

Codec Networks
Coding Threats. Decoding Solutions.

POWER & ELECTRICITY CYBERSECURITY

Secure grids. Reliable power.

IT/OT security, ICS/SCADA assessment, SOC, remote access reviews, resilience and CEA compliance for power utilities.

Three questions every utility leader should be able to answer

Are we ready for the CEA Regulations from April 2027?
The regulations require a senior CISO, a 24-hour Information Security Division, policies, crisis plans and audits (as reported).

Who can reach our SCADA and substations remotely?
Vendor and OEM access must be brokered, time-bound, recorded and monitored.

Could an IT ransomware attack reach the grid?
Segmentation, OT monitoring and OT recovery plans decide whether IT incidents stay in IT.

31 Jul 2026
CEA Regulations notified

1 Apr 2027
In force

6 hours
Incident reporting (as reported)

50 MW
Generator and storage threshold

Built for every power organisation

Thermal, hydro and gas generators · transmission utilities · state and regional load dispatch centres · distribution companies (DISCOMs) · electricity traders and exchanges · captive and industrial power plants.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CEA Cyber Security Regulations, 2026 (in force Apr 2027)	CISO, 24-hour ISD, policy, crisis plan, audits (as reported)
Incident reporting	CSIRT-Power and CERT-In within six hours (as reported)
NCIIPC · DPDP	Critical infrastructure protection; consumer data safeguards

WHAT WE DO

IT/OT security, ICS/SCADA, SOC, remote access, resilience and CEA compliance

IT/OT Security
Architecture, segmentation, OT inventory and IEC 62443-aligned reviews.

ICS/SCADA Assessment
SCADA, EMS, DCS, substation, relay and head-end assessments.

24/7 OT SOC
IT and OT monitoring, hunting and 6-hour reporting support.

Remote Access Reviews
Vendor access brokering, MFA, recording and jump hosts.

Resilience
Crisis management plans, mock drills and OT recovery testing.

CEA Compliance
CEA Regulations gap assessment, policy, CISO support and audits.

Choose your starting point

Foundation
CEA gap assessment, IT/OT segmentation and remote access review, policy pack. For captive plants and smaller utilities.

Assurance
SCADA and substation assessments, smart metering review, annual critical-system audit, IT/OT SOC. For state utilities and DISCOMs.

Continuous Resilience
Continuous OT testing and red teaming, threat hunting, crisis plans and drills, Board reporting. For large generators and grid operators.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

Certified
ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped
Every finding mapped to the CEA Regulations 2026, CERT-In, NCIIPC and DPDP.

One connected partner
Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your assets, control systems and obligations. We will propose a practical, OT-safe assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001
Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018
Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220
Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Source: CEA (Cyber Security in Power Sector) Regulations, 2026, as reported; confirm against the official gazette notification.