Milesight IoT's Commitment to Cybersecurity and Compliance with EU Regulations

Milesight IoT, a pioneering provider of IoT product solutions, underscores its unwavering commitment to cybersecurity and regulatory compliance by aligning with the **European Union's NIS2 Directive**, as well as actively supporting the objectives of the **Cyber Solidarity Act** and the **Cyber Resilience Act**.

Through comprehensive security assessments, robust vulnerability management, supply chain protection, and enhanced encryption measures, Milesight IoT continues to strengthen its cybersecurity practices. We remain dedicated to collaborating with stakeholders across the value chain to foster a safer, more resilient digital environment.

Understanding the EU Cybersecurity Framework

NIS2 Directive

The **Directive on Security of Network and Information Systems (NIS2)** is a pivotal legislative measure that comes into effect in **October 2024**, aiming to raise cybersecurity standards across the EU. Building on the original NIS Directive, it introduces:

- **Expanded Scope:** Broader coverage of industries and medium-to-large enterprises, including healthcare, energy, transport, and public administration.
- **Stricter Cybersecurity Requirements:** Stronger obligations for risk management, incident reporting, and supply chain controls.
- **Unified Enforcement Mechanism:** Clearer enforcement rules and enhanced cross-border cooperation.
- **Incident Reporting:** Mandatory reporting of major incidents to authorities within 24 hours of detection.

Cyber Solidarity Act

The Cyber Solidarity Act (CRA) aims to enhance collective EU cybersecurity preparedness, detection, and response capabilities. It establishes a European Cybersecurity Shield and introduces a Cybersecurity Emergency Mechanism, enabling member states and organizations to collaborate in addressing large-scale cyber incidents.
Learn More

Cyber Resilience Act

The Cyber Resilience Act (CRA) sets out cybersecurity requirements for products with digital elements, ensuring they are designed, developed, and maintained with security in mind throughout their lifecycle. It emphasizes "security by design" and "security by default" principles for connected devices, reducing

vulnerabilities and improving resilience.

Learn More

How Milesight IoT Aligns with EU Cybersecurity Regulations

- **Assessment of Existing Security Systems**
  Milesight IoT conducts continuous, comprehensive assessments to ensure compliance with NIS2 requirements and readiness for CRA obligations.
- **Security Vulnerability Management**
  We proactively identify, mitigate, and report vulnerabilities with transparency, reducing risks across our product portfolio.
- **Supply Chain Security**
  Rigorous supplier audits and risk assessments ensure full compliance with NIS2 and CRA requirements throughout our global supply chain.
- **Strengthened Data Encryption**
  Milesight IoT implements advanced encryption to protect video data and sensitive information during transmission and storage.
- **Collective Cybersecurity Preparedness**
  In line with the Cyber Solidarity Act, Milesight IoT is committed to cross-border collaboration and rapid response capabilities to support customers and partners during cyber emergencies.

Our Ongoing Commitment

Milesight IoT stands firm in its mission to deliver secure, resilient, and compliant solutions. By aligning with the NIS2 Directive, the Cyber Solidarity Act, and the Cyber Resilience Act, we go beyond regulatory requirements to safeguard digital assets, strengthen cyber resilience, and foster trust with our customers and partners.

Together, we build a robust cyber ecosystem where technology and security move forward hand in hand.

If you have any questions or require further information on our cybersecurity and compliance measures, please contact us at iot.sales@milesight.com.