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 Robert S. Mueller, III, Director FBI made this famous quote but almost by the time he made the quote it was out of date – it should be 'There are only two types of companies: Those that have been hacked and those that don't know they have been hacked.'

Vijay MENGHANI

CHIEF ENGINEER (IT),

CENTRAL ELECTRICITY AUTHORITY

CISO, Ministry OF POWER

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 cyber security framework to identify the critical cyber asset and protect them so as to support reliable operation 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 countries".

  - 13. Cyber Security:

    (i) Communication infrastructure shall be planned, designed and executed to address the   network security needs as per standard specified by CEA.

Recent Cyber Attacks

- Cyber-attack in the form of ransomware virus hitting more than 150 countries on 12.05.2017.

- Black out in three cities of USA: A series of power outages in Los Angeles, San Francisco, and New York City left commuters stranded on 21.04.2017, yet to be recognized, whether due to cyber-attack.

- Cyber Attack on Ukraine's power grid on 17.12.2016.

- Cyber Attack on Hydropower Generation in New York in year 2013.

- Cyber Attack on Korea Hydro and Nuclear Co Limited in December, 2014.

- Security breach in Iran's Nuclear plant in 2010.

2017 : Cyber attacks

- **2017**
- February: The Cloudbleed bug was discovered by Google Project Zero team.
- April: A hacker group calling itself "The Dark Overlord" posted unreleased episodes of *Orange Is the New Black* TV series online after they failed to extort online entertainment company Netflix.
- May: WannaCry ransomware attack started on Friday, 12 May 2017, and has been described as unprecedented in scale, infecting more than 230,000 computers in over 150 countries.
- May: 25,000 digital photos and ID scans relating to patients of the Grozio Chirurgija cosmetic surgery clinic in Lithuania were obtained and published without consent by an unknown group demanding ransoms. Thousands of clients from more than 60 countries were affected.[87] The breach turned attention to weaknesses in Lithuania's information security.
- June: 2017 Petya cyberattack.
- May–July 2017: The Equifax breach.
- September 2017: Deloitte breach.
- **Indian Power Sector: Nov 2017 : Hydro Utility in Northern Region**
  - **Feb,2018 : Discom website , ransom call in Bitcoin**

Utility as target of Cyber attack
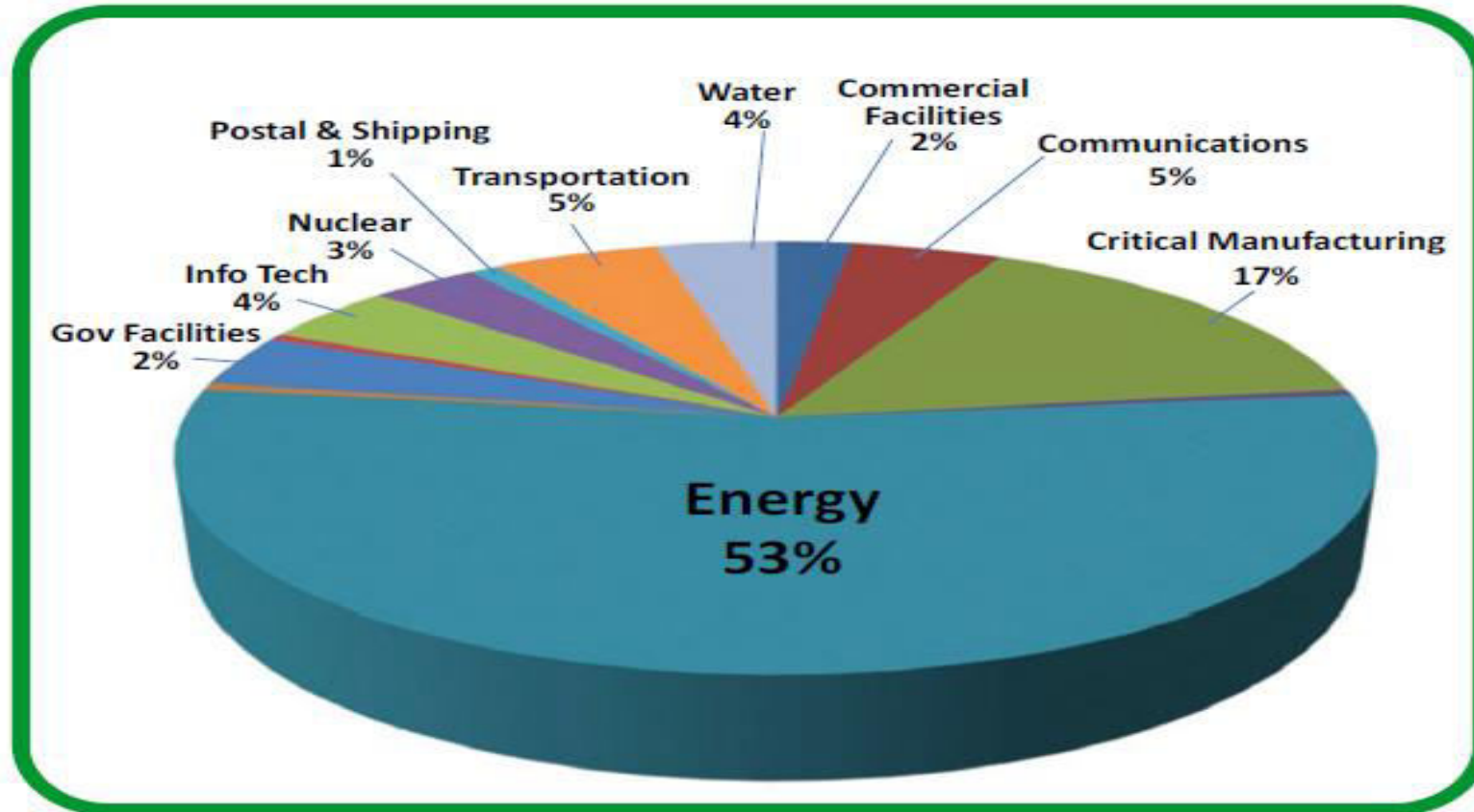
According to US Deptt Of Home land security's Industrial Control system Computer Emergency response team (ICS-CERT) , majority of Cyber attacks in 2013 were related to Energy Industry.

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
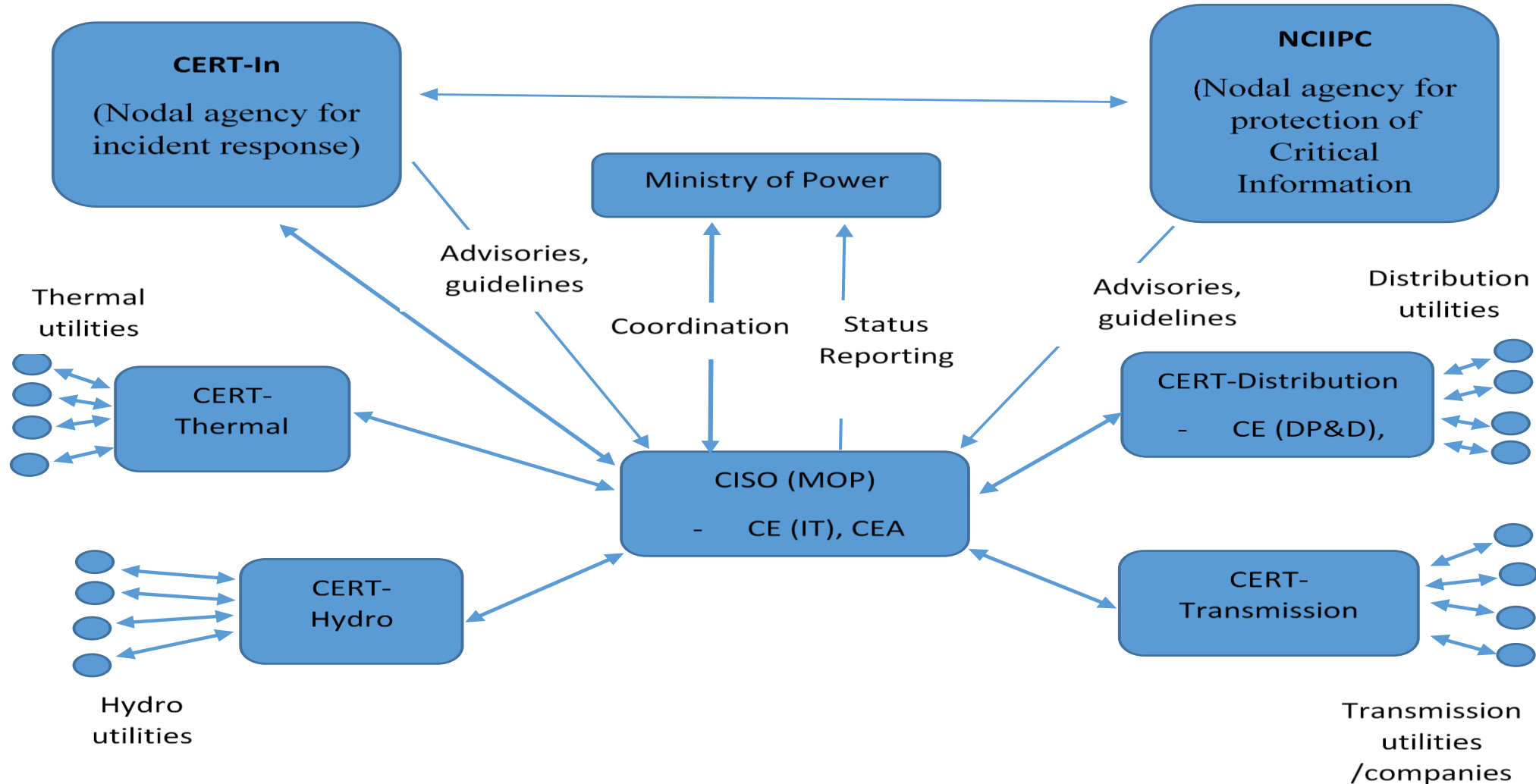
Cyber Security in Power system

- 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.

Constitution of Committee under Member (E&C)

- Ministry of Power vide letter dated 21.3.2017 constituted a committee under Chairmanship of Member (E&C).

- **To look into issues of power firms seeking to enter Indian Power transmission sector and to study the related issues of Cyber Security.**

- **To look into matter related to Standards of Technical specification, Testing standards and Sourcing of equipment/materials.**

- Members of the Committee:
    - Director (Transmission),MOP.
    - Sh.V.N. Kothari, Director D/O Commerce
    - Chief Engineer (PSETD),CEA
    - Chief Engineer (IT),CEA
    - Director(Projects), PGCIL
    - ED(NTAMC), PFCIL
    - Director (Public policy & Economic Taxation), IEEMA
    - Co-opted Chief Engineer (legal), Chief Engineer (F&CA) & GM (POSOCO)

- Meetings held on 28.3.2017 and 20.4.2017

- Report submitted on 19.7.2017

Issue 1 Foreign Firms in Transmission

 1. Relevant service is "Service incidental to energy distribution (CPC 887) .

2. The GATS schedule in the WTO, India has not taken any commitments on this particular service and, therefore, we retain the full policy space to restrict the tendering process as per its requirements and considerations.   With regard to non-committed sectors, such as, in this particular case, India can place restrictions on national treatment or market access.

Issue 1. Foreign Firms in Transmission(Contd.)

- While we are in a position to limit the participation of foreign countries in the tendering process here in India, the case of Japan, South Korea and Singapore stand out separately since we have a Free Trade Agreement (FTA) with them.
  - Even in the case of these three countries, there is a provision to exclude them in two specific instances.
  - The first being the case where the purchase made is for the Government only and for non-commercial use. An example in this regard would be any purchase made by the BSF or the BRO etc. The other instance is that we can invoke a security exception which is permissible under Article XVI of GATS.
- However, it seems that due caution has to be exercised in invoking the **security exception and the Department of Commerce has pointed out that it has not really been tested in any case so far**
- **"principle of reciprocity"** - if any foreign country debars firms of a country from bidding in their market on a flimsy ground, the same stance could be adopted by country for firms from that particular foreign country.

Issue 1. Foreign Firms in Transmission(Contd.)

- National Capital Good Policy 2016

" To make procurement of Heavy Electric Equipment under local competitive bidding and not under international competitive bidding (ICB) in domestically funded projects under Ministry of Power, Ministry of Steel and Ministry of Non-Conventional Energy , CPSUs and in the projects funded by PFC and REC."

- CEA Notification vide CEA/PEETD/205/218-296 dated 19.5.2016

(http://www.cea.nic.in/reports/others/ps/psetd/domestic_competitive_bidding_2016.pdf)

- Preferred market access in Telecom : http://www.dot.gov.in/pma-policy

- However only these restriction would not be sufficient to deal with Cyber security

Supply chain of a utility

Figure 1. Utility Supply Chain
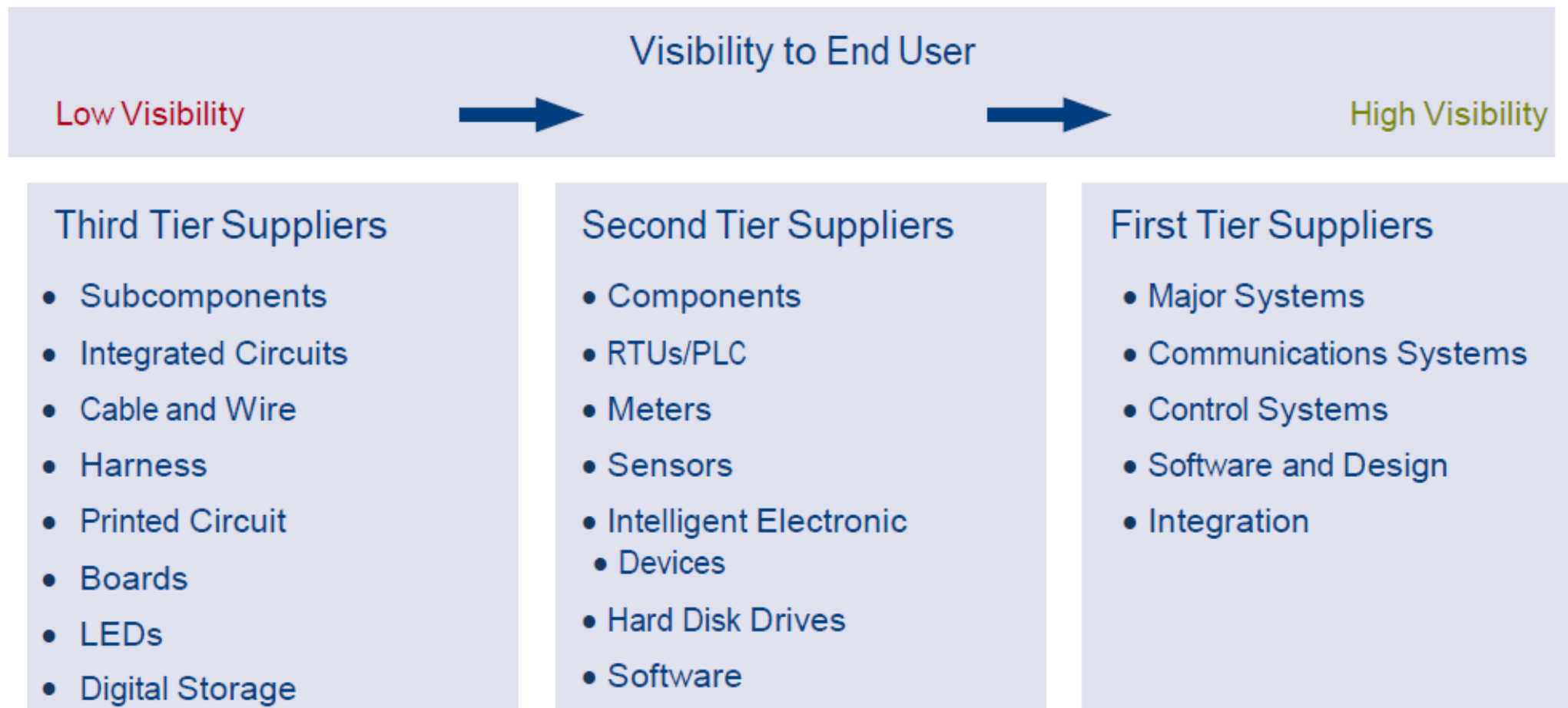
Visibility to End User

Low Visibility → → High Visibility

Third Tier Suppliers

- Subcomponents
- Integrated Circuits
- Cable and Wire
- Harness
- Printed Circuit
- Boards
- LEDs
- Digital Storage

Second Tier Suppliers

- Components
- RTUs/PLC
- Meters
- Sensors
- Intelligent Electronic
  - Devices
- Hard Disk Drives
- Software

First Tier Suppliers

- Major Systems
- Communications Systems
- Control Systems
- Software and Design
- Integration

Sub station Protection
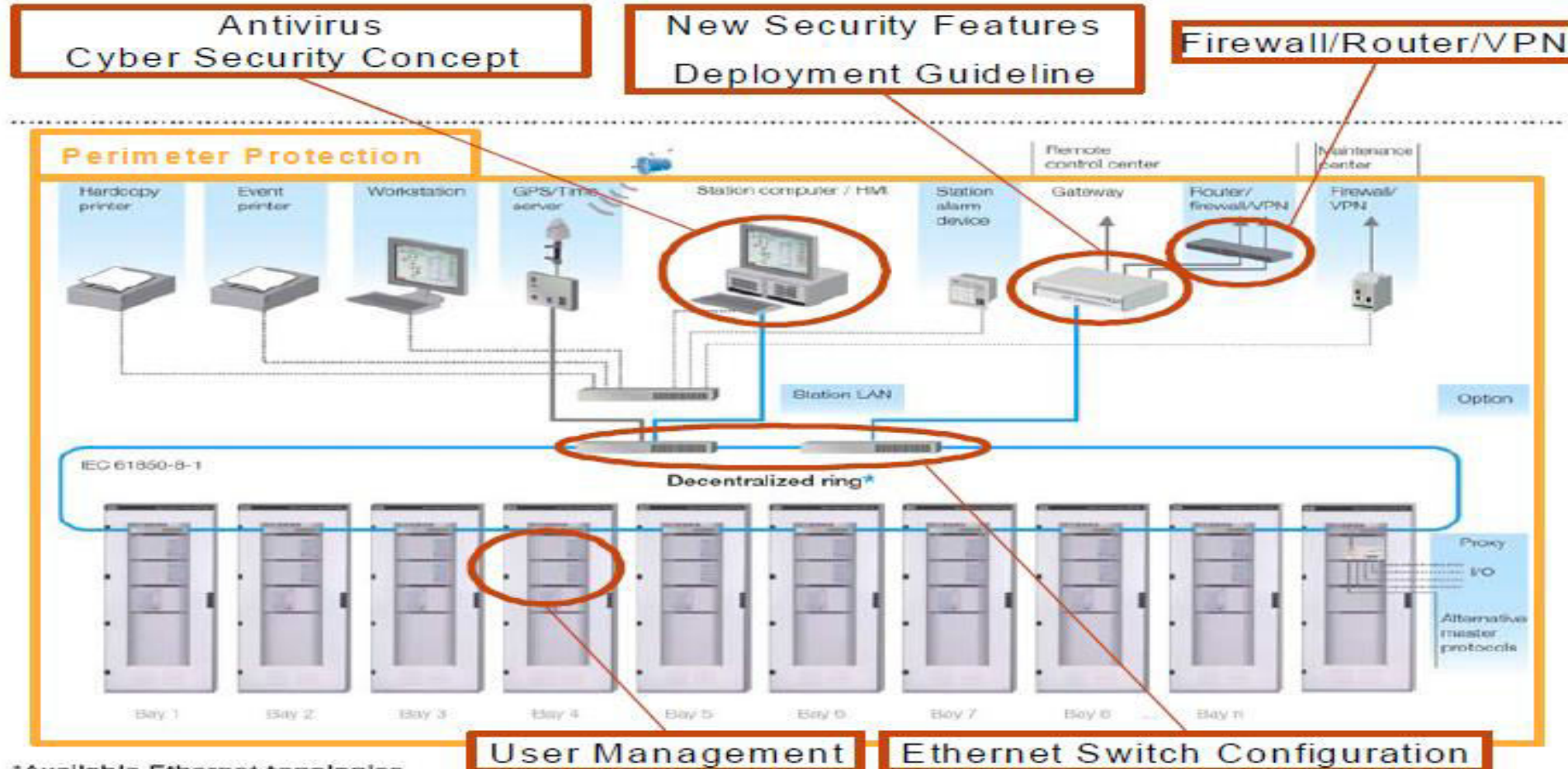
International experience

- The Australian Government in 2012 had intervened to block a privately owned Chinese Communication Company from winning lucrative contracts to help build the $ 36 billion fiber optic National Broadband Network. The decision, it seems was based on the advice from the Australian Security Intelligence Organization (ASIO).

- China Cyber Security Law (w.e.f.1.6.2017)

- Article 23 Critical network equipment and special cybersecurity products can only be sold or provided after being certified by a qualified establishment, and are incompliance with national standards. China's cyberspace administrative bodies and the relevant departments under the State Council will **draft a catalogue of critical network equipment and special products.**

- Article 35   Critical information infrastructure operators that purchase network products and services that might affect national security must pass a national security review.

Issue No. 2 Technical standards for material and equipment

- CEA Technical standards for construction and connectivity to grid does not specifically provide for Cyber security. These stipulates technical requirements .
- In procurement procedure testing following provisions may be incorporated:
  - The organization shall induct only those network elements which have been tested as per relevant contemporary Indian or international Security Standards (e.g. ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, BIS standards IS 16335: 2015 for power control systems etc.).

  - Vulnerability and Penetration test of Main and Back-up system shall be conducted during the FAT (Factory Acceptance Test). Accredited labs (like M/S Standardisation Testing and Quality Certification, a GOI enterprise) shall carry out third party security audit (Vulnerability and Penetration test) of SCADA/EMS system at site.

  - "Safe to connect' certification from supplier of hardware, software including their manufacturer, vendor, and service provider

Action to be taken

- Framing and implementation of Institutional and Legal, Technical, Contractual and Universal testing of equipment policy.

- **Institutional and Legal framework:** Every organization shall establish:
  - an institutional framework for ensuring compliance of legal, contractual and technical framework to make the system nearly 100% secure from cyber-attacks,
  - legal framework to incorporate various mandatory provisions for compliances from procurement to installation to operation.

- **Technical framework:** The security policy to lay down technical framework to be followed for the operation of the system to ensure cyber-security.

- **Contractual framework and Universal Testing:** The bidding documents should be so framed so as to encourage only firms which are manufacturing equipment in India to participate in the bid, including certification from the supplier that the equipment is "Safe to Connect".
  - The equipment procured under the specified guidelines shall be required to be tested for 100% reliability from any vulnerability from malware and cyber-attacks.

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 .

Social Engineering : Man & Mind

Baiting

ONLY AMATEUEURS ATTACK MACHINES, PROFESSIONALS TARGET PEOPLE

IF YOU THINK TECHNOLOGY CAN SOLVE YOUR SECURITY PROBLEMS, THEN YOU DON'T UNDERSTAND THE PROBLEMS AND YOU DON'T UNDERSTAND THE TECHNOLOGY.

Response to a question you never had

Creating distrust

Invest in both : Technology and People
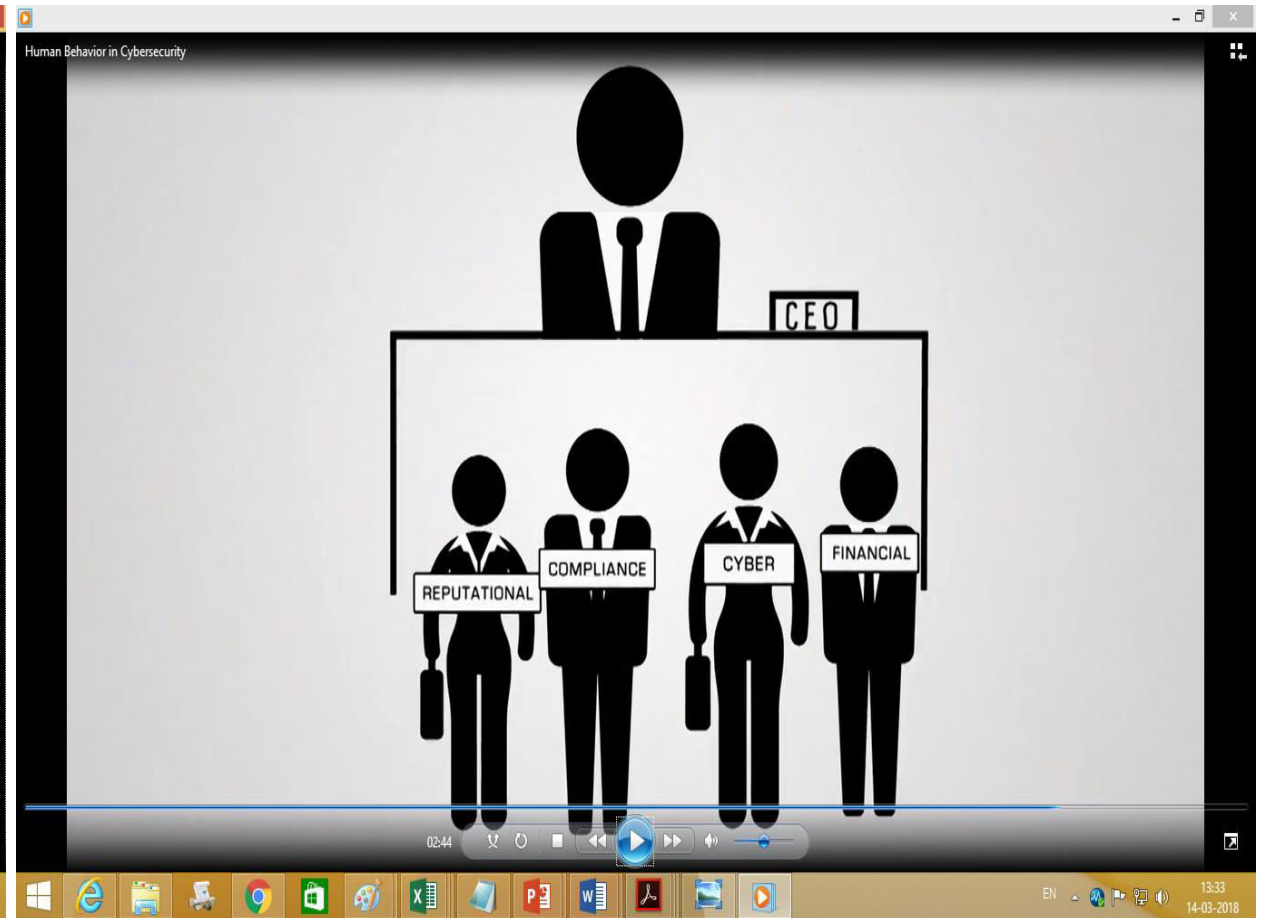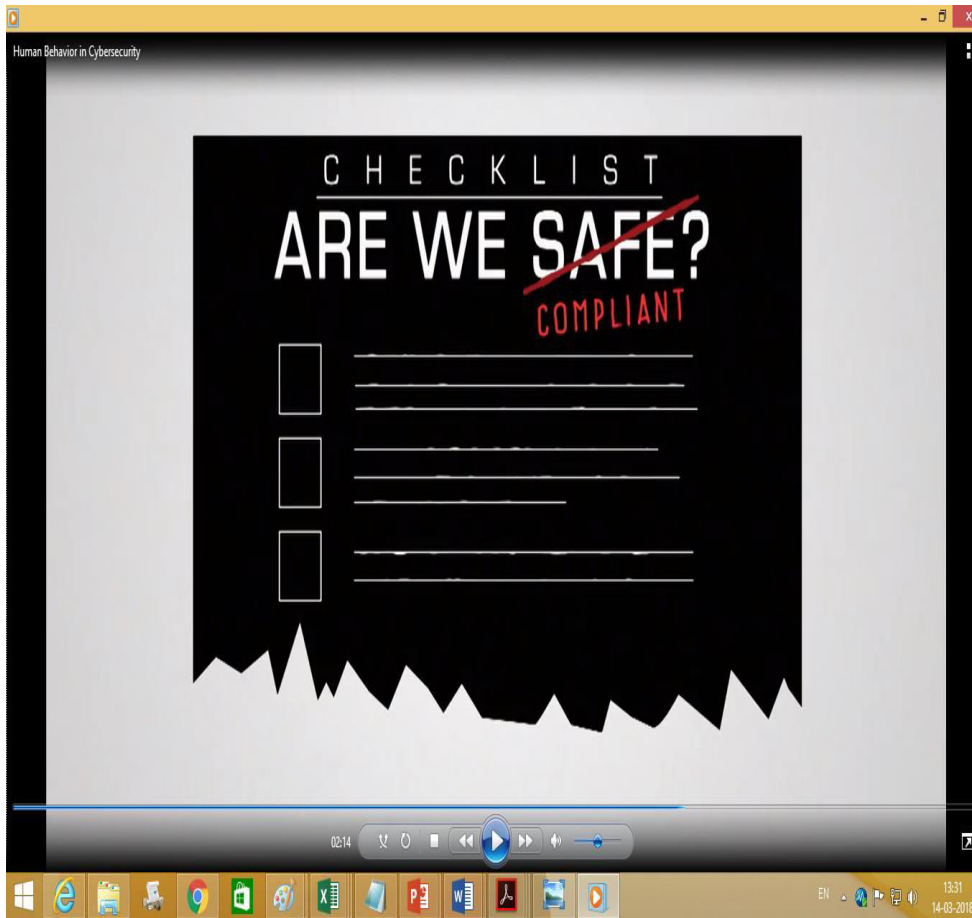
Present Status 1: Appointment of organization & plant level Chief Information Security Officers (CISO)

- **Single point of contact between organization and CEA/Sectoral CERT/CERT-In for all cyber security matters**

- **Accountability for implementing Cyber Security policies at organization level**

Present Status

- **4 Nodal officers – Sectoral CERTs**
- **121 Nodal officers – power utilities/IPPs**
  - CERT-Thermal (32)
  - CERT-Hydro (29)
  - CERT-Transmission (20)
  - CERT-Distribution (40)

Way Forward

- **Request State Chief Secretaries to facilitate nomination of CISOs of state utilities (within 15 days)**

- **Request IPP heads to submit CISO nominations (within 15 days)**

2. Identify organization-wise Critical Infrastructure

- **For implementing security policies & controls over the identified critical infrastructure**
- **Security auditing of the identified critical infrastructure.**
- **Vulnerability assessment & penetration testing of identified critical infrastructure**

Present Status

- **NTPC, NHPC and PGCIL have identified their infrastructure in respect of business criticality and implemented ISO 27001 controls**

Way Forward

- **Instruct nodal officers of power utilities/IPPs to identify their critical infrastructure and submit status to CEA (within 15 days)**
- **Collection of security policies & control implementation status from nodal officers of power utilities/IPPs (within 1 month)**
- **Request nodal officers to conduct security audit, vulnerability assessment & penetration testing of the identified critical infrastructure**

3. Formulate Crisis Management Plan (CMP)

- **Organization specific plan for tackling IT/operation related crisis**

Present Status

- **NTPC, NHPC and PGCIL have drafted their CMPs**
- **NHPC has submitted CMP for Hydro sector**
- **Distribution CMP has been prepared and issued in December,2017.**
- **CERT-In conduct workshops on CMP**

Way Forward

- **Request CERT-In to conduct CMP workshops for power sector utilities (within 15 days)**
- **Instruct nodal officers of utilities/IPPs to attend CERT-In workshop on CMP (within 1 month)**
- **After workshops, instruct nodal officers to prepare their organization specific CMP (within 2 months)**

4. Security Mock Drills

- **Readiness of organization to tackle cyber incidences**
- **Mock drills are facilitated by CERT-In**

Present Status

- PGCIL participated in mock drill in the past

Way Forward

- Instruct NTPC, NHPC and PGCIL to participate in mock drills at their organization level in co-ordination with CERT-In (within 3 months)
- Nodal officers of other utilities (sector specific) and CEA representatives can be invited in mock drills for acclimatization.
- Thereafter, instruct other utilities to conduct mock drill at their end in coordination with CERT-In (within 6 months)

5. Information Sharing & Analysis Centre (ISAC) – Power

- **Common platform for sharing & analyzing cyber security incidences in Power Sector**

Present Status

- **ISAC-Power static page is available on CEA website**
- **ISAC-Power page provides information about nodal officers, links to IT act, rules, guidelines & presentations**

Way Forward

- **Develop dynamic and database supported ISAC-Power portal for better coordination between stakeholders.**
  - **Concept paper for ISAC-Power** (within 1 month)
  - **Design & develop ISAC-Power portal** (within 6 months)

6. Trainings / workshops on Cyber Security

Present Status

- CERT-In organizing cyber security workshops.
- Sectoral CERTs organizing workshops/presentations (last workshop conducted on 15.02.17 by PGCIL)
- **CEA with IPPAI taken imitative and organized three Regional workshops in Bangalore, Mumbai & Delhi**

Way Forward

- Request to DG, NPTI to conduct cyber security courses for power utilities.
- Nodal officers of power utilities to register themselves for CERT-In workshops.
- All Nodal officers to submit quarterly reports to CEA on training attended / organized by them on cyber security

CISO Nomination

Sector	CISO Nomination Status SR	
	Received	Not Received
Hydro	All State Utilities	Private Utilities
Thermal	NTPC. Tamilnadu, Karnataka	Telangana(TSGENCO),Kerala(KSEB), Andhra Pradesh (APGENCO), IPPs,Nuclear
Transmission	All State Utilities	Private Transmission Licensees
Distribution	Karnataka(5),Andhra Pradesh(2/4),Tamilnadu,Kerala	Andhra Pradesh (2-Central , Eastern),Kerala(KINESCO, Infopark), Tamilnadu (Technopark), Lakshdeep,A&N Islands

CISO Nomination

Sector	CISO Nomination Status-ER	
	Received	Not Received
Hydro	West Bengal, Odisha	Jharkhand (DVC, JUVNL)
Thermal	Bihar (KBUNL Muzaffarpur, NPGCPL Patna), Jharkhand (TVNL), West Bengal (DVC, WBSEDCL, CESCL, WBPDCl)	Bihar (BSPGCL), Jharkhand (JUVNL), Andaman Nicobar (ED A&N)
Transmission	Bihar, Odisha, West Bengal	Jharkhand, Sikkim
Distribution	Bihar(BSPHCL, SBPDCL), Jharkhand (Tata Steel Ltd.), Odisha (CESCL), West Bengal (WBSEDCL, CESCL)	Bihar (NBPDCL), Jharkhand (JSEB, JUSCO), Odisha (NEESCO, SOUTHCO, WESCO) West Bengal (IPCL)

Quarterly Preparedness Monitoring -AGENDA

(Status as on :
)

S.No.	State	Sector (G/T/D)	Utilities	Status of CISO Nomination	Critical Infra Identified	Crisis management Plan Prepared	Status of CS mock drill	Status of Training/ Workshops organized/ participated by utility	Action taken on CERT-In/NCIIPC Advisories
1	Tamilnadu	T	TANGEDCO	Yes/No	Yes/No	Yes/No	Done on ____		

Tools

No	Name	Download URL
1	TeraTerm	https://ttssh2.osdn.jp/index.html.en
2	WinSCP	https://winscp.net/eng/docs/start
3	GeoIP	https://www.maxmind.com/en/geoip2-services-and-databases
4	Sigcheck	https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck
5	HashMyFiles	http://www.nirsoft.net/utils/hash_my_files.html
6	FTK Imager	https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1
7	Strings	https://technet.microsoft.com/en-us/sysinternals/bb897439.aspx
8	TCPView	https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
9	WireShark	https://www.wireshark.org/
10	Process Explorer	https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
11	Process Monitor	https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
12	Reg Ripper	https://github.com/keydet89/RegRipper2.8
13	Event Viewer	Windows –[Admin Tools]–[Event Viewer]
14	Autoruns	https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
15	Windows Registry Recover	http://www.mitec.cz/wrr.html
16	Windows Prefetch Folder	C:¥Windows¥Prefetch

Cyber security : Many battles and A war

If you know the enemy and know yourself, you need not fear the result of a hundred battles.
If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
If you know neither the enemy nor yourself, you will succumb in every battle."

Each of these three points of 5th Century B.C book directly applies to the world of cyber Security.
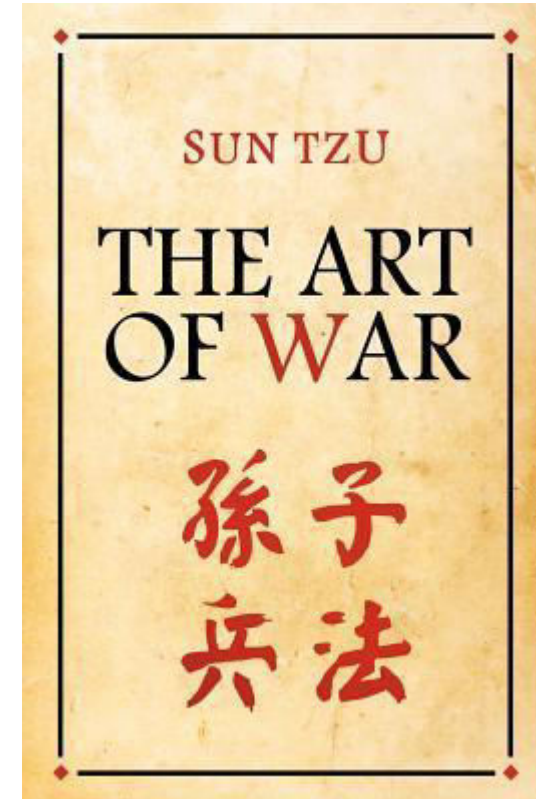
New   IT initiatives and need of support from States

- National Power Portal(NPP) –Dashboard and Data analytic for power sector at one place
  - Data entry for all six application is being done and report is being generated in testing phase. Launched by Hon'ble Power Minister on 14th November,2017
  - Five to be held in next two months.
  - While data of Coal supply is fed regularly in NPP, the data entry **by generating station for daily generation report (DGR) in NPP is yet to pickup.**
  - If there is requirement of training , CEA can arrange regional workshops

- Geo Spatial Energy Map
  - NITI Aayog on the instruction of PMO initiated this project .
  - ISRO and CEA are preparing Geo spatial map o all Generation, transmission and distribution assets.
  - Any state which want GIS mapping of its assets above 33 kV (initially) , can get it done free of cost
  - Map would be useful for operation and asset management .
  - **Format for Data shared by concerned Divisions of CEA with all state utilities . Data from Transmission and Distribution utilities is awaited.**

Installed Capacity
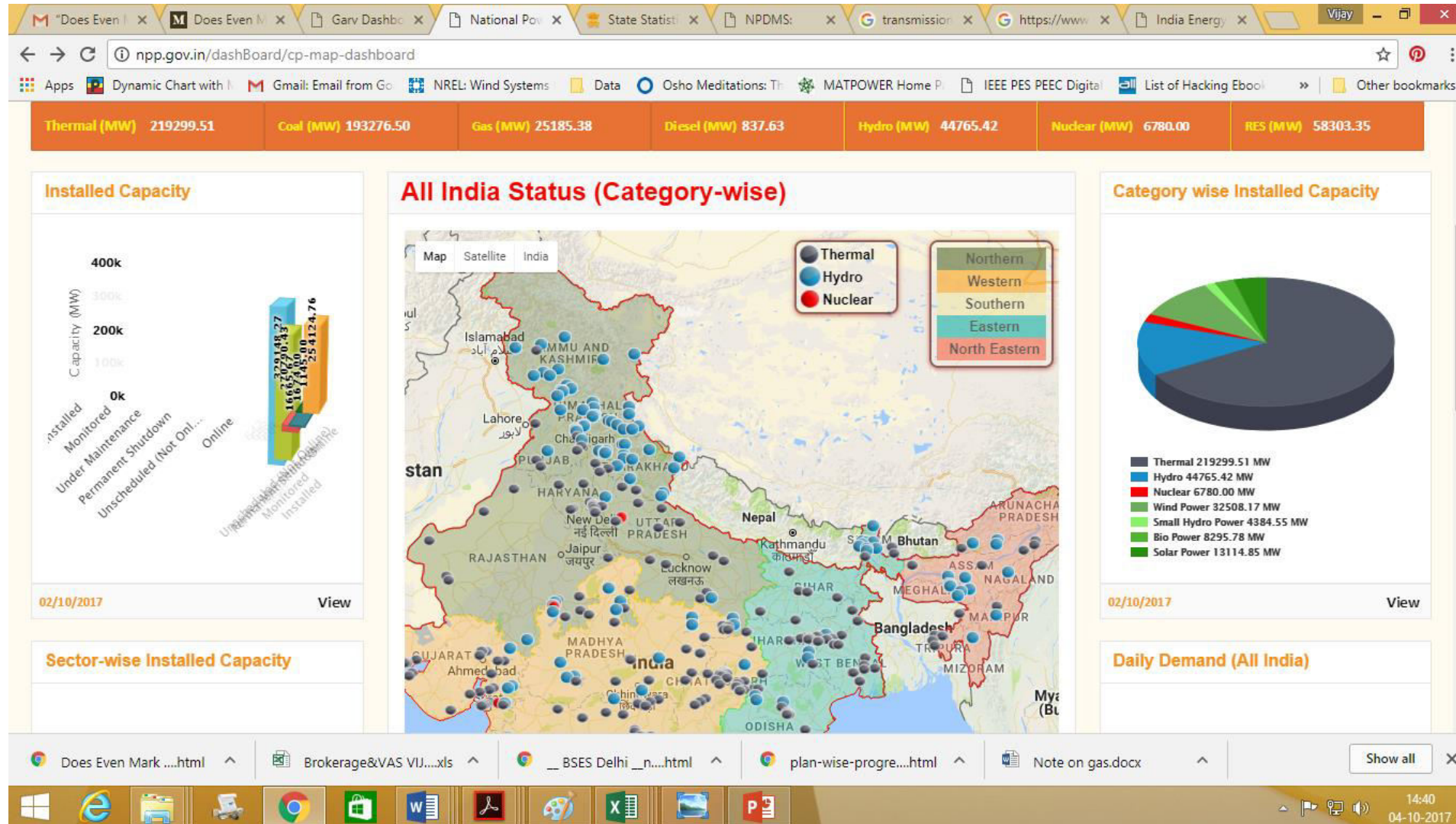
State wise Information
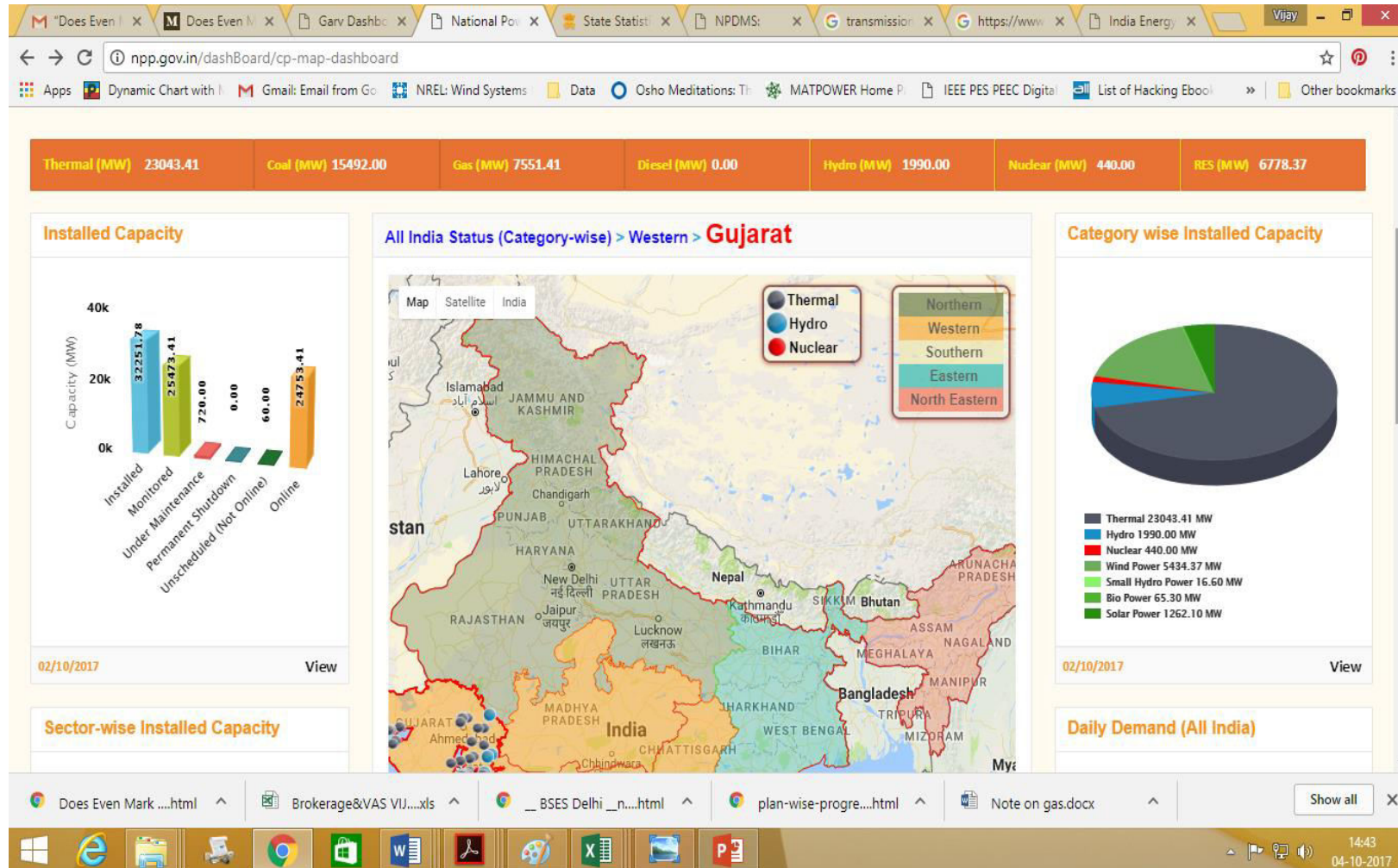
ISRO-CEA Geo spatial Energy Map
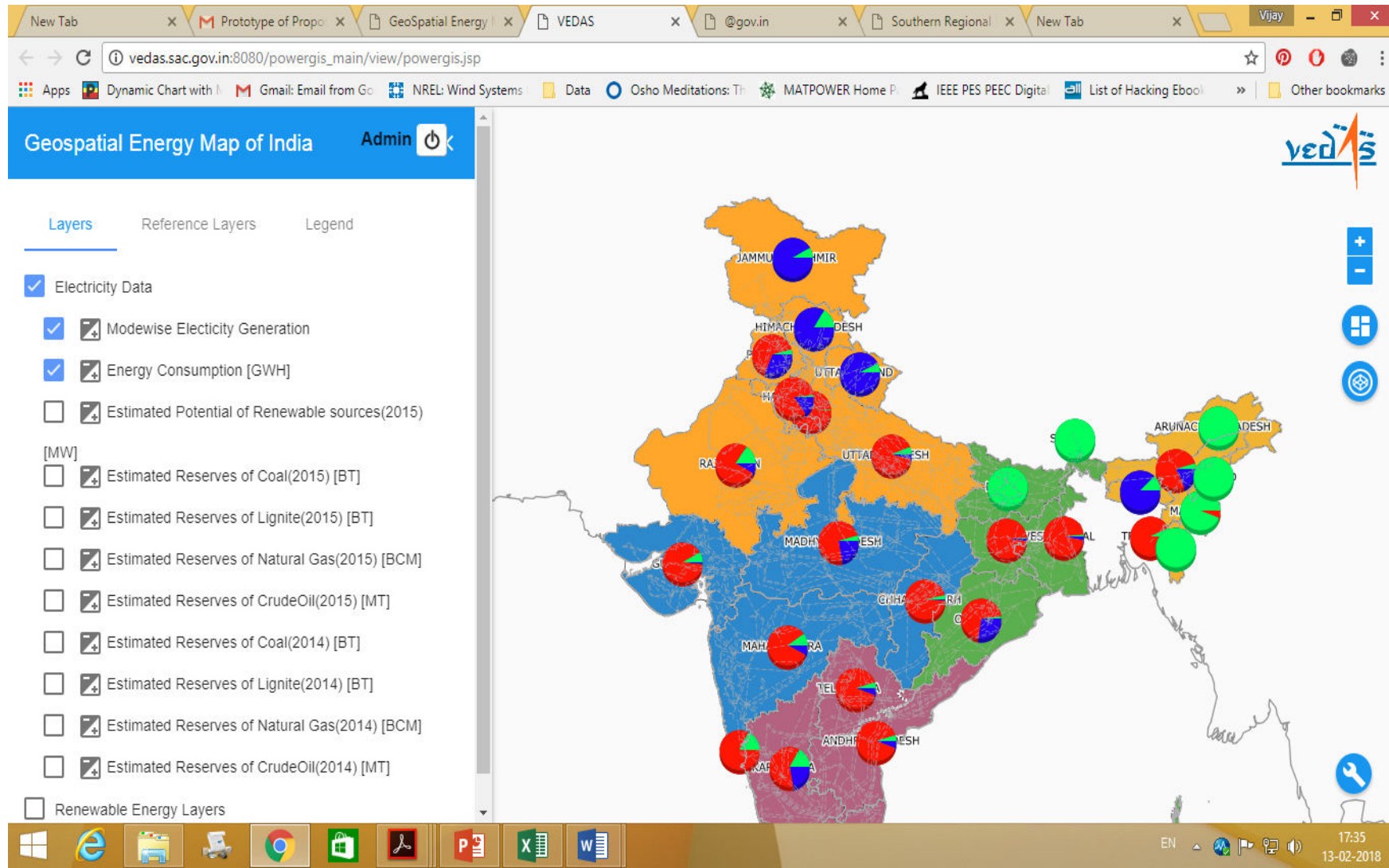
Geo Spatial Map with layer control
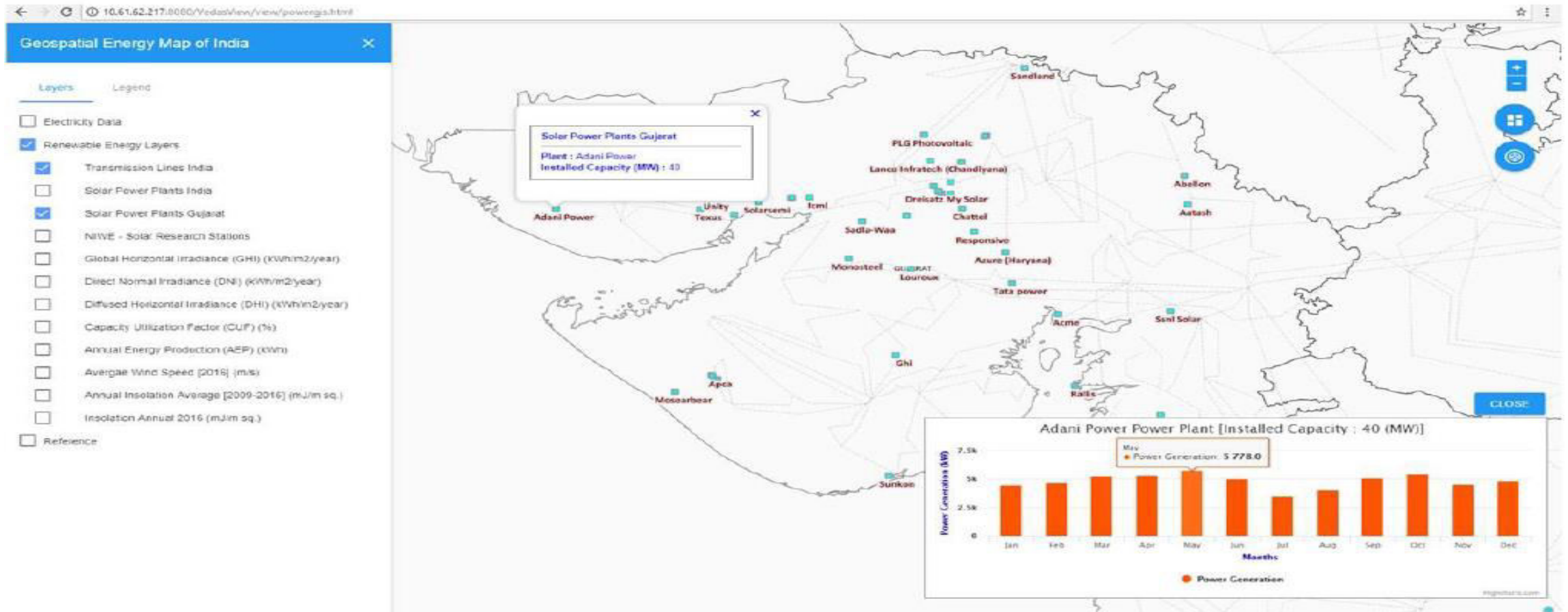
Shared Responsibility

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

— **Newton Lee**, **Counterterrorism and Cybersecurity: Total Information Awareness**

IT adoption can change Life

Twitter & MOP Mobile Application

A success story of Village Electrification

10th June,2017 A village boy from Bharthapur , Kanpur Dehat UP tweet

10ᵗʰ June ,2017

15th June,17 Garv2 App study

18th June,2017

19th June,2017 Contact with REC

20ᵗʰ June,2017 REC TEAM REACHED VILLAGE

21st June,2017 Engineer informed applicant

22rd June,2017 Documents collection by REC

24th June ,17 Pillar reached village

6th July,2017 REC village survey

7th July ,2017 All worked together

20th July,17 REC Implementation agency inform reason of delay in transformer delay

23rd July 17 Encourage locals to get connection and issue of Transformer discussed with REC

24th July 17 Discom provided meters

14ᵗʰ Aug,2017 Village Electrified within 64 days

Happiness reached home

Aware consumer consume Energy Efficiently

Happy Diwali from a remote village

Diye Se Diya Jale

Let us work together to bring Light in life of everyone.

Thank you
vmenghani@nic.in