Subject: AMI and the EU Cyber Resilience Act

Dear Customer(s) and/or Supply Chain Partner(s)

Thank you for your inquiry regarding AMI's approach to the EU Cyber Resilience Act (Regulation (EU) 2024/2847) ("CRA"). At AMI, we are committed to empowering our customers — device manufacturers — with robust firmware solutions and support to navigate the evolving landscape of cybersecurity regulations, including the CRA. As a trusted firmware supplier to the global computing industry, AMI understands the CRA is a priority for our customers, and we want to share how AMI is addressing it.

AMI's CRA Compliance Program

AMI is actively assessing and addressing all CRA obligations applicable to its firmware products and is committed to supporting our customers in meeting their CRA obligations. AMI has established a dedicated compliance program to ensure that its products meet applicable CRA requirements within the regulatory timelines, including the mandatory vulnerability reporting obligations that take effect on September 11, 2026, and full compliance requirements by December 11, 2027. As part of this program, AMI has already taken a number of steps, including:

- AMI maintains an active Product Security Incident Response Team (PSIRT) with established vulnerability identification, tracking, and remediation processes. AMI's PSIRT advisories include confirmation of actively exploited vulnerabilities, description and severity information, available information about malicious actors, and details of available security updates, enabling customers to take timely action in support of their CRA reporting obligations.
- AMI has implemented secure development lifecycle practices across its firmware products, consistent with the CRA's secure-by-design and secure-by-default principles. AMI's firmware is continuously audited by an external firm as part of AMI's annual ISO 27001 certification.
- AMI maintains a coordinated vulnerability disclosure policy and publishes security advisories to customers.
- AMI is building automated SBOM generation capabilities to deliver machine-readable SBOMs in SPDX and/or CycloneDX format for each firmware release, with the intention of delivering product-level SBOMs to customers as part of each firmware version release ahead of the December 11, 2027 compliance deadline.
- AMI is conducting product classification analysis to determine the applicable CRA tier for each firmware product line, which will inform the applicable conformity assessment pathway. AMI intends to CE-mark applicable firmware products and provide customers with corresponding EU Declarations of Conformity ahead of the December 11, 2027 deadline.
- AMI is working toward completion of all applicable technical documentation and related compliance deliverables within the regulatory timelines.

AMI intends to be fully compliant with all applicable CRA requirements by the dates specified in the regulation, and is committed to collaborating closely with our customers to support their compliance efforts.

Customer CRA Obligations

As you may be aware, the CRA establishes independent compliance obligations for each entity in the supply chain based on its role with respect to the products it places on the EU market. Your organization's CRA obligations for its finished products are determined by its role under the regulation and are assessed separately from AMI's obligations for its firmware products. At the same time, AMI recognizes that the CRA's supply-chain framework creates important connections between AMI's compliance and yours. For example, AMI's conformity documentation, including CE markings and EU Declarations of Conformity, can support your organization's due diligence process for integrated firmware components. Similarly, AMI's SBOM deliverables serve as a direct input into your organization's product-level SBOM generation. We expect that as your legal and compliance advisors assess your organization's specific CRA obligations, these connection points will be an important part of that analysis.

AMI's Commitment to Supporting Customer Compliance

AMI is committed to supporting customer compliance efforts through a number of concrete deliverables and commitments:

- **Integrator information and documentation.** As part of AMI's CRA compliance obligations, AMI will provide customers with the integrator information and instructions package contemplated by the CRA, including product security information, known cybersecurity risks relevant to integration, secure integration guidance, and support period information.
- **Vulnerability notification.** When AMI identifies or is notified of an actively exploited vulnerability in a firmware product, AMI will notify affected customers promptly and in sufficient time to support their regulatory reporting obligations under Article 14 of the CRA.
- **Conformity documentation.** As noted above, AMI intends to provide CE-marked firmware products with corresponding EU Declarations of Conformity, enabling customers to rely on AMI's conformity documentation in their due diligence processes.
- **SBOM delivery.** AMI intends to deliver product-level SBOMs with each firmware release and to keep SBOMs current throughout the applicable support period.
- **Support period commitments.** AMI will declare a support period for each applicable firmware product consistent with CRA requirements and reflective of that product's expected use lifecycle. Customers requiring extended support periods aligned with specific product deployment lifecycles should discuss this with their AMI account representative.

AMI expects these deliverables to be available within the regulatory timelines, with vulnerability reporting infrastructure operational by September 11, 2026, and full compliance deliverables available ahead of the December 11, 2027 deadline.

If you have specific questions about AMI's CRA compliance efforts or the information AMI can provide to support your compliance program, please contact AMI's CRA compliance team at security@ami.com or reach out to your AMI account representative.

Thank you for your continued partnership.

The AMI Cybersecurity and Compliance Team