Final Report on "Domestic Manufacturing Capacity & Potential Cyber Security Challenges in the wind sector and Way Forward"

March, 2024

Acknowledgments

This report was prepared under the chairmanship of Dr. V. K. Saraswat, Member (Energy) & guidance of Sh. Rajnath Ram, Adviser (Energy), NITI Aayog. We extend our sincere gratitude to Ministry of Power (MoP), Ministry of New and Renewable Energy (MNRE), Central Electricity Authority (CEA), Ministry of Electronics and Information Technology (MeitY), National Institute of Wind Energy (NIWE), Indian Computer Emergency Response Team (CERT-In), Solar Energy Corporations of India (SECI) and National Critical Information Institute of Infrastructure Protection Centre (NCIIPC) for their contribution & guidance for preparing the report.

We acknowledge all other stakeholders who contributed in the successful completion of the Final Report on "Domestic Manufacturing Capacity & Potential Cyber Security Challenges in the Wind Sector and Way Forward".

Contents

Executive Summary

This comprehensive report delves into the dynamic landscape of India's wind energy sector, aiming to address critical challenges of cyber security and capitalize on opportunities. The report's primary focus is to raise specific concerns of cyber security due to import (specially from China) of the Wind Sector components by Wind Turbine Original Equipment Manufacturers (OEMs). The main issues are OEMs data collection servers which are situated outside of the country, vulnerabilities in data and power system network operations due to updating operating software's of Wind Plant devices by OEMs without any permission from Grid-Operator and MNRE etc.

As the wind energy sector globally achieves substantial growth, reaching a cumulative installed capacity of 906 GW in 2022 with a notable 9% year-on-year increase, India emerges as a crucial player. Ranked fourth globally in installed wind power capacity, India plays a pivotal role in achieving ambitious targets for non-fossil fuel capacity and Net Zero by 2030 and 2070, respectively.

Despite the significant potential highlighted by the National Institute of Wind Energy, only 6% of the assessed capacity has been realized, signalling room for substantial growth. The report underscores the robust policy framework supporting domestic wind manufacturing, coupled with the challenges faced in the production of critical components, leading to significant import reliance.

A noteworthy aspect is the escalating competition with China, holding a 61% share of global wind-turbine assembly capacity. The report addresses challenges faced by the RoDTEP scheme, aimed at boosting India's exports, and emphasizes the exclusion from the Advance Authorization scheme and increased costs in the supply chain.

The second half of the report delves into the challenges and opportunities surrounding India's wind energy sector, with a focus on domestic manufacturing capacity and potential cybersecurity threats. The key findings and recommendations are summarized as follows:

i. **Manufacturing Capacity Challenges:** The report identifies critical challenges in the manufacturing of key components such as blades, towers, gearboxes, and bearings. Issues such as the lack of availability of non-standard sizes, quality concerns, and inconsistent demand have resulted in a significant reliance on imports, hindering the growth of domestic manufacturing capacity.
ii. **Critical Minerals Availability Analysis:** A detailed analysis of critical minerals required for wind turbine components reveals challenges in the availability of materials such as balsa wood, specialized resins, and steel plates with non-standard specifications. Import dependence is prevalent, especially for components like tower flanges and castings, posing a risk to the sustainability of the industry.
iii. **Cybersecurity Threats and Risks:** Wind turbines' capability to exchange information through Power Plant Controllers poses a significant cybersecurity threat. The PPC (Power Plant Controller) software is of critical importance and associated with risks- used in the device which connects the wind farm directly to the national/state grid. PPC OEMs of

foreign origin especially neighboring countries, need to be examined and call needs to be taken for their suspension while not adhering to the protocol. The report emphasizes the potential risks associated with cyberattacks on wind turbines, including the compromise of grid operations, especially when managed remotely by owners stationed outside India. The need for robust security measures is crucial to safeguard national infrastructure.

iv. **Competitive Landscape and Incentives:** The global competitive landscape is discussed, with China emerging as a major competitor in wind equipment exports. The report outlines the incentives provided by the Indian government, such as the Remission of Duties and Taxes on Export Products (RoDTEP) scheme, while acknowledging challenges, including the exclusion from the Advance Authorization scheme and increased manufacturing costs.

v. **Mandatory Certification of foreign Software/Hardware:** Certification and approval of all IPRs, software and device/hardware from the OEMs of foreign origin especially from neighboring countries by Central Electricity Authority of India (CEA), Ministry of Electronics and Information Technology (MeitY) and Standardization Testing and Quality Certification (STQC).

vi. **Budgetary provision for building infrastructure to address cyber-Security threats**. Every Utility must appoint CISO (chief information security officer) who should reside in India and report for compliance to the proposed independent agency on the Power Sector Cyber Security aspects.

vii. A**ll the OEMs of the Wind Sector needs to locate and re-locate their Data Centre and Research & Development Centre inside the country** failing which OEMs should be de-bar from participating in the tenders and supplying the items in the Country. Ministry of New and Renewable Energy should prepare timelines for relocation of the Wind Sector OEMs Data, R&D Centre inside the country.

In conclusion, this report advocates for a multi-pronged approach integrating policy interventions, manufacturing support, and robust cybersecurity measures. With a distinct emphasis on the rising influence of Chinese OEMs and the associated security concerns, the report urges stakeholders to collaboratively address challenges and harness opportunities, ensuring India's sustained growth in renewable energy and cybersecurity resilience.

Final Report on "Domestic Manufacturing Capacity & Potential Cyber Security Challenges in the wind sector and Way Forward"

Wind Energy Potential

As per the Global Wind Energy Council Report 2023, the total cumulative wind power installed capacity globally stood at 906 GW in 2022, with YoY growth of 9%. Since 2010, more than half of all new wind power capacity was added outside the traditional markets of Europe and North America, mainly driven by the continuing boom in China and India. According to the GWEC's Global Wind Report, 2023, the top five countries with respect to Installed wind power were China (333 GW), followed by EU (225 GW), the US (144 GW), Germany (58 GW) and India (44.73 GW).

2. India is the South Asia leader in wind energy sector and the sector growth is largely led by the indigenous wind power manufacturing industry and now ranks fourth in Installed wind power capacity in the world. Wind energy is crucial to achieve 50% installed capacity from non-fossil fuel-based energy resources by 2030 and Net Zero by 2070. India has significant potential for both onshore and offshore wind energy production. With the continuous efforts, India has developed around 17.25 GW of domestic wind manufacturing capacity (Table-1).

3. The government, through National Institute of Wind Energy (NIWE), has installed 993 wind-monitoring stations all over the country for assessing the potential. The latest assessment indicates the wind power potential of 302.25 GW, 695.50 GW and 1,164 GW at the hub height of 100 meters,120 meters and 150 meters respectively and most of these potentials exist in the seven windy States as listed in the table below:

Table 1: Potential of Wind by windy states

S.No.	State	Wind Power Potential at 100 mtr agl (GW)	Wind Power Potential at 120 mtr agl (GW)	Wind Power Potential at 150 mtr agl (GW)
1	Andhra Pradesh	44.23	74.90	123.33
2	Gujarat	84.43	142.56	180.79
3	Karnataka	55.86	124.15	169.25
4	Madhya Pradesh	10.48	15.40	55.42
5	Maharashtra	45.39	98.21	173.86
6	Rajasthan	18.77	127.75	284.25
7	Tamil Nadu	33.80	68.75	95.10
	Total (7 windy States)	292.97	651.72	1082
	Other states	9.28	43.78	81.85
	All India Total	302.25	695.50	1163.85

4. Only 6% of India's wind potential has been capitalized through the wind farms. The onshore wind stations likely to occupy more land area and installation of more wind turbines may lead to RoW issues and may affect realization of wind potential at large scale.

5. India has 7600 km of coastline. The initial estimates indicate the potential of offshore wind in Gujarat and Tamil Nadu coasts alone is around 70 GW. The offshore wind potential of Gujarat and Tamil Nadu stands at 36 GW and 35 GW respectively. Currently, the share of non-fossil fuels in total electricity installed capacity stands at 43% which includes wind installation of 44.73 GW as on Dec, 2023. To achieve the 45% emission intensity reduction by 2030, we have to install about 120-140 GW cumulative wind capacity by 2030 under the net-zero scenario.

Policy incentives for domestic wind manufacturing

6. To encourage domestic manufacturing of Wind Turbine Generators (WTG), the Government provides financial incentives like custom duty exemption on critical components, waiver of Inter-State Transmission System charges for the projects to be commissioned by 30th June, 2025. Renewable Purchase Obligations (RPO) up to 2030 has been also notified. Standard Bidding Guidelines are in place for tariff based competitive bidding process for procurement of Power from Grid Connected Solar PV and Wind Projects. Government has also issued orders that power shall be dispatched against Letter of Credit (LC) or advance payment to ensure timely payment by distribution licensees to renewable energy generators.

Domestic Manufacturing Capacity of Wind Turbine Component

7. India is a major wind turbine manufacturing hub with the presence of leading global and Indian companies such as Suzlon Energy Ltd., Siemens Gamesa Renewable Power Private Ltd., and GE India Industrial Private Ltd. With over 17 wind turbine manufacturing companies' annual production capacity in country exists about 15,000 MW. These companies export wind turbines and blades to Australia, Brazil, Europe, USA and other countries. Table 2 summarizes the Annual domestic manufacturing capacity by Manufacturers.

Table 2: Status of Domestic Manufacturing Capacity

Manufacturer	Country of origin	Turbine size (MW)	Annual Manufacturing (MW)
Suzlon Energy Ltd.	India	2.1 - 3.0	4,500
Vestas Wind Technology	Denmark	2.0-3.6	3,000
Siemens Gamesa Renewable Power	Spain	2.0-3.6	4,000
Envision Wind Power Technologies	China	2.5-3.3	1,000

Senvion Wind Technology	Germany	2.3-2.7	1,000
Nordex India Pvt. Ltd.	Spain	3.0	1,000
GE India	USA	2.3-2.7	1,000
Inox	Austria	2.0-3.0	1,000
Emergya Wind Turbine	The Netherlands	1.0	250
Others			500
Total			**17,250**

8. Table 3 provides the status of domestic manufacturing capacity of various components. Towers, Blades and Gearbox account for almost 60% of the total cost of WTG set-up. Table-4 provides details of critical materials required for each component and their domestic availability. The table highlights availability of non-standard sizes, quality, and lack of consistent demand has resulted imports. A thrust is required to promote domestic manufacturing.

Table 3: Domestic Manufacturing Capacity: Local & Import share

Name of the Wind Turbine Component	Total Manufacturing Capacity (Per annum)	% Cost Share of Wind Turbine Generator (WTG) setup	100% local content by OEMs	Imported by major OEMs (% varying)
Towers	5,200 MW	26%	Vestas, Inox, Envision, Suzlon, GE	Siemens, Gamesa
Blades	Not available	22%	Vestas, Inox,Senvion, GE, Siemens, Gamesa, Suzlon, Envision	-
Gearbox	8,000 MW	12%	Suzlon, Siemens, Gamesa, GE	Vestas, Envision, Inox, Senvion
Power Converters	Not available	5%	GE, Siemens, Gamesa, Vestas, Inox	Envision, Suzlon, Senvion
Generators	Not available	4%	Suzlon, GE, Siemens, Gamesa	Vestas, Envision, Inox, Senvion
Transformers	Not available	3.6%	GE, Siemens, Gamesa, Vestas, Inox, Senvion, Suzlon	Envision (only Aux. Transformer)

Castings	11,590 MW	27. 4%		
Yaw Drives	10,000 MW			
Pitch Drives	5,000 MW			
Others (Main Shaft, Rotor bearing etc)	Not available			

1. *Domestic component share of Suzlon S120 Model is approximately 85%.
2. Envision is sourcing Blades from 2 plants in India i.e., LM Wind Power in Dabaspet (Karnataka) and Halol (Gujarat). Notably, Envision has now set up a new Blades factory in Trichy (Tamil Nadu) and will commence production shortly.

Table 4: Domestic Manufacturing Capacity: Critical Minerals Availability Analysis

S. No.	Component	Critical metals/minerals	Availability Status
1	Blade	Balsa wood, Foam, Pultruded carbon fibre, Specialized Resins (Adhesive resins), High Modulus and Glass Fibres	Manufacturers fully import Carbon & Balsa, while rest of the components are locally purchased and at times Resin is partially imported based on new basis requirement.
2	Tower	Steel plates	Indian vendors are not ready to supply non-standard sizes due to low volume which do not justify capex investment. Indian Steel Producers can produce such specifications. However, they are not producing due to lack of consistent demand. Requires steel plates with non-standard specifications. No specific size available from Indian suppliers, hence imported from South Korea, China.

		Tower Flanges and Paint	No domestic supplier for wind turbines with diameter > 5.5 m. However domestic suppliers are available to supply tower flanges upto a diameter of 5 m. Some manufacturers procure all the rings locally, however, some players import rings from low-cost neighboring countries resulting in underutilized capacity in India. Low volumes make it difficult for Indian suppliers to upgrade their facilities to supply tower flanges forever increasing size of new turbine models.
			Sufficient quantity of paint is locally available; as multiple suppliers are available in India. Over the years, quality & consistency issues have improved to a great extent.
3	Bearings	Specialized alloy steel	Quality related issues in domestic sector
4	Forging	Main Shaft	If the main shaft is casted then it is available in India otherwise it is imported (mostly from Asia pacific/China).
		Forged rings (for pitch bearings and slew/yaw bearings)	There are no domestic steel supplier manufactures to supply the continuous cast bloom steel with large diameter. (Imported from China, South Korea, Italy)
		Tower Flanges Special alloy steel/Concast (Continuous cast) with higher diameter	

5	Casting	Wind turbine Castings and Gear box Castings	As per inputs received from industry, most manufacturers procure all the castings locally. However, some players import from low-cost neighboring countries due to factors like cost competitiveness and implementing global sourcing method. Low volumes make it difficult for Indian suppliers to upgrade the existing facilities to supply castings for ever increasing size of new turbine models.
6	Gear box	Not available	There are three domestic manufacturer /supplier of gearbox i.e.M/s. Flender Drives Private Limited (Winergy), M/s. ZF Wind Power Coimbatore Private Limited and M/s. NGC Transmission, Chennai. NGC exports 100% of its products, Flender product is not suitable for Suzlon WTG models and ZF gearboxes are supplied from SEZ.

9. The Ministry of New and Renewable Energy (MNRE) cnotifies the Revised List of Models & Manufacturers (RLMM) from time to time. This list consists of the certified types and quality of wind turbines models/manufacturers eligible for installation in the country. As per updated RLMM list of November 2023, out of 28 wind turbine models/ 12 manufacturers, there is only one Chinese company namely; M/s Envision Wind Power Technologies India (Pvt) Ltd, which is a subsidiary of Envision Energy (Jiangsu) Co. The multinational companies host the data at their head office located outside India. For such OEMs, the data collection servers and research & development operations are normally based outside India. Such practice leads to security concern with regards to vulnerability of data and network operation.

10. Wind Turbines are capable of exchanging information with Utility Operators and Aggregators through a device called the Power Plant Controller (an intelligent cyber-physical device) and because of this functionality, they pose a risk to cyberattack and may render grid operations insecure. Exploiting this attack vector, the attacker can enter the network and carry out lateral movement to other high value assets. Some of the owners of these RE resources are stationed outside India and manage the operations of these devices remotely, this can lead to major threat on the National Grid as well as breach of critical data.

Support offered to manufacturers:

11. China is India's biggest competitor for wind equipment exports, accounting for upto 61% of global wind-turbine assembly capacity in 2023 whereas India's share was 32%. Chinese wind industry developments based on huge incentives provided by the Chinese government and also rebates on export tax to make them globally competitive. Exporters based in China are required to pay export value-added tax (VAT) on goods that they ship abroad and can get an export tax rebate ranging from 6% to as high as 16% (2018 notification).

12. **RoDTEP rates across the industries in India:** The new Remission of Duties and Taxes on Export Products (RoDTEP) scheme effective from 2021 aims at boosting India's exports and global competitiveness by compensating various taxes like VAT and electricity duty. It covers over 8500 tariff lines across sectors like marine, agriculture, gems & jewelry with incentive rates varying from 0.5% to 4%, replacing the earlier Merchandise Exports from India Scheme (MEIS). However, exclusion of Advance Authorization scheme on duty-free imports used for exports is likely to impact exporters. Amongst various sectors, textile products, food and agri products have received maximum favorable rates under RoDTEP, that of upto 4.3%. Metals and automobile sector exports receive the rebates of upto 2.3% whereas exports in wind industry get rebate of 0.8% only under the RoDTEP scheme plus OEMs have to face BCD rates at an average of 10% (excluding cess and surcharges) on raw material or components to manufacture WTG. Recent supply chain disruptions with increased fuel cost have also distorted the market and the cost of manufacturing has gone up and thus OEMs face challenges of less margins

13. The Way Forward for improving Domestic Manufacturing Capacity in the Wind sector

i. **Announcement of bidding calendars - A**nnual wind capacity bidding calendars needs to be announced in advance so that the industry is aware and visualize potential business opportunities. It needs to ensure that the work on state specific bids should be such that crowding is avoided in high wind states. MNRE dated 31.03.2023 has already issued a bidding trajectory for renewable energy power projects wherein bids for RE capacity of 50 GW per annum, with at least 10 GW per annum of wind energy capacity are to be issued each year from financial year 2023-24 to FY 2027-28.

ii. **Enforcement of RPO trajectory:** Ministry of Power, under the Energy Conservation Act 2001, specified minimum shares of renewable energy consumption by designated consumers. This applies to electricity distribution licensees, open access consumers, and captive users, as a percentage of their total energy consumption. The notification also specifies that any shortfall in specified renewable energy consumption targets shall be treated as non-compliance and penalty shall be imposed as such rate specified under sub-section (3) of section 26 of the Energy Conservation Act, 2001.

iii. **Standard size components:** Some of the components imported due to non- availability of standard sizes, quality, and lack of consistent demand. With small modification in the existing manufacturing units, the industry can be catered through existing manufacturing units. A scheme for ramping up domestic manufacturing capacity for the components of desired sizes such as **forged** rings (for pitch bearings and slew/yaw bearings), **tower**

flanges (Special alloy steel/Continuous cast) with higher diameter, **main shaft**, **steel plates** can be manufactured domestically.

iv. A major cybersecurity threat remains with power Plant Controller (an intelligent cyber-physical device) which is being imported. A committee needs to be constituted with representatives from Industry, the Ministry of Power/Ministry of New and Renewable Energy, relevant institutions, and Academia to develop a roadmap for domestically **manufacturing Power Plant Controller and SCADA system**s.

v. **Enabling finance**: Crowd sourcing of fund at low cost-long tenor and also deploying innovative tools like Blended Finance, Green Bonds, etc. are needed to boost the manufacturing in the RE sector.

vi. GST is not levied on sale of electricity. Hence, the corporates and industrial customers, are unable to get a GST pass through. This is also one of the factor for discouraging investment in the renewables. Bringing renewable electricity under GST regime for commercial and industrial customers will accelerate adoption of renewables in C&I (commercial and industrial) segment.

Cyber Security Framework in India:

14. The Existing Cyber security framework for Wind energy and Power systems deployed in the wind sector is summarized below:

i. **Central Electricity Authority (Technical Standards for Communication System in Power System Operation) Regulations, 2020**: As per regulation 14 of aforesaid Regulations, all users and control centers connected to the communication system shall have robust programs in place to adequately and continuously manage cyber security risks that could have adversely impact power system communications infrastructure. Further said cyber security program shall address the following, namely: -

a) Compliance with provisions of the Information Technology Act, 2000 (21 of 2000) and National Cyber Security Policy, 2013 as amended from time to time;

b) Implementation of the National Critical Information Infrastructure Protection Centre (NCIIPC) Guidelines;

c) Implementation of guidelines and advisories issued by Computer Emergency Response Team (CERT India) and applicable Sectoral Computer Emergency Response Team (CERT); and

d) Compliance to the Central Electricity Authority (Cyber Security) Regulations, as and when they come into force.

ii. **Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations:** CEA (Cyber Security in Power Sector) Guidelines, 2021 under the provision of Regulation (10) of the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019 has been issued by CEA on 7th October 2021. It has 14 articles related to cyber security that need to be complied with

by Responsible Entity, including Generation utilities (Hydro, Thermal, Nuclear, and RE) and Generation Aggregators. The guidelines mainly cover following issues about the Cyber Security:

Cyber Security Policy, CISO appointment, CII identification, Electronic Security Perimeter, Cyber Security Requirement, Cyber Risk Assessment & Mitigation Plans, phasing out of Legacy System, Cyber Security training, Cyber Supply Chain risk management, Cyber Security Incident Report and Response Plan, C-CMP, Sabotage Reporting, Security and Testing of Cyber Assets and Cyber security Audit".

A brief about each of the 14 articles of the guidelines is highlighted at **Annexure- 1.**

iii**. Framework applicable for Wind turbine manufacturers:** Ministry of Power (MoP) has issued an order dated 02.07.2020 in which following directions were issued:

a) All equipment, components, and parts imported for use in the power Supply System and Network shall be tested in the country to check for any kind of embedded malware/trojans/cyber threat and for adherence to Indian Standards.
b) All such testing shall be done in certified laboratories that the MoP will designate.
c) Any import of equipment/components/parts from "prior reference" countries as specified or by persons owned by, controlled by, or subject to the jurisdiction or the directions of these "prior reference" countries will require prior permission of the Government of India.
d) Where the equipment/components/parts are imported from "prior reference" countries, with special permission, the protocol for testing in certified and designated laboratories shall be approved by the MoP.
e) MoP has issued order dated 24.12.2021 notifying the List of Designated laboratories for Cyber Security Conformance testing of imported equipment for which standards for communication protocols and security conformance and testing protocols to be followed by the buyers (like utilities) including import from prior reference countries.
f) So far there is **no testing capability to detect the embedded malware and hardware trojan at chip level at any of the testing facilities in the country on commercial level**. The malicious code in the application & OS can be detected through the testing facilities developed at (Standardization Testing and Quality Certification) STQC, if the supplier makes the source available.

iv. The Ministry of Power has created 6 (six) Sectoral Computer Emergency Response Team (CERTs) namely Thermal, Hydro, Transmission, Grid Operation, RE and Distribution for ensuring cyber security in Indian Power Sector. **SECI has been designated as CERT-RE.** Nodal officers of the sectoral CERTs co-ordinate with their respective constituent utilities for nomination of utility level CISO and alternate CISO, preparation and implementation of utility specific Cyber Crisis Management Plan (C-CMP) and for early identification of their Critical Information Infrastructures (CIIs). At bottom level, nominated CISOs of Power Utilities work in co-ordination of respective CERTs and are responsible for implementation of Cyber Security Activity in their organization. **The capacity of SECI needs to be strengthen to take up the role of CERT-RE being a critical sector.**

15. As per MOP dated 05th April, 2023, a Computer Security Incident Response Team (CSIRT)-Power i.e., CSIRT-Power, specifically for the power sector has been setup at Central Electricity Authority. **The CSIRT-Power is an extended arm to Indian Computer Emergency Response Team (CERT-In)** (**Annexure -2**). All the utilities in the Power Sector (Generating Companies, Load Dispatch Centers, Transmission Licensees, Distribution Licensees) reports to and comply with the instructions of CSIRT-Power along with CERT-In (CERT-In being the national Nodal Agency in the area of Cyber Security), while dealing with the activities pertaining to Cyber Security of Power Sector.

The key activities of CSIRT-Power are given below.

- Laying down the Cyber Security framework and protocol for the Power Sector;
- Laying down Standard Operating Procedures for Cyber Security;
- Reviewing the Cyber Security arrangements in the different wings from time to time and strengthening such arrangements;
- Implementation of Trusted Vendor System;
- Drafting of Model Contractual Clauses for Cyber Security;
- Analysis of Cyber Security Incidents;
- Cyber Security Testing;
- CISO Workshop;
- Analysis, follow-up & action on Alert and Advisories, issued by NCIIPC, CERT-In and MHA;
- Capacity development for using Vulnerabilities Scanning tools;
- Security Control Selection & Tailoring Process; and
- Vetting of Cyber Testbed Proposals

16. To implement cyber security best practices in the power sector, the Information Sharing and Analysis Centre (ISAC-Power) was established as a central coordinating agency for sharing and analyzing cyber security incidents across six sectoral CERTs. As a central information pooling and sharing platform, the ISAC-Power portal requires mandatory registration by wind sector developers to enable information sharing on cyber security issues.The cyber security program shall address the following, namely:

a) Compliance with provisions of the Information Technology Act, 2000 (21 of 2000) and National Cyber Security Policy, 2013 as amended from time to time;
b) Implementation of the National Critical Information Infrastructure Protection Centre (NCIIPC) Guidelines;
c) Implementation of guidelines and advisories issued by Computer Emergency Response Team (CERT India) and applicable Sectoral Computer Emergency Response Team (CERT); and
d) Compliance to the Central Electricity Authority (Cyber Security) Regulations, as and when they come into force.
e) Compliance to the Central Electricity Authority (Cyber Security in Power Sector) Guidelines, 2021.
f) Report to and comply with the instructions of CSIRT-Power, CEA along with CERT-In (CERT-In being the national Nodal Agency in the area of cyber security), while dealing with the activities pertaining to Cyber Security of Power Sector.

The Present Cybersecurity Testing Mechanisms

17. Ministry of Power (MoP) vide order no 9/16/2016 -Trans-Part (2) dated 18th November 2020 notified that the equipment/components/parts may be imported from "prior reference" countries, subject to the following conditions.

a) The imported equipment must be examined by CPRI or appropriate testing laboratory on arrival
b) The testing should also ensure that testing equipment do not have any adverse impact (both on account of cybersecurity as well as quality point of view) on transmission Grid.
c) The other shortcomings as mentioned below need to be resolved at the earliest including the infrastructure build up for testing

   i. STQC tests until EAL-4, which is insufficient to rule out any malicious content embedded in software/hardware.
   ii. DRDO and ISRO has their own testing mechanism like security loop analysis which is for their own security and do not have breadth for commercial testing of power sector equipment.
   iii. Some of the OEMs like Siemens and Hitachi have their own in-house testing facilities and have concerns of IP (Intellectual Property).
   iv. The present testing available at CPRI and other testing labs are not in a position to certify any security target as cyber secure.

i. Until the setting up of an adequate certification facility in India, a digitally signed self-declaration can be submitted by the OEM w.r.t. conformance to the IEC 62443-4 standards during design and manufacture of the equipment/system. **In this regard, MoP has issued directives and has proopsed to up a committee to finalize the format and criteria for accepting the self-certification submitted by OEM.**
ii. MoP dated 08.06.2021 notified Central Power Research Institute (CPRI) as the nodal agency for testing power system equipment for cyber security. This order indicates List of designated laboratories for cyber security conformance testing. For ensuring supply chain cybersecurity the essential cyber security tests needs to be carried out during Factory Acceptance Test (FAT) and Site Acceptance Test (SAT)
iii. To address the issue of cyber supply chain risk management, MoP has worked out a scheme of trusted vendor system for power sector and has initiated action on model contractual clauses to be incorporated in the bid for procurement of ICT based devices.
iv. While granting the connectivity to the RE plant CTU must ensure that necessary provision for adherence to the trusted vendor procedure by the RE utility requesting for the connectivity is included in the relevant agreement process. While allowing the first-time charging of the RE generator, compliance with the above procedure shall be submitted to the concerned LDC. Model Contractual clauses on cybersecurity to be mandatorily included in the bid documents.

The Way Forward

i. **Mandatory Certification of foreign Software/Hardware:** The Grid Controller of India Limited (POSOCO) must obtain all relevant certificates and IPRs, software and device/hardware from the OEMs of foreign origin especially from neighboring countries and send them for certification and approval by Central Electricity Authority of India (CEA), Ministry of Electronics and Information Technology (MeitY) and Standardization Testing and Quality Certification (STQC) as per applicable rules/guidelines. Clearances from the above three organizations or any other relevant organizations as deem fit, need to be made mandatory prior to permission of connectivity to the national or state grid as specified below:
   a) OEMs need to incorporate security related requirements for SDLC (Secure Development Life Cycle) in lines with ISO 27002:2022 controls i.e. (8.25 – 8.30), and as per clause mandated in the proposed MCC (Model Contractual Clauses) procurement requirements.
   b) National Institute of Wind Energy (NIWE) may be instructed to follow the exact protocol as mentioned above at the time of commissioning of wind sector projects.

ii. As per Revised List of Models & Manufacturers (RLMM) policy, OEMs in wind power sector need to get approval for their WTG as either Nacelle assembled or Nacelle manufactured in India (The Nacelle is the main housing of the turbine, which is assembled with the yaw drive, it is directly mounted on the tubular tower. The main carrier is a single cast frame that permits stable mechanical behavior and performance.). This must be modified so that RLMM approval is only given when major equipment like Nacelle (Gear Box, Generator etc.), Blades, Tower, Hub, Controller are manufactured in India.

iii. The guidelines need to include a minimum requirement of local content of 60% by value mandatorily sourced from India

iv. **The PPC (Power Plant Controller) software is of critical importance and associated with risks-** used in the device which connects the wind farm directly to the national/state grid. PPC OEMs of foreign origin especially neighboring countries, need to be examined and call needs to be taken for their suspension while not adhering to the above protocol. One of the mitigation measures for arresting this concern is the deployment of Layer 7 Firewall or NGFW (Next Generation Firewall) with DPI capability capable of understanding ICS protocols at the POI (Point of Interconnection) at utility end. The NGFW firewall must only allow traffic related to ICS communication protocol (say IEC 104 etc.) and block the rest of traffic flowing through the communication link to the designated control center wherefrom the control actions on the PPC are being performed.

   a) OEMs provide a means to disable the "Server's" "WRITE CAPABILITIES", and putting in to a "READ-ONLY" mode across all its various protocol-based implementations (Like SOAP/ HTTP, OPC-XML DA implementations etc.).
   b) For all the implementations of Wind Power Plants where the SCADA cum PPC is hosted off-site and away from the actual wind farm site, the software operators must only be granted "READ ONLY" rights so that they must not be able to control the plant operations remotely

c) The SBOM (Software Bill of Materials) must be part of essential requirement for procurement of SCADA/PPC software to contain the cyber supply chain risks.
d) Further, following controls & practices must be implemented
   i. Blocking IPs by Implementing the Geo Fencing service at the perimeter firewall.
   ii. Mandating the MFA (Multi Factor Authentication) for any remote VPN connectivity request.
   iii. Segregating the IT/OT network.
   iv. Allowing Only whitelisted devices/IPs through such firewalls.
   v. Implementation of IDS/IPS solutions
   vi. Implementing Principle of Lest Privilege and Least Access.

v. **The equipment supplier and the developer of the wind power plant needs to provide an undertaking** with enough backup information to the Grid Controller of India (POSOCO), ensuring that there is no access or control of any device, software, IPR or data of any wind turbine from outside of India under any circumstances and all data should be positioned strictly to the servers located in India. Both parties i.e., the equipment supplier and the developer of the wind power plant must establish their server, data center, R&D center, design center etc. inside the country. Any company violating these norms must be penalized and debar from all the business & engagement in the country. A timeline must be set for those company, which has already established its data center & server outside country for shifting data server to India.

vi. **Mandatory Cyber Security audits for wind farms at regular intervals:** There should be firewalls in each windfarm for accessing control and all the turbine components which communicate through IP (like PLC/Switch/Convertor, Pitch control) and have access control through VPN. Further, Cyber Security audits for wind farms should be a regular exercise.

vii. **Institutionalization of AI/ML based threat detection systems:** AI/ML based threat detection, end point detection & response tools, and vulnerability management modules to build a cyber-resilient environment may be explored.

viii. As per Article 14, CEA (Cyber Security guidelines for Power Sector), 2021, IT audit has been mandated half yearly basis while OT audit is mandated annually through a Cert-In empaneled auditors with costs of such audits to be borne by the respective organization. **The Ministry of New and Renewable Energy also needs to enforce these guidelines for third-party audit for Power System infrastructure cyber security** (Solar & Wind farm – grid interactive inverters, OEMs software, data center, communication devices, etc.) in consultation with Ministry of Power. The accreditation body for ISO 27001 Certifications must be an INDIAN agency in view of the critical systems being audited.

ix. **MNRE/Ministry of Power needs to create a separate budgetary provision for building infrastructure to address cyber-Security threats**. Every Utility must appoint CISO (chief information security officer) who should reside in India and report for compliance to the proposed independent agency on the Power Sector Cyber Security aspects.

x**. Wind power generation assets need to be classified as critical energy infrastructure** that are required to be built, operated and maintained by experienced, reputable companies on a

trusted technology track record, with accountable information technology systems, international standards and procedures.

xi. **Wind turbine type certification is to be conducted by a Renewable Energy Certification Body (RECB)** via the IECRE (IECRE is a Conformity Assessment System based on International Standards prepared by the IEC (International Electrotechnical Commission) for equipment and services used in renewable energy (RE) applications. The system aims to facilitate the international trade of equipment and services in the marine, solar photovoltaic (PV) and wind energy sectors, while maintaining the required level of safety. In addition to IECRE scheme, the IS/IEC 61400-22 scheme published by Bureau of Indian Standards (BIS) may also be referred and allowed for wind turbine type certification. Also, a 3rd party certificate of compliance is required to ensure electromagnetic compatibility of the asset's equipment and systems, so that they do not introduce intolerable electromagnetic disturbance.

xii. **Promote cyber security research and development:** Due to ever evolving threats, cyber security research and development need to be highly important to progress towards the long-term vision for cyber-resilient wind energy systems. The research areas can be identified in consultation with MEiTY.

xiii. **Adoption of best practices** to promote basic cyber hygiene which includes training personnel in cyber security, creating cyber asset lists, Onboarding Public IPs assigned to the organization with the CSK, implementing various requirements as stated in the CEA (Cyber Security in Power Sector) Guidelines, 2021 and developing better means of communicating cyber threat and vulnerability information. A cell needs to be created and to be made responsible for such activity.

xiv. **The RE critical equipment /software suppliers must declare and provide self-certification,** not limited to the following:

a) Malware detection techniques used before final packaging and delivery (e.g., scanning finished products for malware.
b) Practices to manufacture, deliver and service products without counterfeit components.
c) Secure transmission and handling controls to lower risk of tampering
d) Secure coding practices used to avoid common errors leading to vulnerabilities (e.g., input validation, compiler flags)

xv. **Reference architecture for RE sector**: The reference architecture for renewable energy sector needs to be finalized. Currently draft architecture by MoP is enclosed as per **Annexure-A**, that needs to be finalized in consultation with MNRE.

xvi. A**ll the OEMs of the Wind Sector needs to locate and re-locate their Data Centre and Research & Development Centre inside the country** failing which OEMs should be de-bar from participating in the tenders and supplying the items in the Country. Ministry of New and Renewable Energy should prepare timelines for relocation of the Wind Sector OEMs Data, R&D Centre inside the country.

Annexure-A

The Architecture for solar and wind plants are generally divided in three areas as follows;

1. Solar PV Generator/ Wind Generator
2. Inverter
3. AC Switchyard (SAS)

All the above-mentioned areas report to centralized SCADA system for Control and monitoring of the respective Solar Park/ Wind Park

Solar PV Generator: Solar PV generator area comprises of number of PV panels spread over the wide area of land. PV panels are connected (series/ parallel configuration) to make string. SCADA system monitors the string of the park. In case rotating mounting module structures are used, the PLC related to MMS (Module Mounted Structure) is to be monitored through the centralized SCADA system.

Wind Generator: It comprises of group of wind turbines in the same location. Wind farms vary in size from a small number of turbines to several hundred wind turbines covering an extensive area. Various parameters, variables as mentioned below are monitored to review the healthiness and performance of the Turbine on the centralized SCADA system.

i. Environmental parameters - Wind Speed, Wind Direction, Ambient & Nacelle Temperatures etc.
ii. Electrical characteristics - Active & Reactive Power Output, Generator Voltages Current, Frequency etc.
iii. Temperatures of various parts of turbine - Gearbox Bearing & Lubricant oil, Main Bearing, Rotor Shaft, Generator Shaft, Generator Slip Ring, Inverter Phase, Transformer Phase etc.
iv. Control variables - Pitch angle, Yaw Angle, Rotor Shaft Speed, Generator Speed, Fan Speed / Status, Number of Yaw Movements, Set Pitch Angle / Deviation, Number of Starts / Stops etc.

Inverter: A solar inverter or PV inverter, is a type of power inverter which converts the variable direct current (DC) output of a photovoltaic (PV) solar panel into a utility frequency alternating current (AC) that can be fed into a commercial electrical grid or used by a local, off-grid electrical network.

SAS System: The typical SAS architecture shall be structured in three levels, i.e. Field level, Bay level and Station level. The SAS provides an extensive range of Supervisory Control and Data Acquisition (SCADA) functions.
Field Level, is at the switchyard level where instrument transformers, switchgear, transformers/reactor are located and are hard wired to bay level equipment like IEDs (Intelligent Electronic Device), BCU (Bay Control Unit) etc.

A bay comprises of one circuit breaker and associated disconnectors, earth switches and instrument transformers. At Bay Level, the IEDs/BCUs provide all bay level functions regarding control (command outputs), monitoring (status indications, measured values) and protection. The bay level intelligent electronic devices (IED) for protection and control shall provide the direct connection to the switchgear without the need of interposing components and perform control, protection, and monitoring functions.

Each bay control IED is independent of the others and its functioning is not affected by any fault occurring in any of the other bay control units of the station.

The data exchange between the electronic devices on bay and station level is realized through optical fiber cables in dual redundant ring mode on IEC 61850 Protocol.

At Station Level, redundant server PC enables station control through the SCADA package. The station level contains the station-oriented functions e.g., alarm list or event list related to the entire substation, gateway for the communication with remote control centers or respective load dispatch center.

At station level there is also Power Plant Controller (PPC servers) used to regulate and control the networked inverters, devices and equipment at a solar PV plant in order to meet specified set points and change grid parameters at the Point of Interconnect (POI). This enables fast and stable control at the grid connection point.

Ethernet switches are provided for connecting the IEDs in the bay level catering the requirements. The connection from each IED to the switch is by a single fiber optic link. The switches are connected in a ring. At the station level, to provide communication redundancy, two Ethernet switches are used to connect the redundant servers, Gateways, DR/EWS and other station level equipment.

The alarms and events when required, reports and graphics will be printed on laser printer connected to the system over the Ethernet LAN.

A dedicated GPS master clock is provided for the synchronization of the entire system. This master clock is independent of the station computers and gateways, and it synchronizes all devices via the-inter bay bus using SNTP protocol as defined by the IEC 61850 standards.

Weather Monitoring Station (WMS): Weather Monitoring Station is one of the most crucial instruments installed in Solar PV / Wind Power plants. A weather monitoring station can be immensely helpful in monitoring the efficiency and performance of any solar/ wind power plant.

Photovoltaic (PV) system performance depends on both the quality of the system and the weather. As the weather varies, the output of the PV system changes. The key factor affecting the PV system performance is the solar radiation data. But along with solar radiation data, the weather parameters like ambient temperature, relative humidity, wind speed, wind direction, atmospheric pressure, and rain are the other important factors affecting the performance. The

data of all these sensors can be used to schedule the maintenance of the plant and to calculate if the PV system is generating electricity as per the expectations.

The effective operation of the wind turbine is also dependent on the direction of the wind. Speed air density, which in turn depends on the temperature and humidity. Thus, the speed of the wind worked effectively in its composition must include the weather. Weather monitoring station helps and prevents the healthiness of wind turbines. In case of increase in wind speed above the maximum design value, WMS sends a signal to the lock assembly of the wind turbine and stops the operation of the wind turbine in order to prevent any damage to the wind turbine due to climatic change.

Power Plant Controller (PPC): The Power Plant Controller in a Wind Power Plant (WPP) is an intelligent system for dynamic wind power plant control and grid code compliance in order to

- Meet specified setpoints and change grid parameters at the point of interconnect (POI) by regulating voltage, frequency, reactive power, active power, power factor and ramp control.

- Control plant behavior in terms of grid stability, compliance, production levels and revenue.

- Perform remote starts/stops or other troubleshooting actions on WTGs and other field and substation equipment

Communication Protocol: For monitoring of RE plant data to load dispatch center, the communication channel is realized through /OPGW (Optic Fibre Ground Wire) /PLCC (Power Line Carrier Communication) in Secure IEC 60870-5-101/104 protocol. It may be noted that communication channel using GPRS/GSM is not found reliable and suitable by many SLDCs. Moreover, said data channel is also prone to cyber-attacks, hence communication channel using GPRS/GSM should not be permitted due to cyber security reasons.

A dedicated REMC (Renewable Energy Management Center) server is installed at LDC fetching the data of RE generators and forwards the same to SCADA system of LDC. At present, there are 13 (thirteen) REMCs and some REMCs are co-located with SLDCs, while remaining are co-located with RLDCs with NLDC at the top of hierarchy.

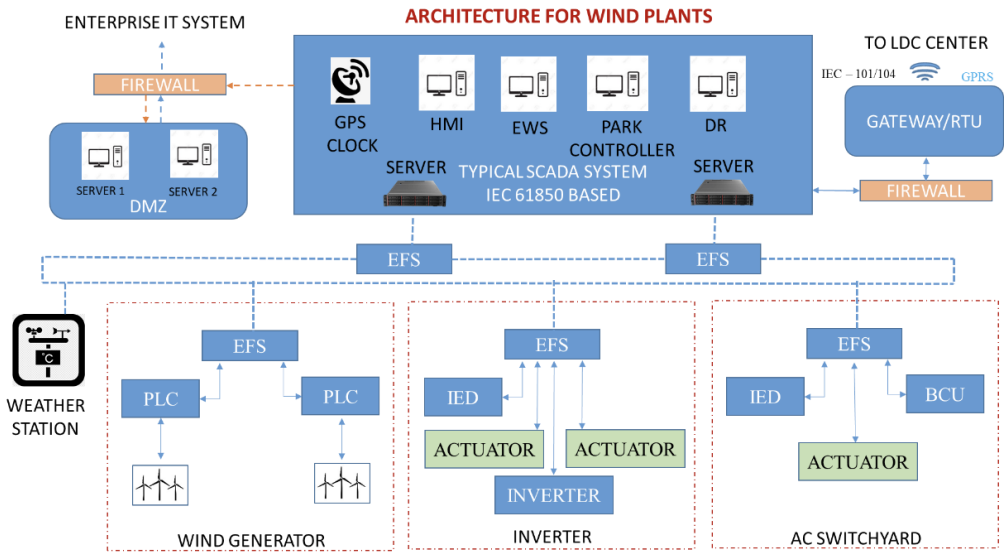
REMC systems are specialized SCADA systems deployed to cater exclusively to the requirements of the integration and operation of Renewable Energy (RE) sources, which include real time data acquisition, scheduling and forecasting of RE generation sources. The REMCs are equipped with a Forecasting tool and provides generation forecasts for Solar and Wind power generators and facilitates their scheduling and integration into the power grid. It helps balance the intermittent nature of renewable energy generation with the demand for electricity. The REMC collects, analyzes and manages data related to renewable energy generation, consumption, and grid integration. It maintains necessary systems to ensure accurate and up-to-date information on renewable energy resources and their utilization.

Data Communication is one way only for LDC, i.e., from RE station to LDC. The data connectivity is through redundant gateway / RTU and dedicated firewall in high availability mode. The gateway / RTU fetch data from SCADA LAN through firewall and provides the required data to LDC on IEC 60870-5-101/104 protocol.

Interconnection with Enterprise IT System (Centralized Data collection center of Wind Developer Company for data acquisition is an online (continuous), unit-directional communication of generation data and this link is protected by using firewall and IPS at Process Control Network end. The Enterprises IT system may be co-located or remotely located. Only the services required for this communication are permitted in the firewall and others are blocked. This connectivity provides data to the Central database for MIS purposes only with one-way data flow i.e., from plants to MIS server (unidirectional) and no traffic is allowed in to plant network.

For updations of system patches/software upgrades and antivirus definition etc. the patches shall be downloaded in the Patch Management Servers located in the enterprise IT system and then forwarded to respective servers located in the External DMZ. The forwarding of patches to the servers in OT environment shall be scanned through firewall, IP/Port filters and access rules governing such data exchange between the servers in two networks.

Architecture layouts for RE plants (with ON-Premise SCADA) are as under:



Annexure -1

Brief about each Article of CEA (Cyber Security in Power Sector) Guidelines, 2021

Article1: Cyber Security Policy.

What: The article states that an organization shall document, establish, approve by top management, publish, communicate to relevant stakeholders the Organization Cyber Security Policy. The organization shall also review the same at planned intervals and after occurrence of significant changes.

Purpose of Article: The establishment of Organization wide Information Security Policy basically sets out the organization's approach to managing its information security of its OT /IT assets and helps it in ensuring effectiveness of management direction/security controls/business continuity plans in accordance with business, legal, statutory, regulatory and contractual requirements.

Major Requirements of Article1

i. There must be hard isolation between OT Systems from any internet facing IT Systems.
ii. The communication to OT environment must be through a firewall allowing only the approved list of whitelisted IP / Port addresses.
iii. Formulation of topic specific policies for ensuring access control to Cyber Assets owned or controlled by the utility.
iv. Sourcing of all ICT based equipment/systems deployed in infrastructure/system mandatorily CII from the list of "Trusted Sources".
v. The utility shall be ISO/IEC 27001 certified (including sector specific controls as per ISO/IEC 27019).
vi. Communication between OT equipment / systems must be realized through secure communication channel preferably of PowerTel through Optic Fibre Cable.
vii. Ensuring to take up the cyber security issues as agenda items in utility's Board Meetings once in every quarter.

Article2: Appointment of Chief Information Security Officer (CISO).

What: The article states that a utility shall mandatory appoint a responsible authority, namely a CISO and an Alternate CISO. The roles and responsibilities of the CISOs shall be to ensure the cyber security of the Cyber Assets of the utility.

Purpose of Article: CISO's appointment is required to steer the implementation of Cyber Security Policy as well as to lead the Information Security Division, a division which need to execute various cyber security activities required for protecting Cyber Assets of the Utility.

Major Requirements of Article2

i. Mandatory appointment of a CISO (Chief Information Security Officer) and an Alternate CISO.
ii. Conformance to the qualification standards of CISO, if any, laid by the Quality Council of India (QCI).

iii. Acquisition of minimum required cyber security skill sets by the Alternate CISO within six months from the date of his appointment.
iv. Regular updating of the details of the CISO and Alternate CISO by the Utility with the Sectoral CERTs as well as on the ISAC Portal.
v. CISOs to comply with the roles and responsibilities laid by the CERT-In with focus to ensure the cyber security of the Cyber Assets of the Utility.

Article3: Identification of Critical Information Infrastructure (CII).

What: The article states that a utility shall mandatorily identify its Critical Information Infrastructure by submitting the details of its Cyber Assets employed in its Critical System to NCIIPC within 30(thirty) days from the date of their commissioning in the Critical System.

Purpose of Article: To protect and safeguard the Critical Assets which are within the purview of the utility and are such facilities, systems and equipment which, if destroyed, degraded or otherwise declared unavailable, would affect the reliability or operability of the Power Supply System. CII protection helps in avoiding any debilitating impact on National Security, Economy, Public Health or Safety.

Major Requirements of Article3

i. Mandatory identification of CII by submitting to the NCIIPC through the Sectoral CERT, the details of those Cyber Assets which are employed in its Critical Systems such that the Cyber Asset uses a routable protocol to communicate both outside the Electronic Security Perimeter or within control centre and also when such Cyber asset is dial up accessible.
ii. The utility shall submit the details of Critical Business Processes and underlying information infrastructure along with the corresponding impact and Risk Profile to NCIIPC.
iii. The utility shall review their declared/notified CIIs at least once a year to examine changes if any in the functional dependencies, protocols and technologies or upon any change in security architecture.
iv. The utility shall review their declared/notified CIIs once in every 6 months, in case if NCIIPC has directed them to constitute an Information Security Steering Committee

Article 4: Electronic Security Perimeter (ESP).

What: The article states that a utility shall identify and document the ESP(s) and all Access Points to such perimeter(s) and shall also ensure that every Critical System resides within an ESP.

Purpose of Article: To protect the Critical Asset from possible Cyber Attacks by dividing & segregating the network into logical domains/zones, also known as ESPs. The inter ESP access, if allowed, must be through perimeter security devices.

Major Requirements of Article 4

i. The utility shall perform a cyber-Vulnerability Assessment of each electronic Access Points to the Electronic Security Perimeter(s) at least once in every 6 (six) months and/or after any change in Security Architecture.

ii. The utility shall ensure that all critical, high and medium vulnerabilities identified as a result of cyber–Vulnerability Assessment shall be closed and verified for the effective closure.
iii. The Responsible Entity shall follow procedure of identifying "Electronic Security Perimeter" in case of distributed and/or hybrid information infrastructure, as per IEC 62443 / IS16335 (as amended from time to time).

Article 5: Cyber Security Requirements.

What: The article states that a utility shall form an Information Security Division (ISD) to be headed by the CISO of the utility. The article also states the functions of the ISD as well as other cyber security requirements for ensuring the cyber security of Critical Systems.

Purpose of Article: Articulation of various cyber security requirements for ensuring the security of Critical Systems by way of mandatory formation of an ISD, stating various functions of ISD, suggestions for designing a secure network architecture of the OT/IT systems etc.

Major Requirements of Article 5

i. Onboarding of Public IPs of utility with the Cyber Swachhta Kendra (CSK) of Cert-In.
ii. Deployment of Intrusion Detection System and Intrusion Prevention System for detection of behavioral anomaly in both IT &OT systems.
iii. Updating of firmware/software with digitally signed OEM validated patches.
iv. Maintenance logs of firewalls for a period of six months.
v. Enabling only those ports and services that are required for normal operation.
vi. Designing of a secure architecture for control system as per IEC 62351-10
vii. Retaining Cyber logs and cyber forensics records of an incident for at least 90 days.
viii. Timely acting upon the advisories, guidelines and directives of NCIIPC, CSK, Cert-In and Sectoral CERTs.
ix. Retaining document of FAT, SAT test results and report/ certificate of cyber tests carried out for compliance of Government Orders and Cyber Security Audit.

Article 6: Cyber Risk Assessment and Mitigation Plan (CRMP).

What: The article states that a utility shall conduct a Cyber Risk Assessment & Mitigation plan for identification & mitigation of the threats to and vulnerabilities in the Critical Systems by considering the likelihood and adverse impact of unauthorized access/breach of Critical Systems.

Purpose of Article: To contribute in providing assurance about privacy, security of Critical Systems through appropriately selected security controls & risk mitigation measures in place.

Major Requirements of Article 6

i. The Cyber Risk Assessment and Mitigation Plan shall be approved by the BOD of the utility.
ii. The CRMP shall assess the cyber risks of both IT and OT environment and risk acceptance criteria.
iii. The utility shall review the CRMP at least once in a quarter.

Article 7: Phasing out of legacy System.

What: The article states that utility shall draw a replacement plan for phasing out of those identified legacy Communicable Equipment/ Systems which are nearing end of life or are left without support from the OEM. The article also mandates developing a procedure for safe and secure disposal of such outlived or legacy systems/devices.

Purpose of Article: To address the cyber security concerns associated with legacy systems in use through development of procedures for hardening of such assets by integrating additional controls in consultation with OEMs or alternate suppliers as well as through establishing SOPs for their safe & secure disposal in phased manner.

Major Requirements of Article 7

i. The Utility shall ensure that the Information Security Division shall draw the list of all communicable equipments/systems nearing end life or are left without support from OEM. Thereafter CISO shall identify equipment/systems to be phased out from the list drawn, firm up their replacement plan and put up the replacement plan for approval before the Board of Directors.

ii. The CISO shall ensure that till equipments /systems nearing end life or left without support from OEM are not replaced, their cyber security is hardened and ensured through additional controls provisioned in consultation with the OEM or alternate Supplier(s)*.

iii. The Utility shall document in their Cyber Security Policy a Standard Operating Procedure for safe and secure disposal of outlived or legacy devices.

Article 8: Cyber Security Training.

What: The article states that utility shall document, establish, maintain and review an annual cyber security training program for its personnel authorized to work with critical systems. The article also states that all personnel engaged in O&M of IT & OT Systems shall mandatorily undergo courses on cyber security of Power Sector.

Purpose of Article: To train and make aware the authorized personnel about relevant cyber security topics and also to ensure that personnel fulfill their cyber security responsibilities.

Major Requirements of Article 8

i. The Utility shall review annually their cyber security training program and shall update it whenever necessary. Annual Review shall record evaluation of the effectiveness of the trainings held.

ii. All Personnel engaged in O&M of IT & OT Systems shall mandatorily undergo courses on cyber security of Power Sector from any of the training institute designated by CEA, immediately within 90 days from the notification of CEA Guidelines on Cyber Security in Power Sector.

iii. The Utility shall ensure that none of their newly hired or the current Personnel have access to the Critical System, prior to the satisfactory completion of cyber security training programme from the Training Institutes designated in India, except in specified circumstances such as cyber crisis or an emergency.

Article 9: Cyber Supply Chain Risk Management.

What: The article states various provisions for addressing the concerns related to Cyber Supply Chain Risk Management i.e., Provision for inclusion of MCC in every bid document for procurement, mandating such procurement from "Trusted Sources", getting such procured product tested, from designated labs in India for the embedded Malware/Trojan/Cyber Threats and adherence to Indian Standards.

Purpose of Article: The article tries to ensure the cyber security requirements for Secure product development processes as well as Secure Supply Chain management practices for avoiding the deployment of counterfeit and maliciously tainted products in the Power Supply System through various checks at different phases of product procurement and commissioning.

Major Requirements of Article 9

i. The Utility shall ensure that, as and when Ministry of Power, Government of India notifies the Model Contractual Clauses on cyber security, these clauses are included in their every Bid invited for procurement of any ICT based components/equipment's/System to be used for Power System.

ii. The Utility shall ensure that all the Communicable Intelligent Equipment's and the Service Level Agreements (SLAs) for their Critical Systems shall be sourced from the list of the "Trusted Sources" as and when drawn by MoP/CEA.

iii. The Utility shall ensure that, in case, for the any Communicable Intelligent Devices, if no Trusted Source has been identified, then the successful bidder in compliance with the provisions made in MoP order dated 2.7.2020 and any other relevant MoP order has got the product cyber tested for any kind of embedded malware/Trojan/cyber threat and for adherence to Indian Standards at the designated lab.

iv. The Utility shall ensure that the essential cyber security tests are carried out successfully during FAT, SAT as detailed in Annexure A. The equipment/System besides for functionality shall also be tested in the factory for vulnerabilities, design flaws, parts being counterfeit or tainted, so as to minimize problems during on-sitetesting and installation. Cyber Security Conformance Testing are to be carried out in the designated Lab as listed in Annexure-I of MoP Order No. 12/13/2020-T&R dt. 8th June, 2021(Order at Annexure-B).

v. The Utility shall ensure that the Equipment/System supplied by the successful bidder shall accompany with a certificate$, obtained by OEM from a certification body accredited to assess devices and process for conformances to IEC 62443-4 standards during design and manufacture. The Utility shall accept the certificate submitted along with the supplied Equipment/System only if it's in line with the Testing Protocol as notified by Ministry of Power, Government of India, from time to time.

vi. The Utility shall dispose all unserviceable or obsolete Communicable Intelligent Devices as per the procedure laid in their Cyber Risk Assessment and Mitigation Plans which shall be in line with the prevailing best practices.

Article 10: Cyber Security Incident Report and Response Plan.

What: The article articulates the requirements of establishing a Cyber Security Incident Response Plan by covering its various aspects including identification of various criteria(s) based on their impact analysis for declaring the occurrence of such cyber incident(s) as Cyber Crisis, designating an authority to declare an incident as cyber crisis, ways of handing of an incident, reporting the same in prescribed formats to regulatory authorities like Cert-In/NCIIPC etc.

Purpose of Article: To guide the utilities in preventing, detecting, responding a cyber incident in a structured & matured way with least impact on their critical business functions.

Major Requirements of Article 10

i. Root cause analysis for all reportable events shall be carried out and corrective action taken, so as to ensure that any re-occurrence of such event can be managed with ease.

ii. The CISO shall ensure that during any Cyber Security Incident, ISD monitors and minutely records every detail of cyber security events and incidents in both IT as well as the OT System owned or controlled by the Utility.

iii. The Utility shall ensure that the efficacy of the Cyber Security Incident Response Plan is tested annually through mock drill(s) carried out, if feasible, as simulation exercise(s) or as table top exercise(s) with wider participation of their employees, in consultation with CERT-In and sectoral CERT. In case if any shortcoming is observed in the Cyber Security Incident Response Plan suitable changes shall be made in it.

Article 11: Cyber Crisis Management Plan (C-CMP).

What: The article mandates a utility to prepare a Cyber Crisis Management Plan and states the process for its implementation, management including enforcement and review.

Purpose of Article: To guide the utilities in defining roles & responsibilities for a coordinated, approach to prepare for rapid identification, information exchange, response, and remediation to mitigate and recover from malicious cyber related incidents impacting their critical business functions and processes.

Major Requirements of Article 11

i. The Utility shall prepare a Cyber Crisis Management Plan and submit to their sectoral-CERT for review with intimation to Ministry of Power/CISO-MoP. Utility shall update their C-CMP on the basis of comments made by sectoral-CERT and then submit for vetting to CERT-In. The C-CMP shall be updated once again to include the observations made by CERT-In before seeking approval of Board of Directors for implementation of C-CMP.

ii. The Utility shall ensure that the C-CMP is reviewed at least annually. The CISO shall ensure that all changes are made in C-CMP only with the due approval of Board of Directors and the changes made in C-CMP have been communicated through a verifiable means to all the concerned Personnel of the Utility.

iii. The CISO shall be accountable for ensuring enforcement of C-CMP by Information Security Division of the Utility, during a cyber-crisis, as and when declared by the designated Officer.

Article 12: Sabotage Reporting.

What: The article states the requirements for a utility to prepare a procedure for identification and reporting of sabotage on their Critical Systems. It also states the action to be taken in the event of occurrence of any sabotage.

Purpose of Article: To protect the CIIs from any disturbances or unusual occurrences identified, suspected or determined to be caused by a sabotage.

Major Requirements of Article 12

i. The CISO shall be held liable for non-reporting of identified sabotage(s) as per procedure laid for identifying and reporting of sabotage in the Cyber Security Policy of the Utility.

ii. The CISO shall submit to NCIIPC within 24 hours of occurrence the report on every sabotage classified as cyber incidents(s) on "Protected System".

iii. The CISO upon occurrence on every sabotage shall take custody of all log records as well as digital forensic records of affected Cyber Assets, Intrusion Detection System, Intrusion Protection System, SIEM and shall preserve them for at least 90 days and shall make them available as and when called upon for investigation by the concerned Agencies.

Article 13: Security and Testing of Cyber Assets.

What: The article states that the utility shall obtain the information about technical vulnerabilities of its in-service phase as well as standby Cyber Assets, evaluate the utility's exposure to such vulnerabilities, and take appropriate actions like regular firmware/Software updates and patching, Vulnerability Management, Penetration Testing etc.
The article also states that all Communicable Devices are to be tested for Communication Protocol conformance before being deployed in Power Supply System.

Purpose of Article: To prevent exploitation of technical vulnerabilities of Cyber Assets.

Major Requirements of Article 13

i. The Utility shall carry out regularly Vulnerability Assessment of all Cyber Assets owned or under their control. If a Cyber Asset is found vulnerable to any exploits or upon any patch updates or major configuration changes, then further Penetration Testing may be carried out offline or in a suitably configured laboratory test-bed to determine other vulnerabilities that may have not been identified so far.

ii. The Utility shall ensure that all Communicable devices are tested for communication protocol as per the ISO/IEC/IS standards listed in MoP Order No. 12/13/2020-T&R dated 8th June, 2021.

iii. The Utility shall ensure that all Critical Systems designed with Open-Source Software are adequately cyber secured.

iv. The Utility as a best practice upon any incidence of Cyber Security Breach shall carry out cyber security tests at any lab designated for cyber testing by Ministry of Power. These tests shall be similar to Pre-Commissioning Security Test and those essential for carrying out Post Incident Forensics Analysis.

Article 14: Cyber Security Audit.

What: The article states that the utility shall implement the Information Security Management System (ISMS) covering all its Critical Systems. Moreover, the utility shall also get their IT as well as OT systems audited as per ISO/IEC 27001 along with sector specific standard ISO/IEC 27019, IS 16335 standards and other guidelines.

Purpose of Article: To identify, improve, assure a utility about cyber security preparedness of its Critical Systems through application of adequate controls of ISO/IEC 27001 standard.

Major Requirements of Article 14

i. The Utility shall implement Information Security Management System (ISMS) covering all its Critical Systems.
ii. The Utility shall through a CERT-In Empaneled Cyber Security OT Auditor shall get their IT System audit at least once in every 6(months) while OT System audited within every 12 (twelve) months and shall close all critical and high vulnerabilities within a period of one month and medium as well as low non-conformity before the next audit. Effective closure of all non-conformities shall be verified during the next audit.
iii. The Utility shall ensure that CISO has all the required systems and documents in place, as mandated by NSCS for base line cyber security audit.

Annexure -2

F.No. 1/32/2021/IT&CS (258359)
Government of India
Ministry of Power
IT & Cyber Security Division

Shram Shakti Bhavan, Rafi Marg, New Delhi

Dated: 05th April, 2023

Office Order

With the approval of the competent authority, **Computer Security Incident Response Team (CSIRT)-Power** i.e. **CSIRT-Power**, specifically for the power sector **has been setup at Central Electricity Authority, which will function as an extended arm to Indian Computer Emergency Response Team (CERT-In)**, which was established in 2004, as a functional organization of the Ministry of Electronics and Information Technology (MeitY), Government of India (GoI), for the effective implementation of cyber security measures, in all power utilities, under Section 70 B of the Information Technology (Amendment) Act-2008 (IT Act). The CSIRT-Power would help the utilities in cyber incident handling and to ensure better cyber security preparedness in the power sector.

2. As per the Guidelines of CERT-In, CSIRT- Computer Security Incident Response Team (CSIRT) is a Team that performs, coordinates and responds to security incidents that occur within a defined sector.

3. The envisaged key activities of CSIRT-Power are given below:

i. Laying down the Cyber Security framework and protocol for the Power Sector;
ii. Laying down Standard Operating Procedures for Cyber Security;
iii. Reviewing the Cyber Security arrangements in the different wings from time to time and strengthening such arrangements;
iv. Implementation of Trusted Vendor System;
v. Drafting of Model Contractual Clauses for Cyber Security;
vi. Analysis of Cyber Security Incidents;
vii. Cyber Security Testing;
viii. CISO Workshop;
ix. Analysis, follow-up & action on Alert and Advisories, issued by NCIIPC, CERT-In and MHA;
x. Capacity development for using Vulnerabilities Scanning tools;
xi. Security Control Selection & Tailoring Process; and
xii. Vetting of Cyber Testbed Proposals.

4. All the utilities in the Power Sector (Generating Companies, Load Despatch Centres, Transmission Licencees, Distribution Licencees) shall hereby report to and comply with the instructions of CSIRT-Power alongwith CERT-In (*CERT-In being the national Nodal Agency in the area of Cyber Security*), while dealing with the activities pertaining to Cyber Security of Power Sector.

5. CISO-MoP, shall be the Nodal Officer for co-ordination of activities for CSIRT-Power.

6. An Empowered Committee, constituted by the Ministry of Power under the Chairmanship of Secretary (P), vide OM No.1/9/2021-IT.I dated 16/03/2021, shall also act as an Advisory Committee to CSIRT-Power.

7. The CSIRT-Power will function through a Team of Officers, consisting of full time dedicated Officers of CEA, personnel having necessary experience and detailed for 2 to 3 years from respective CPSEs under the control of Ministry of Power and domain sector experts engaged on a fixed term contract basis. Detailed instructions in this regard shall be issued by Chairperson, CEA.

8. This issues with the approval of Hon'ble Minister of Power and New & Renewable Energy.

(Benjamin Karunakaran)
Deputy Secretary to Government of India
Tel.No.2371394

Distribution to:-

1. Secretary, Ministry of Electronics and Information Technology (MeitY).
2. Chairperson, Central Electricity Authority (CEA).
3. CISO-MoP, [Kind Attention: Member, Hydro], CEA.
4. Chairman, Department of Atomic Energy (DAE).
5. Cyber Security Coordinator, National Security Council Secretariat (NSCS).
6. All CMDs of CPSUs under MoP.
7. MD, Solar Energy Corporation of India Ltd. (SECI).
8. DG, Indian Computer Emergency Response Team (CERT-In).
9. DG, National Critical Information Infrastructure Protection Centre (NCIIPC).
10. DG, Central Power Research Institute (CPRI)/ National Power Training Institute (NPTI)/ Bureau of Energy Efficiency (BEE).

11. Chairman, Bhakra Beas Management Board (BBMB)/ Damodar Valley Corporation (DVC).
12. Registrar, Appellate Tribunal for Electricity (APTEL).
13. Secretary, Central Electricity Regulatory Commission (CERC)- For circulation to all the State Electricity Regulation Commissions.
14. Sectoral Computer Emergency Response Teams (Sectoral CERTs).

Copy for information to:-

1. Additional Chief Secretary/Principal Secretaries (Energy)/ Secretary(Energy)- All States/UTs for Information.
2. All IPPs, Transmission Licensees, Distribution Licensees-CISO-MoP and respective Sectoral CERTs may ensure the circulation of the order.
3. JS (PS)/JS(MA)/EA/CE(HP)/CE(NS).
4. PS to Secretary, Power.
5. PSO to SS&FA.
6. Sr.PPS to AS(IT&CS).
7. PA to DS (IT&CS).

File No. P-11071/17/2022-RE(P&E) (Computer No. 40084)

338279/2022/ENERGY

अजीत डोभाल, कीर्ति चक्र
राष्ट्रीय सुरक्षा सलाहकार
Ajit Doval, KC
National Security Adviser
Tel : 23019227

सत्यमेव जयते

CONFIDENTIAL
प्रधान मंत्री कार्यालय
नई दिल्ली-110 011
PRIME MINISTER'S OFFICE
NEW DELHI - 110 011

D.O. No. SS34870/NSA/22

August 20, 2022

Dear Shri Bery,

Please find enclosed herewith a copy of the letter dated 29th June 2022 received from the CEO & President-Asia-Pacific, Vestas Wind Systems A/S, Shri Purvin Patel.

2. The letter raises specific concerns about the increasing inroads being made by Chinese wind turbine Original Equipment Manufacturers (OEMs) in the country. Economic security concerns emerge from the fact that the Chinese OEMs have been importing components instead of undertaking local manufacturing. Further, given the China-based data collection servers and R&D operations of these Chinese OEMs, serious security concerns in terms of vulnerability of data and network operations also emerge. A brief note on the above concerns of the Chinese presence in the wind sector prepared by NSCS is enclosed herewith.

3. In view of the above, I would be grateful if NITI Aayog carries out an assessment of the issues highlighted on a priority basis and, in consultation with the Ministry of New and Renewable Energy, recommends necessary policy interventions to address the concerns raised. This would enable India's wind power sector to grow to its full potential, in line with GoI's efforts towards *Atmanirbhar Bharat*.

With Best Regards,

→ CEO: Please see and advise what action is to be proposed. Does NITI have capacity to assess such matters?

Yours sincerely,

(Ajit Doval)

Office of VCH, NITI Aayog
Diary No. 3734/S
Received on 22-8-22
Sent on 22-8-22

Shri Suman Bery
Vice Chairman
NITI Aayog
Sansad Marg, New Delhi
(Encl.: as above)

→ I will reply to acknowledge receipt, copying you.
SB
22/8

Regards

Copy to: Shri Indu Shekhar Chaturvedi, Secretary, Ministry of New and Renewable Energy, Block-14, CGO Complex, New Delhi (for information and necessary action).