July 31, 2026

MINISTRY OF POWER

Power sector cyber security rules bind vendors from April 2027

From April 1, 2027, CEA's power sector cyber security regulations require vendors to give recovery plans, signed or authenticated patches and a bill of materials.

THE CENTRAL ELECTRICITY Authority (CEA) made the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, by notification F. No. CEA-HY-91-19/8/2024-Cyber Security Division, dated July 31, 2026 and published the same day in the Gazette of India, Extraordinary, Part III, Section 4, No. 484. It made them under section 177(1) read with section 73(c) of the Electricity Act, 2003, with the concurrence of the Ministry of Electronics and Information Technology, after the draft 2025 regulations were made available to the public on October 7, 2025. They come into force on April 1, 2027. Regulations 5(9), 5(24), 5(33), 5(39), 6(2) and 6(7) come into force "on such dates, as may be specified by the Authority through separate orders with prior approval of the Central Government"; the notification gives no dates for them. These cover an Information Security Division within India, ISO/IEC 27001 or Technical Criteria certification, cyber security courses for staff, vendor staff included, procurement of IT and OT equipment and services from trusted sources, and perimeter security devices for OT systems. The regulations are signed by Sharvan Kumar, Secretary.

KEY FACTS

AUTHORITY

Ministry of Power

PUBLISHED

July 31, 2026

ISSUED BY

Central Electricity Authority

DOCUMENT

Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, F. No. CEA-HY-91-19/8/2024-Cyber Security Division

Power sector cyber security rules bind vendors from April 2027

Ministry of Power · July 31, 2026

The Central Electricity Authority (CEA) made the Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, by notification F. No. CEA-HY-91-19/8/2024-Cyber Security Division, dated July 31, 2026 and published the same day in the Gazette of India, Extraordinary, Part III, Section 4, No. 484. It made them under section 177(1) read with section 73(c) of the Electricity Act, 2003, with the concurrence of the Ministry of Electronics and Information Technology, after the draft 2025 regulations were made available to the public on October 7, 2025. They come into force on April 1, 2027. Regulations 5(9), 5(24), 5(33), 5(39), 6(2) and 6(7) come into force "on such dates, as may be specified by the Authority through separate orders with prior approval of the Central Government"; the notification gives no dates for them. These cover an Information Security Division within India, ISO/IEC 27001 or Technical Criteria certification, cyber security courses for staff, vendor staff included, procurement of IT and OT equipment and services from trusted sources, and perimeter security devices for OT systems. The regulations are signed by Sharvan Kumar, Secretary.

They apply to all entities that own, operate or manage Operational Technology (OT) infrastructure associated with the interconnected power system, and their Information Technology (IT) infrastructure connected to it, existing and upcoming. Entities include generating companies, captive generating plants, organizations having an Energy Storage System, transmission and distribution licensees, the national, regional and state load dispatch centers, power exchanges and over the counter platforms. Generating companies, captive plants and storage owners are covered only at an installed capacity of 50 MW or more; smaller ones are encouraged to apply CERT-In's "15 Elemental Cyber Defense Controls for Micro, Small and Medium Enterprises". Regulation 2(2) says the vendor shall comply with regulations 11 and 12, as applicable. A "vendor" is an "original equipment manufacturer, original equipment supplier, system integrator, supplier of hardware or software associated with original equipment, contractor or service provider including cloud service provider", and the manufacturer and supplier of hardware, firmware or software for the original equipment or control systems of a Distributed Generation Resource owned by a prosumer, "including but not limited to inverters, communication modules, monitoring systems, and related control or energy management software". A Distributed Generation Resource is a generating station feeding electricity at below 33 kV, including grid-connected rooftop solar systems and Energy Storage System.

Under regulation 11, the vendor must give the entity documented and tested procedures and a recovery plan for restoring the systems it supplied from potential cyber crisis scenarios (11(1)). It must make security patches and updates, "either digitally signed or validated and authenticated", available for all systems and components it supplied throughout the contract period or the systems' useful life, whichever is later (11(2)). It must give the entity a detailed document of all requirements and processes, including the security patches and updates to be installed on third-party components, needed to integrate a component or sub-system it supplies (11(3)), and give

details of end of support or end of life of the software, hardware and systems it supplied, including third-party ones (11(4)). It must provide a bill of materials "as per Indian Computer Emergency Response Team guidelines issued from time to time", listing all components supplied for applications, including firmware, deployed in critical systems (11(5)), and harden hardware and software before supply by enabling all inherent security capabilities, secured configuration and controls (11(6)). It must set up a formal structured process for entities to report vulnerabilities in its products and services, and furnish them to the Computer Security Incident Response Team - Power (CSIRT-Power) through its vulnerability disclosure and management program (11(7)). Vendors must also comply with CSIRT-Power's directions and guidelines, as applicable (4(3)).

Regulation 12 covers vendors for prosumers' Distributed Generation Resources. The vendor must ensure that "any application, associated monitoring and control servers, and the real-time data of such systems including any data or information hosted on cloud platforms as well as associated historical data or information, be stored in an encrypted, secure, and protected environment and shall reside exclusively within India" (12(1)). Remote access and remote operation of grid-connected devices, and exchange of their real time data with remote applications, aggregators and distribution licensees, "shall be established through secure channel after mutual authentication and such communication shall be encrypted" (12(2)). The vendor must also provide information needed to verify a trusted source under Central Government orders (12(3)). For existing prosumer Distributed Generation Resources, regulation 12 comes into force on a date the Authority specifies by separate order. Power exchanges and over the counter platforms are exempt from regulations 6, 11 and 12.

Some duties the regulations place on entities also concern their vendors. Service level agreements with vendors must include all cyber security requirements and a non-disclosure agreement. A vendor with cyber or physical access to critical systems, its staff included, may be permitted after a personnel risk assessment and an undertaking. After a cyber security breach, the entity must inquire into it and initiate action against the vendor that committed it, cloud service providers included (5(20)). Procurement must include Factory and Site Acceptance Tests that test cyber security requirements (5(31)). An entity's cyber security policy has OT updates and patches digitally signed by the original equipment manufacturer, or their validity and authenticity verified where that signature is not available (8(25)). An entity's Chief Information Security Officer must report cyber security incidents to CSIRT-Power and CERT-In within six hours (7(3)(a)). In specific cases, the Chief Information Security Officer of the Ministry of Power may recommend to the Central Government proceedings under the Information Technology Act, 2000, or a petition before the Appropriate Commission under section 142 of the Electricity Act (regulation 16); the regulations do not say whether this reaches vendors. They do not define useful life, do not say how a vendor shows compliance, and leave trusted sources and IT and OT equipment requirements to Central Government orders.

Issued by | Central Electricity Authority

Document	Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026, F. No. CEA-HY-91-19/8/2024-Cyber Security Division
Dated	July 31, 2026
Published	Gazette of India, Extraordinary, Part III, Section 4, No. 484, July 31, 2026
Takes effect	April 1, 2027
Later dates	Regulations 5(9), 5(24), 5(33), 5(39), 6(2) and 6(7): dates the Authority specifies by separate orders, with prior approval of the Central Government; regulation 12 for existing prosumer Distributed Generation Resources: a date the Authority specifies by separate order
Applies to	Entities that own, operate or manage OT infrastructure of the interconnected power system (generators, captive plants and storage at 50 MW or more; transmission and distribution licensees; load dispatch centers; power exchanges and over the counter platforms, except regulations 6, 11 and 12), and vendors under regulations 11 and 12
Vendor	Original equipment manufacturers and suppliers, system integrators, hardware or software suppliers, contractors and service providers including cloud service providers, and suppliers of equipment and software for prosumer Distributed Generation Resources, such as inverters
Prosumer equipment data	Applications, monitoring and control servers and real-time and historical data, cloud-hosted included, encrypted and to "reside exclusively within India"
Patches	Digitally signed or validated and authenticated, for the contract period or the system's useful life, whichever is later
Incident reporting	By the entity's Chief Information Security Officer, within six hours to CSIRT-Power and CERT-In; an incident concluded to be cyber sabotage in critical systems, within twenty-four hours (7(3)(a))
Legal basis	Section 177(1) read with section 73(c), Electricity Act, 2003; concurrence of the Ministry of Electronics and Information Technology
Draft	Draft 2025 regulations, made available to the public on October 7, 2025
Signed by	Sharvan Kumar, Secy.

What vendors must do, by regulation

Regulation	Applies	Requirement
2(2)	Vendor	Comply with regulations 11 and 12, as applicable
4(3)	Vendor	Comply with CSIRT-Power's directions and guidelines on power sector cyber security, as applicable
11(1)	Vendor	Documented and tested procedures and a recovery plan for restoring supplied systems from potential cyber crisis scenarios
11(2)	Vendor	Security patches and updates, digitally signed or validated and authenticated, available for the contract period or the systems' useful life, whichever is later
11(3)	Vendor	A detailed document of all requirements and processes, including security patches and updates to be installed on third-party components, to integrate a component or sub-system it supplies
11(4)	Vendor	Details of end of support or end of life of supplied software, hardware and systems, third-party ones included
11(5)	Vendor	A bill of materials as per CERT-In guidelines, listing all components supplied for applications, including firmware, deployed in critical systems
11(6)	Vendor	Hardware and software hardened before supply: all inherent security capabilities enabled, secured configuration and controls
11(7)	Vendor	A formal structured process for entities to report vulnerabilities; vulnerabilities furnished to CSIRT-Power through its vulnerability disclosure and management program
12(1)	Vendor, prosumer Distributed Generation Resources	Applications, monitoring and control servers and real-time and historical data, cloud-hosted included, encrypted and residing exclusively within India
12(2)	Vendor, prosumer Distributed Generation Resources	Remote access, remote operation and real-time data exchange through a secure channel after mutual authentication, with encrypted communication
12(3)	Vendor, prosumer Distributed Generation Resources	Information needed to verify a trusted source, under Central Government orders
5(20)	Entity, in its contracts	Service level agreements with all cyber security requirements and a non-disclosure agreement; a vendor with cyber or physical access to critical systems, its staff included, permitted after a personnel risk assessment and an undertaking; inquiry and action against a vendor, cloud service providers included, that commits a cyber security breach

5(31)	Entity, in procurement	Factory and Site Acceptance Tests, including tests of cyber security requirements
5(33)	Entity (date to be specified)	Staff, vendor staff included, in day-to-day operation and maintenance of critical systems to have undergone designated cyber security courses
5(39), 6(7)	Entity (dates to be specified)	IT and OT equipment and services procured from trusted sources, under Central Government orders
5(41)	Entity	Structured vulnerability disclosure and management programs with vendors and CSIRT-Power
8(25)	Entity's cyber security policy	OT updates and patches digitally signed by the original equipment manufacturer, or their validity and authenticity verified where that signature is not available

The notification (regulations) (PDF, 1.2 MB)

Source: Gazette of India, CG-DL-E-05082026-275218.

Checked against the official copy on October 28, 2026.

IndusDesk

hello@indusdesk.com · +91 11 4141 3939

9th Floor, Hemkunt House, Rajendra Place, New Delhi, Delhi 110008, India

Read online: indusdesk.com/ministry-of-power/insights/power-sector-cyber-security-rules-bind-vendors-from-april-2027/