Cybersecurity Guidelines for Power Sector

Why in News

Recently, the government released **cybersecurity guidelines for the power sector.**

- This is the **first time that a comprehensive guideline has been formulated** on cyber security in the power sector.
- The guidelines are a **precursor to cybersecurity regulations** that the **Central Electricity Authority** (CEA, Ministry of Power) is working on.

Key Points

- **About:**
  - CEA has framed the guidelines under the **Central Electricity Authority** (Technical Standards for Connectivity to the Grid) (Amendment) **Regulations, 2019.**
  - It **lays down a cyber assurance framework,** strengthens the regulatory framework, puts in place **mechanisms for security threat early warning,** vulnerability management and **response to security threats,** and secures remote operations and services, among others.
  - The **norms are applicable to all responsible entities** as well as system integrators, equipment manufacturers, suppliers/ vendors, service providers, and Information Technology (IT) hardware and software OEMs (Original Equipment Manufacturers) **engaged in the Indian power supply system.**

    Responsible Entities include power generation utilities, distribution utilities, transmission companies and load dispatch centres among others.

- **Major Guidelines:**
  - **Procure from Trusted Source:**
    Mandates Information & Communication Technology-based **procurement from identified 'trusted sources' and 'trusted products'** or else the product has to be tested for malware/hardware trojan before deployment for use in the power supply system network.
  - **Chief Information Security Officer:**
    Appointment of a **Chief Information Security Officer (CISO) at each responsible entity** as well as the setting up of an Information Security Division headed by the CISO.
  - **Procedure for Identifying and Reporting:**
    The **entities will also be required to incorporate a procedure for identifying and reporting** any disturbances suspected or confirmed to be caused by sabotage and submit the report to the sectoral CERT and **Computer Emergency Response Team -India** (CERT-In) within 24 hours.
- **Significance:**
  It will **promote research and development** in cybersecurity and open up the market for setting up cyber testing infra in public as well as private sectors in the country.

Source: IE