Microchip's Commitment to the EU Cyber Resilience Act

At Microchip, we recognize the impact of the EU Cyber Resilience Act (EU CRA) on the digital product and software ecosystem. As a longstanding leader in secure systems—including MCUs, MPUs, FPGAs, SoCs, Secure Elements and Root of Trust Controllers—we have consistently provided robust cybersecurity and supply chain transparency across our global operations.

We fully support the EU CRA's objectives and are proactively aligning our business practices with its forthcoming requirements.

Our readiness efforts are well underway and deeply embedded into our ongoing security and compliance strategy. These include:

- Comprehensive Portfolio Evaluation: Assessing our entire product portfolio in the context of the CRA's classification framework to ensure full compliance.
- Secure Development Lifecycle: Advancing our secure development lifecycle and vulnerability management processes in line with CRA principles.
- Industry Engagement: Engaging directly in relevant standardization efforts to help shape and anticipate implementation best practices.

Some of the strengths we bring to this effort include:

- A Long History in Secure Systems: Our expertise spans secure MCUs, Secure MPUs, FPGAs, SoCs, Secure Elements and Root of Trust (RoT) controllers, reflecting our deep commitment to secure product design.
- Automotive-Focused Quality and Cyber Processes: We operate with ASPICE-compliant software processes and ISO 21434-certified cybersecurity practices, ensuring the highest standards for automotive applications.
- Secure Factory Programming and Provisioning Systems: Our manufacturing processes are designed to protect product integrity from inception through delivery.
- Robust Cyber Processes: We have established Product Security Incident Response Team (PSIRT) protocols, comprehensive vulnerability handling and maintain a detailed Software Bill of Materials (SBOM) for transparency and rapid response.
- Preemptive elimination of vulnerabilities: We rely on both internal testing as well as evaluation by accredited labs to identify vulnerabilities in our products. We are scaling our internal resources and embedding threat and risk assessments early in the product development lifecycle. This includes integrating penetration testing throughout the development flow to detect vulnerabilities as early as possible.

Microchip is dedicated to maintaining the highest standards of security, quality, and regulatory compliance. We view the CRA as an important evolution in our industry and an opportunity to further demonstrate our leadership in secure, resilient product development.

We will continue to provide timely updates as formal guidance is refined by the European Commission and national authorities. Should you have questions regarding specific products or our approach, please contact your Microchip sales or technical representative.