Codec Networks

Coding Threats. Decoding Solutions.

RENEWABLE ENERGY & ENERGY STORAGE

Clean Power. Secure by Design.

OT/IoT security, telemetry and cloud assessment, vendor access controls and monitoring for renewable energy, storage and metering operators

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

The CEA Cyber Security Regulations 2026, CERT-In and DPDP

How Codec Networks helps

Services, bundles and packages built for the sector

Proof in scenarios

Five new case studies and the controls that break the chain

Why Codec Networks and next steps

Our value add and how to start

Renewables now fall under binding cyber regulations

The CEA Regulations cover generators and storage of 50 MW and above (as reported)

50 MW

Generators and storage covered by CEA Regulations (as reported)

1 Apr 2027

CEA Cyber Security Regulations in force

6 hours

To report incidents to CSIRT-Power and CERT-In (as reported)

May 2027

Most DPDP obligations take effect

What this means: renewable and storage operators must control remote and vendor access to their fleets, inspect equipment, secure telemetry and clouds, monitor around the clock and meet CEA governance, audit and reporting requirements.

Source: CEA (Cyber Security in Power Sector) Regulations, 2026, as reported in public sources.

Who we serve across renewables and storage

Solar operators

Utility-scale and rooftop

Wind operators

Onshore wind farms

Battery storage

Grid-scale BESS

Hybrid and RTC parks

Solar, wind and storage

Asset managers and O&M

Portfolio operations

Smart meter providers

AMI service providers

EV charging operators

Charging networks

OEMs and integrators

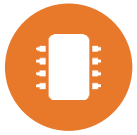
Equipment and controls

The threats that cost renewable operators the most

Six priorities from our 18-threat renewables assessment

Vendor cloud control

Fleet-wide remote commands



Rogue equipment modules

Undocumented communications

Exposed site controllers

Default credentials online

Connectivity loss

Telemetry from remote sites

Insecure updates

Firmware for inverters and meters

Slow detection & reporting

Missing the 6-hour window

Attacks target every layer from field device to portfolio

Where Cyber Risk Sits in Renewable Operations

Every layer from field device to portfolio dashboard carries its own attack surface

Field devices	Site control	Connectivity	Vendor clouds	Asset management	Grid interfaces
SYSTEMS Inverters, turbine controllers, BMS, meters	**SYSTEMS** Plant controllers, SCADA, power plant controllers	**SYSTEMS** Cellular, satellite, VPN links	**SYSTEMS** OEM monitoring and control portals	**SYSTEMS** Portfolio dashboards, analytics, O&M systems	**SYSTEMS** Scheduling, forecasting, metering
TYPICAL ATTACKS Firmware flaws, default credentials, rogue modules	**TYPICAL ATTACKS** Unauthorised control, curtailment	**TYPICAL ATTACKS** Link disruption, exposed services	**TYPICAL ATTACKS** Shared accounts, remote fleet commands	**TYPICAL ATTACKS** Data tampering, ransomware	**TYPICAL ATTACKS** Data manipulation, compliance issues

A renewable fleet can be switched from a laptop—so whoever controls remote access controls generation.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

The CEA Cyber Security Regulations 2026, CERT-In and DPDP

Codec Networks
Coding Threats. Decoding Solutions.

The rules that shape renewable energy cybersecurity

Requirement	Frequency / deadline	Source
Applicability	Generators, captive plants and storage of 50 MW and above	CEA Regulations, 2026
CISO	Senior level, alternate, minimum three-year tenure	CEA Regulations, 2026
Information Security Division	24-hour operation	CEA Regulations, 2026
Cyber Crisis Management Plan	At least one mock drill a year	CEA Regulations, 2026
Audit of critical systems	Annual	CEA Regulations, 2026
Incident reporting	CSIRT-Power and CERT-In within 6 hours	CEA Regulations, 2026; CERT-In
Entities below thresholds	Basic CERT-In controls for MSMEs encouraged	CEA Regulations, 2026
Consumer metering data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Codec Networks
Coding Threats. Decoding Solutions.

Key dates on the regulatory timeline

Regulatory Timeline for Renewable Energy Cybersecurity

Key power-sector and cross-sector instruments shaping renewable cybersecurity

In force Upcoming (from Oct 2026)

Jul 2021	Revamped Distribution Sector Scheme launched, including smart metering
Oct 2021	CEA Cyber Security Guidelines for the power sector issued
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Jul 2026	CEA Cyber Security Regulations notified, covering generators and storage of 50 MW and above
Apr 2027	**CEA Cyber Security Regulations come into force (1 April)**
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: CEA, Ministry of Power, MNRE, CERT-In. Confirm obligations against the official notifications.

Codec Networks

How Codec Networks helps

OT/IoT security · Telemetry & cloud · Vendor access · Monitoring · CEA compliance · Supply chain

Codec Networks
Coding Threats. Decoding Solutions.

One partner from inverter to portfolio

OT/IoT Security

Inverters, controllers, BMS, sites

Telemetry & Cloud Assessment

OEM clouds, portals, telemetry

Vendor Access Controls

Brokered, recorded, approved access

24/7 Monitoring

Fleet-wide OT and cloud monitoring

CEA Compliance

Gap assessment, policy, audits

Supply-Chain Assurance

Equipment and firmware inspection

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **B1** Cyber Assessment & VAPT Assurance
- **B2** Application, API & DevSecOps Security
- **B3** Cloud, Infrastructure & Zero Trust
- **B4** Regulatory Cyber Audit & Compliance
- **B5** GRC, ISO, SOC 2 & PCI DSS Maturity
- **B6** Data Privacy & DPDPA Program
- **B7** Managed SOC, MDR & Threat Monitoring
- **B8** Forensics, Incident Response & Malware RCA
- **B9** Third-Party & Supply-Chain Risk
- **B10** Cyber Simulation, Awareness & Tabletop
- **B11** Emerging Tech, AI & Web3 Security

Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Smaller and single-site operators

- Site exposure review (B1)
- Vendor portal access review (B3)
- Basic MSME controls (B5)
- Policy pack (B5)

Assurance

Portfolio operators (50 MW and above)

- CEA gap assessment (B4)
- Inverter, controller, BMS testing (B1)
- Vendor access controls (B3, B9)
- 24x7 fleet monitoring (B7)

Continuous Resilience

Large IPPs, storage and AMI providers

- Continuous OT and cloud testing (B1, B10)
- Supply-chain assurance (B9)
- SOC with fleet signals (B7)
- Board and lender reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Generators and storage of 50 MW and above covered (CEA Regulations 2026, as reported)	Applicability and gap assessment	B4
Senior CISO, policy and crisis management plan (as reported)	Governance, policy and crisis plan support	B5, B10
Annual audit of critical systems (as reported)	Independent OT and IT audits	B4, B1
Incidents to CSIRT-Power and CERT-In within six hours (as reported)	Fleet monitoring, IR and reporting support	B7, B8
OT separation and vendor accountability (as reported)	Segmentation and vendor access controls	B3, B9
Equipment and supply-chain security	Equipment inspection and OEM assessments	B9, B1
Consumer metering data safeguards (DPDP)	DPDPA programme for metering providers	B6

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Wind Farm That Lost Its Link**	A satellite provider attack cuts telemetry; diverse links and fail-safes limit it	B3 · B9 · B10
2	**The Inverter Portal Everyone Shared**	A shared vendor login curtails plants; MFA and approvals stop it	B3 · B9 · B7
3	**The Rogue Radio in the Inverter**	An undocumented module is found before deployment; inspection catches it	B1 · B9 · B5
4	**The Battery System on the Open Internet**	An exposed EMS with default credentials is misused; hardening prevents it	B1 · B3 · B7
5	**The Smart Meter Update That Went Wrong**	A tampered unsigned update breaks meters; signing prevents it	B2 · B1 · B8

Example: breaking a vendor-portal chain

Case 2: The Inverter Portal Everyone Shared

ILLUSTRATIVE ATTACK PATH

Step 1
An OEM cloud portal can control a fleet of inverters

→

Step 2
Site teams and contractors share one admin login

→

Step 3
The password is phished

→

Step 4
Attacker curtails output across several plants

→

Step 5
Generation loss and PPA penalties

WHERE CONTROLS BREAK THE CHAIN

- Named accounts and MFA on vendor portals
- Role-based control and command approvals
- Monitoring of fleet commands
- Vendor cloud security assessments

Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: vendor portal accounts and MFA, role-based control and command approvals, monitoring of fleet-wide commands, OEM cloud security, and the CSIRT-Power and CERT-In reporting steps.

Why renewable operators choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to the CEA Regulations 2026, CERT-In, DPDP and contracts

Tests the whole chain

Technical, process and monitoring tests together

Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected

Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST

How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement

Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Portfolio, OEMs, vendor clouds, connectivity and compliance calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

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

011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

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.

Codec Networks
Coding Threats. Decoding Solutions.