DRAGOS

WHITEPAPER

India CEA Cyber Security Regulations 2026

Breaking down the new mandatory OT cyber security framework.

REGULATORY OVERVIEW

What This Regulation Requires

India's Central Electricity Authority (CEA) published these regulations under the Electricity Act, 2003. Effective 1 April 2027, they apply to generation companies (≥50 MW), captive plants with Energy Storage Systems, transmission and distribution licensees, Load Dispatch Centres at national, regional, and state levels, and power exchanges.

The framework establishes CSIRT-Power as the sector's cyber security coordinator and creates a responsibility chain from the Ministry of Power CISO down to entity-level CISOs and dedicated 24/7 Information Security Divisions. It is not a documentation exercise — it requires demonstrable OT security capability: asset visibility, continuous monitoring, threat detection, incident response, and annual audit.

1 April 2027

Enforcement date

≥50 MW

Installed capacity threshold

6 hours

Incident reporting window

COMPLIANCE PRIORITIES

Areas That Demand Immediate Attention

These carry the highest operational and governance weight. Most require OT-specific technical capability that standard IT tools cannot deliver.

REGULATION AREA	REQUIREMENT	HOW DRAGOS HELPS	CAPABILITY	PRIORITY
OT Asset Inventory Reg. 5(25), 8(4)	Continuously updated register of all cyber assets — hardware, firmware, OS, patch level, protocols, and data flows.	Most OT asset registers are built manually and go stale within weeks. The Dragos Platform builds and maintains inventory automatically using a multi-detection engine across 600+ industrial protocols — Active Collection fills in segmented or low-traffic environments where passive monitoring alone cannot reach. Engineers get an always-current picture of their environment. No spreadsheets. No guesswork.	• Platform: Asset Visibility • Active Collection	High
Continuous OT Monitoring Reg. 5(36), 6(2)	24/7 surveillance of OT/IT systems. Full logging at Electronic Security Perimeter. 180-day log retention minimum.	The Dragos Platform monitors all xOT assets. It identifies anomalous communications, unexpected device behaviour, and lateral movement disrupting critical operations. OT Watch extends this with 24/7 expert-led monitoring when in-house staffing cannot cover the round-the-clock requirement the CEA mandates.	• Platform: Network Monitoring • Platform: Detection Analytics • OT Watch	High
OT/IT Segmentation Validation Reg. 6(1), 6(2), 6(6)	Physical OT isolation mandatory. Where Interconnection is permitted, logical separation with continuous monitoring required.	Network diagrams show intended architecture. Dragos shows actual architecture and the gaps between the two. Segmentation Validation analyses firewall, router, and switch configuration files to map real network topology, identify unintended cross-zone communication paths, and continuously detect configuration drift. This replaces point-in-time audits that go stale the moment a change is made. When the CEA requires entities to demonstrate that OT/IT interconnections are controlled and continuously monitored, Segmentation Validation produces evidence to support that claim.	• Platform: gmentation Validation • Platform: Network Monitoring	High

REGULATION AREA	REQUIREMENT	HOW DRAGOS HELPS	CAPABILITY	PRIORITY
Threat Detection & Incident Response Reg. 5(36), 7(3a)	Detect and report incidents within 6 hours. Defined IR and Recovery Plans. Root Cause Analysis after every incident.	The Dragos Platform provides four types of threat detection: configuration changes, network & protocol anomalies, indicators of compromise (IoCs), and threat behaviors. Every IoC and threat behavior detection is linked to the adversary group or threat behaviour that produced it — drawn from Dragos tracking of 26+ ICS-specific threat groups. Analysts are not staring at an unexplained anomaly. They see what the behaviour is, which adversary group uses it, and what to do next. OT-native response playbooks authored by Dragos practitioners walk analysts through specific containment and remediation steps for each threat type. Case management captures the full investigation timeline, forensic evidence, and action taken — producing structured documentation to support CSIRT-Power and CERT-In requirements in post-incident reporting. OT Watch Complete adds SLA-backed escalation with first validated alert delivered within defined timeframes.	• Platform: Threat Detection • Platform: IR & Response • OT Watch Complete • Dragos EmberAI	High
Vulnerability Management Reg. 5(26), 5(27)	Risk Assessment and Mitigation Plan updated every 6 months. VA/ Pen test before commissioning. Critical findings fixed within 1 month.	IT-focused vulnerability scoring is wrong for OT in roughly assigning high severity to vulnerabilities that carry no real risk in an OT context, while underselling those that do. The Dragos Platform applies OT-corrected CVSS scores and enriches every vulnerability with operational context: whether it is exploitable in the specific environment, whether Dragos has observed it being used by tracked threat groups, and whether patching is feasible given operational constraints. “Now, Next, Never” prioritisation gives security teams a clear action order. Only 3–6% of OT vulnerabilities require immediate action — Dragos identifies exactly which ones. WorldView provides the threat intelligence layer, confirming which vulnerabilities are actively exploited by adversaries targeting Indian and global power infrastructure.	• Platform: Vulnerability • WorldView • OT Cyber Security Assessment	High

REGULATION AREA	REQUIREMENT	HOW DRAGOS HELPS	CAPABILITY	PRIORITY
OT Threat Intelligence Reg. 7(3f), 4(2a)	CISO must gather and analyse threat intelligence. CSIRT-Power requires sector-specific threat prediction.	Generic threat intelligence was not built for OT. Indicators of compromise designed for IT environments do not map to ICS protocols or power sector attack patterns. Dragos WorldView is the only finished threat intelligence built exclusively for operational technology — produced by the largest private ICS/OT threat intelligence team in the industry. WorldView tracks 26+ named OT adversary groups, including those with demonstrated interest in electric sector infrastructure. It delivers finished intelligence: confirmed adversary TTPs, OT-specific IOCs ready for SIEM integration, and vulnerability context that accounts for operational constraints. Dragos EmberAI makes this intelligence immediately queryable. CISOs and analysts can ask specific questions about threats relevant to their environment and receive answers grounded in over a decade of OT field data.	• WorldView • Dragos EmberAI • Platform: knowledge packs	High
24/7 SOC Coverage Reg. 5(9), 5(36)	InfoSec Division must operate round the clock. 6-hour reporting window demands real-time detection.	Building a 24/7 in-house OT SOC from scratch requires specialised staff, training, tooling, and time that most entities do not have before April 2027. OT Watch Complete provides the equivalent capability immediately. Dragos OT security analysts monitor, triage, and investigate all platform alerts around the clock, escalating only validated, high-confidence threats with full OT context already attached. This eliminates alert fatigue and closes the expertise gap. IT-trained SOC staff cannot accurately triage OT alerts because they lack the protocol knowledge and process context to distinguish a real threat from normal industrial communications. Dragos analysts do this every day across hundreds of environments. The 6-hour CSIRT-Power reporting requirement is met structurally: Dragos identifies, validates, and escalates before the clock runs out.	• OT Watch Complete • OT Watch • Platform: Insights Hub	Medium

REGULATION AREA	REQUIREMENT	HOW DRAGOS HELPS	CAPABILITY	PRIORITY
Incident Response Retainer Reg. 5(35), 8(9)	IR and Recovery Plan maintained and tested. Recover and resume operations. Post-incident reporting required.	When a real incident hits, the cost of starting from scratch is measured in days of downtime. The Dragos Rapid Response Retainer pre-establishes the agreements, environmental documentation, and access arrangements required to mobilise immediately. For Dragos Platform customers, SLA-backed response times begin with first responder contact within one hour of notification and active analysis underway within four. Dragos responders arrive with OT-specific context; not generic IR playbooks adapted from IT. They understand power system architecture, ICS protocols, and the operational constraints that govern what can and cannot be done during an active incident. Post-incident, Dragos produces the structured root cause analysis and lessons learned documentation that the CEA requires entities to complete and share with CSIRT-Power.	• Rapid Response Retainer • IR Services • Platform: IR & Response	Standard

SCOPE NOTE

What Dragos Does Not Cover

Several CEA requirements sit outside OT security tooling entirely. Entities need complementary partners for: CISO HR and designation frameworks, ISO/IEC 27001 certification bodies, India's Digital Personal Data Protection Act compliance, IT-side access control and web application security, vendor contract and NDA management, legal reporting under the IT Act, 2000, and physical access security controls.

Dragos provides the OT visibility, detection, and expert services that make the technical requirements achievable. Governance and legal obligations require separate solutions.

India's Power Sector Needs OT-native Security. Not IT Tools Retrofitted for OT.

With 600+ customers globally, 7.8 million OT assets protected, and the largest private ICS threat intelligence team in the industry, Dragos gives Indian power sector entities what the CEA framework requires: real OT visibility, accurate threat detection, and expert services built for operational environments. Contact your Dragos representative or visit dragos.com to request a briefing.

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com