Reference: Understanding the EU Cyber Resilience Act (CRA)

The EU Cyber Resilience Act (CRA) is a forthcoming regulation designed to strengthen the cybersecurity of Products with Digital Elements (PDEs) placed on the EU market. PDEs include industrial controllers, sensors, firmware, software, and connected devices.

Key Points of CRA:

- **Applies to all manufacturers placing PDEs on the EU market, regardless of where the product is developed or produced.**

- **Requires cybersecurity by design, including secure default configurations, vulnerability handling, and regular security updates.**

- **Requires technical documentation** and declarations of conformity covering cybersecurity aspects.

- **Compliance Deadline:** Full compliance will be required by **December 2027**, with certain obligations taking effect sooner (e.g., vulnerability handling processes).

Impact on Manufacturers:

- Products must demonstrate compliance with baseline cybersecurity requirements, aligned with international best practices (e.g., IEC 62443, ENISA guidance).

- Non-compliant products may face **market access restrictions** within the EU, **recalls**, or **fines**.

For more information, visit the EU CRA information page: [EU CRA Information Page]