

RENEWABLE ENERGY & ENERGY STORAGE CYBERSECURITY

Secure fleets. Reliable clean power.

OT/IoT security, telemetry and cloud assessment, vendor access controls and monitoring for renewables and storage.

Three questions every renewable leader should be able to answer

Who can control our fleet from a vendor portal?

OEM clouds often allow fleet-wide commands; accounts, MFA and approvals decide who can use them.

What is really inside our equipment?

Hardware and firmware inspection finds undocumented modules and insecure defaults before deployment.

Are we covered by the CEA Regulations?

As reported, generators and storage of 50 MW and above are covered from 1 April 2027.

50 MW

CEA Regulations threshold (as reported)

1 Apr 2027

CEA Regulations in force

6 hours

Incident reporting (as reported)

May 2027

Most DPDP obligations take effect

Built for every renewable operator

Utility-scale solar operators · wind farm operators · battery energy storage operators · hybrid and round-the-clock parks · renewable asset managers and O&M providers · smart meter and AMI service providers.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CEA Cyber Security Regulations, 2026 (in force Apr 2027)	Generators and storage of 50 MW and above; CISO, policy, crisis plan, audits (as reported)
Incident reporting	CSIRT-Power and CERT-In within six hours (as reported)
DPDP · contracts	Consumer metering data; PPA, EPC, O&M and OEM obligations

OT/IoT security, telemetry and cloud, vendor access and monitoring

OT/IoT Security

Inverters, controllers, BMS, firmware and site networks.

Telemetry & Cloud Assessment

OEM clouds, portals, telemetry integrity and connectivity resilience.

Vendor Access Controls

OEM and O&M access brokering, MFA, recording and command approvals.

24/7 Monitoring

Fleet-wide OT and cloud monitoring with 6-hour reporting support.

CEA Compliance

CEA Regulations gap assessment, policy, crisis plan and audits.

Supply-Chain Assurance

Equipment inspection, firmware provenance and OEM due diligence.

Choose your starting point

Foundation

Site exposure and credential review, vendor portal access review, basic controls, policy pack. For smaller and single-site operators.

Assurance

CEA gap assessment, inverter, controller and BMS testing, vendor access controls, fleet monitoring. For portfolio operators of 50 MW and above.

Continuous Resilience

Continuous OT and cloud testing, supply-chain assurance, SOC with fleet signals, Board and lender reporting. For large IPPs and AMI providers.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI 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, DPDP and contract obligations.

One connected partner

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

Book a scoping session

Share your portfolio, OEMs 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.