Your Team for EU CRA-Aligned Cybersecurity Service

usafirmware®

Take Action Now: Secure. Comply. Lead.

The European Union Cyber Resilience Act (EU CRA) marks a transformative shift in global cybersecurity expectations—introducing *mandatory*, enforceable cybersecurity requirements for all software and connected devices entering the EU market. **And, time is running out to comply by September 16, 2026.** USA Firmware offers an EU CRA-aligned service offering built to help US-based manufacturers meet the export hardware / software demands of the EU confidently and competitively—without overhauling your current software engineering maintenance contracts.

The EU CRA: More Than Maintenance

While ISO/IEC/IEEE 14764 outlines important software maintenance practices, the EU CRA introduces additional legal cybersecurity obligations that go far beyond ISO-based process guidance. It introduces **specific, measurable commitments** around cybersecurity, such as:

- Threat detection and response mechanisms
- Post-market vulnerability handling
- Supply chain transparency and documentation
- Secure software design principles
- Timely patching and updates

EU CRA violations can result in **significant fines, product bans, and reputational damage**. Your organization needs a partner who can integrate cybersecurity seamlessly into your software development lifecycle.

The Time Is Now. Know These Deadlines.

Product development takes time. Get started now understanding the timeline and EU CRA requirements that will impact your new device EU market entry. Here's what you need to know:

1. **In September 2026**, manufacturers must report exploited vulnerabilities. In order to do that, you should have already built some of the cybersecurity programs and protocols. This means you will need to regularly monitor for security issues, fix vulnerabilities quickly, report active exploits to ENISA within 24 hours, and notify users if their security is at risk. A conservative estimate for implementing and maintaining a vulnerability management process for a single connected product is approximately 0.5 to 1.0 Full-Time Equivalent (FTE) per year. This assumes your company already has a product security team and CI/CD infrastructure in place. If starting from scratch, the initial setup could push your Year 1 needs to 1.5+ FTE.
2. **On July 16, 2027**, full compliance becomes mandatory for all new products with digital elements placed on the EU market. All new connected products (hardware or software) introduced in the EU must comply with CRA cybersecurity requirements. Manufacturers must complete a conformity assessment (self-assessment or third-party, depending on product class).

Product requirements are as follows:

- Be secure by design and default
- Support automatic security updates for at least 5 years
- Be ready for 24-hour reporting of actively exploited vulnerabilities to ENISA
- Include vulnerability management processes
- Include a Software Bill of Materials (SBOM)
- Display a CE mark to enter the EU market

3. July 16, 2028, is the deadline for legacy products to comply with CRA.

Timeline Chart

Date	Event Description	Requirements at This Point	CRA Reference
Jan 16, 2025	CRA officially enters into force.	Begin planning and gap analysis. Appoint CRA compliance lead.	Article 57(1)
Sept 16, 2026	Start 24-hour reporting of exploited vulnerabilities to ENISA & CSIRTs.	Implement vulnerability management process, ENISA notification workflow, and Cyber Coordinated Vulnerability Disclosure (CVD) policy.	Article 11 & Article 15 / 57(2)
Jul 16, 2027	Full CRA compliance required for new products placed on the EU market.	Products must meet all CRA essential cybersecurity requirements and complete conformity process.	Article 57(1) + Chapter III & IV
Jul 16, 2028	CRA applies to existing products that receive significant updates.	Ensure updated legacy products comply with CRA before reintroducing to EU market.	Article 57(1), Recital 73

Cybersecurity Services Designed for EU CRA Compliance

With USA Firmware on your side, our EU CRA service offerings ensures your products not only meet regulatory expectations—but *surpass* them. We deliver modular, adaptable packages tailored to your current development and maintenance workflows. Our packages ensure your products meet CRA compliance.

USA Firmware CRA Packages

	CRA Essentials Package	CRA Lifecycle Package	CRA Advanced Cybersecurity Package
Basic Risk Assessment	Annual review to identify vulnerabilities		Everything in the CRA Essentials Package, plus these additional features:
Secure Defaults	Ensure software ships with compliant default configurations		Annual review to identify vulnerabilities
Rapid Patch Service	On-demand patch management for critical vulnerabilities		Ensure software ships with compliant default configurations
Continuous Monitoring		Real-time monitoring of vulnerabilities for full product lifecycle	Real-time monitoring of vulnerabilities for full product lifecycle
Regular Compliance Reporting		Quarterly updates to track CRA readiness	Quarterly updates to track CRA readiness
Lifecycle Risk Mitigation		Support for post-market and EOL planning	Support for post-market and EOL planning
Third-Party Dependency Incident Response			Proactive evaluation of software supply chain risks
Penetration Testing			Simulated attack assessments
Basic Risk Assessment			Annual security testing to uncover vulnerabilities
24/7 Managed Incident Response			Real-time support for security events
Optional Enhancement for Accuracy			Mandatory 24-hour ENISA reporting for exploited vulnerabilities (Article 11(1)): Manufacturers must notify the EU cybersecurity agency (ENISA) of actively exploited vulnerabilities within 24 hours
CE Marking Obligations for CRA Compliance			Conformity assessment and CE marking are required to demonstrate compliance, especially for higher-risk (Class I/II) products.

Why It Matters: The High Cost of Inaction

Failing to meet CRA requirements is more than a compliance risk—it's a business risk. Consider these **proof points**:

Legal Consequences: Non-compliance can lead to EU market exclusion, product recalls, or civil liability.

Financial Penalties: The official CRA Sanctions (Article 53) are a gradation of fines, which state:

- Up to €15 million or 2.5% of global annual turnover for intentional or negligent non-compliance with essential cybersecurity requirements (Articles 10–15).
- Up to €10 million or 2% for incorrect declarations, certification misuse, etc.
- Lower penalties for administrative failures.

Loss of Trust: Consumers and regulators alike demand transparency and action around software security. A vulnerability without a clear mitigation strategy is no longer tolerated.

Benefits Beyond Compliance

By adopting USA Firmware EU CRA services, you're not just avoiding regulatory penalties—you're **enhancing your brand's security posture**, market credibility, and customer trust.

Build Differentiation: Proactively complying with CRA gives your company an advantage over competitors lagging behind.

Drive Brand Value: Security is now a key product differentiator—especially in regulated markets.

Mitigate Risk: Lifecycle management reduces the cost and impact of vulnerabilities over time.

Your Road to EU CRA Compliance Starts Here

USA Firmware can help you meet the evolving expectations of global regulators with *precision-engineered* cybersecurity services that deliver more than box-checking—they deliver confidence.

Whether retrofitting your existing product line or designing your next innovation, we help you:

- Navigate CRA's legal landscape
- Maintain trust with regulators and customers
- Enhance security across the lifecycle
- Extend value beyond compliance

Partner with the team that understands EU-CRA obligations: USA Firmware. Together, we can help you integrate compliance, minimize disruption, and secure your place in the future of connected devices.

Contact Us Today!

Bob Scaccia
CEO
USA Firmware
bob.scaccia@usafirmware.com
(440) 570-1809

usafirmware.com

usafirmware®