Cyber Resilience Act (CRA)

September 11, 2026

Working Together for Secure and Resilient Energy Solutions

Cybersecurity is a core commitment at Siemens Energy

At Siemens Energy, cybersecurity is an essential part of how we design, develop, operate, and support our products and solutions.
As the energy industry becomes increasingly digital, cybersecurity is more important than ever for protecting critical infrastructure, ensuring reliable operations, and maintaining customer trust. We consider cybersecurity not only as a regulatory requirement, but as a core responsibility and a key quality attribute of our products.
The European Union's Cyber Resilience Act (CRA) establishes common cybersecurity requirements for products with digital elements (PDEs). As a manufacturer of products that fall within the scope of the CRA, Siemens Energy is committed to implementing these requirements and continuously strengthening cybersecurity throughout the lifecycle of our products.

What is the Cyber Resilience Act?

The Cyber Resilience Act (CRA) is the EU's first horizontal cybersecurity regulation to boost security and cyber resilience across the EU. It applies to 'Products with Digital Elements' (**PDEs**) that are made available in the EU market and are intended or expected to connect directly or indirectly to a device or network, either via a logical or a physical connection.
The CRA sets the mandatory and essential cybersecurity requirements, and vulnerability reporting obligations for the entire lifecycle of such products. Compliance with the obligations must be indicated with an appropriate CE marking.
The regulation introduces requirements for:

- Secure product design and development
- Cybersecurity risk management
- Vulnerability handling and remediation
- Security updates and lifecycle support

Siemens Energy is a trademark licensed by Siemens AG.

- Incident and vulnerability reporting
- Product compliance documentation

The CRA applies to manufacturers, importers, distributors, and other relevant economic operators who place products with digital elements on the European market.

Why suppliers are important

Cybersecurity is a shared responsibility across the entire value chain.

To comply with the CRA and to maintain strong cybersecurity standards, Siemens Energy works closely with suppliers whose products, components, software, services, or technologies contribute to Siemens Energy solutions and/or products.
Our objective is not simply regulatory compliance. Together with our suppliers, we aim to continuously improve cyber security, resilience, and long-term sustainability of the products and solutions we deliver to customers worldwide.

This collaboration helps Siemens Energy:

- Meet regulatory obligations
- Maintain secure and resilient products
- Strengthen vulnerability management processes
- Ensure lifecycle support for products and components
- Protect customers and critical infrastructure

We believe successful cybersecurity requires transparency, collaboration, and a long-term partnership approach.

What we may request from suppliers

Depending on the products or services provided, Siemens Energy may request information or support related to:

- Product cybersecurity capabilities
- Technical compliance documentation
- Secure development practices
- Vulnerability management processes

Siemens Energy is a trademark licensed by Siemens AG.

- Software Bill of Materials (SBOM), where applicable
- Product support and maintenance periods
- Security updates and patch management
- Cybersecurity incident or vulnerability notifications
- Product discontinuation or end-of-support information

Specific requirements may arise from the CRA, customer expectations, contractual obligations, or Siemens Energy cybersecurity requirements.

Products with Digital Elements (PDEs)

A product with digital elements (**PDE**) is defined as '*a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately*'.
Examples include:

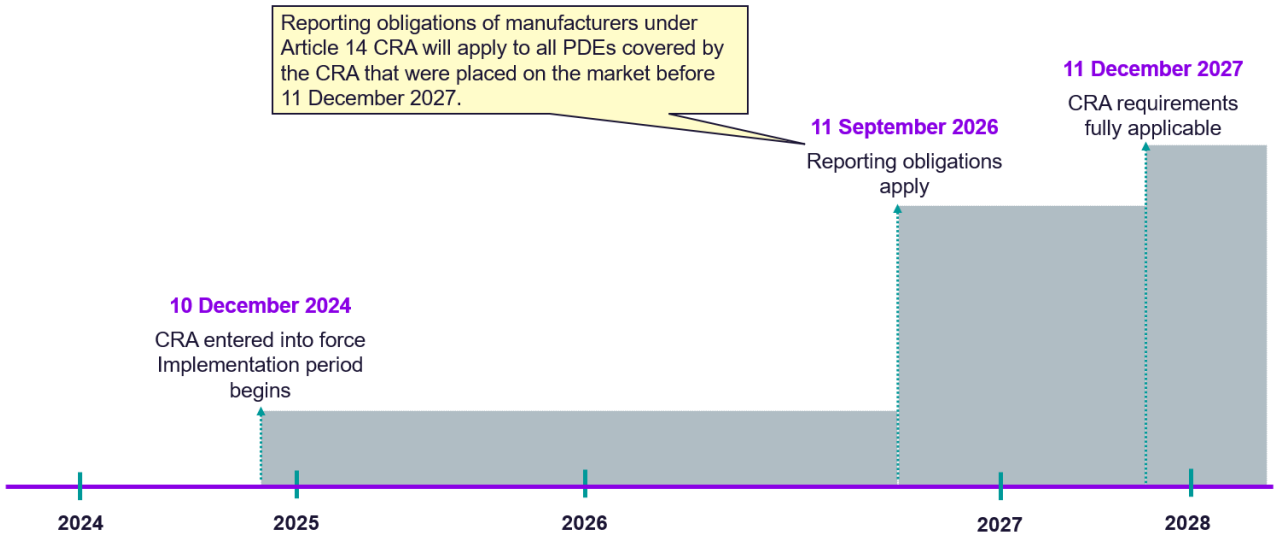
- Industrial control systems
- Embedded devices
- Software applications
- Connected hardware
- Operating systems
- Digital monitoring and automation solutions

Many components supplied into Siemens Energy products may therefore fall within the broader CRA ecosystem.

Siemens Energy is a trademark licensed by Siemens AG.

Key CRA milestones

While the EU CRA came into force on 10 December 2024, the reporting obligations will apply from 11 September 2026, and the CRA will fully be applicable from 11 December 2027 (for PDEs placed on the market from this day onwards). Some of the obligations detailed below apply to products with digital elements that were placed on the EU market before 11 December 2027 only if, from that date onwards, those products undergo a substantial modification.



Learn more

- European Commission – Cyber Resilience Act
- CRA Summary and Guidance
- Official CRA Regulation (EU) 2024/2847
- BSI CRA

Together towards secure and resilient products

Cybersecurity is a key enabler of trust, resilience, and sustainable innovation. Siemens Energy looks forward to working closely with suppliers to strengthen cybersecurity capabilities, support regulatory compliance, and deliver secure products for the future.

Disclaimer: This document is intended for general information purposes only and does not constitute legal advice. Suppliers remain responsible for assessing their own obligations under applicable laws and regulations.

Siemens Energy is a trademark licensed by Siemens AG.