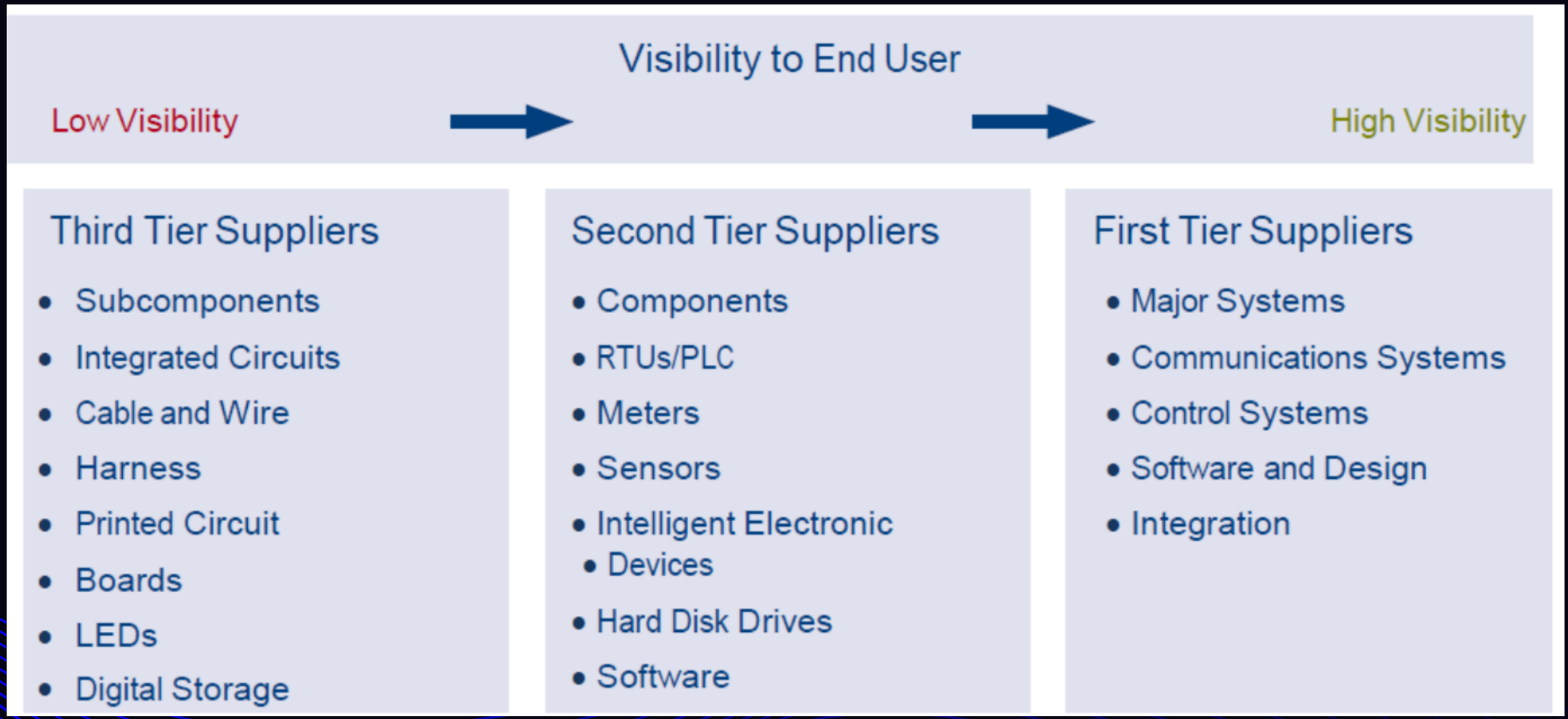
Cyber Security in Power system

- Vulnerability :
  - Generation : UMPP and Renewable generating stations(like Solar Inverter)
  - Transmission : Protection system and communication
  - System Operation : SCADA-EMS
  - Distribution : Smart meters

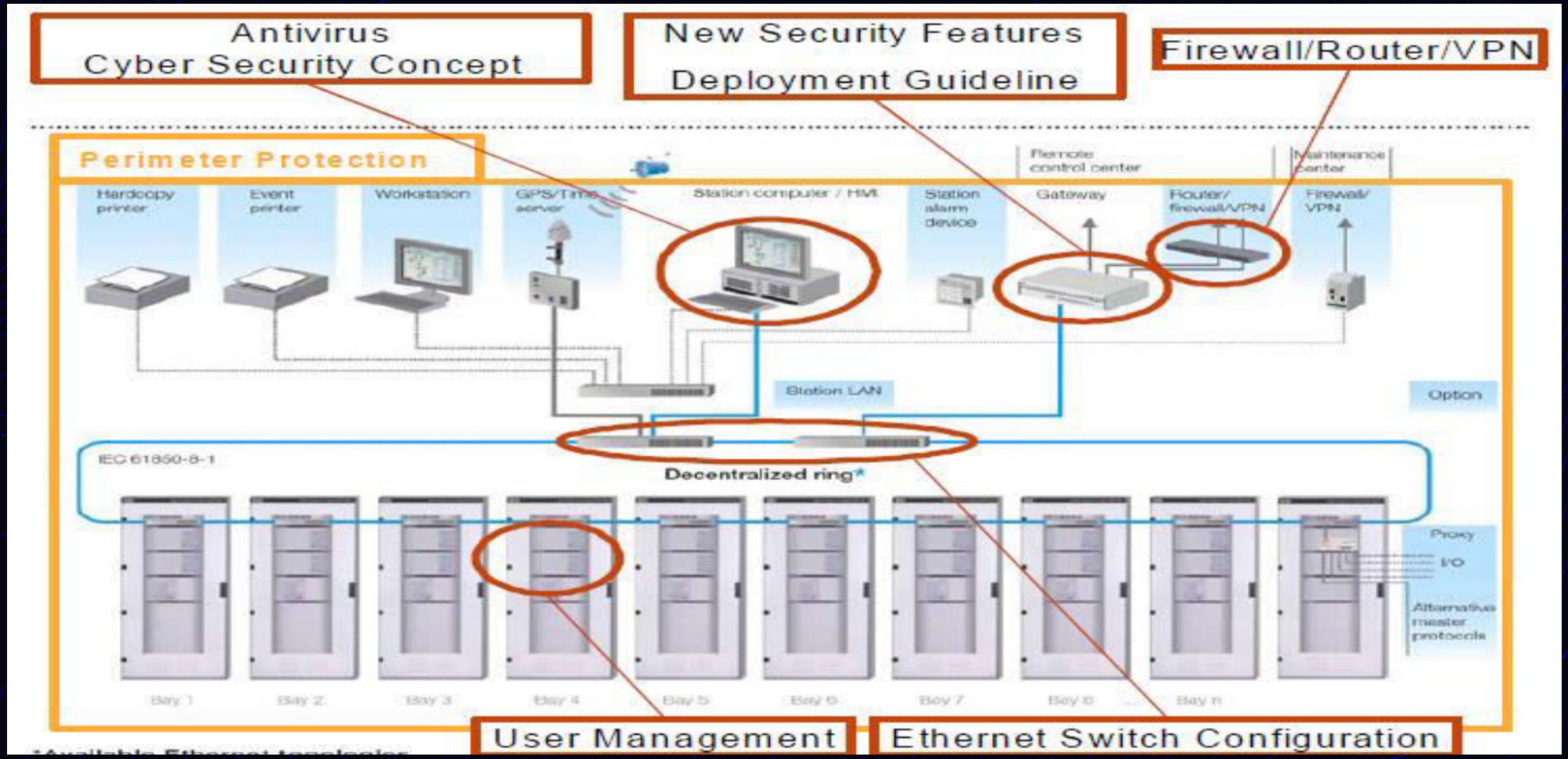
February ,2013 CEA brought out report on Guidelines mandating clearance from Security Angle wherever sensitive equipment is procured from overseas as well as for the procurement of electronic products by Government or its agencies for Power sector

- It lists out Critical equipment in Power sector considering physical and cyber security aspects.
- Also list out Electronic products deployed in Power system having security implication.

Supply chain of a utility



Sub station Protection



Action points on Cyber Security

- Review of CEA Regulations to incorporate suitable provisions for compliance of Cyber Security .
- Testing standards and procedure for cyber security compliance .
- Creation of test bed at CPRI .
- Guidelines for procurement to incorporate provisions for more local content and cyber security compliance.
- Scheme of testing and cyber security audit of all SCADA/EMS .
- CEA is coordinating cyber security in power sector. Further action to enhance cyber security awareness, preparation of crisis management plan and Cyber security audit in state utility specifically in distribution utilities is required, for this CEA will interact vigorously with State and formulate action plan so activities like appointment of CISO, identification of critical assets and crisis management plan is completed in a time bound manner.
- Formation of a umbrella organisation on cyber security issues in power sector Power Security Council of India
- Training and certification program on Cyber Security to be formulated

Cyber Security Preparedness

- Since last two years through CERT (Thermal, Hydro , Transmission and Distributions) efforts are made to sensitize and prepare all utilities for cyber security in power system

- Not much progress and lot need to be done .

- Organisation structure and documents are necessary but not sufficient as cyber security threat is too pervasive and it strike weak points too suddenly and more dangerous than a natural disaster .

THANK YOU