From: Software Safety Institute (SSI)
March 31, 2026
To: European Commission

Re: Draft Commission Guidance on the Application of Regulation (EU) 2024/2847 (Cyber Resilience Act)

Dear Commissioners,

The Software Safety Institute (SSI) appreciates the opportunity to provide feedback on the draft guidance supporting implementation of the Cyber Resilience Act (CRA). We commend the Commission for advancing a coherent, product-centered approach to cybersecurity that more clearly assigns responsibility to manufacturers and begins to align software with established safety regimes in other critical sectors.

The draft guidance provides important clarification on scope, lifecycle responsibility, and the role of economic operators. It will meaningfully reduce ambiguity for market participants and support more harmonized enforcement across Member States. In particular, we view the emphasis on lifecycle obligations, vulnerability handling, and risk-based compliance as foundational steps toward a more accountable software ecosystem.

At the same time, we believe there is a critical opportunity to strengthen the guidance in ways that will enhance its long-term effectiveness as a safety regime. Our comments focus on ensuring that the CRA not only enables compliance, but also supports system-level learning, measurement, and continuous improvement across the software ecosystem.

1. Strengthening Cybersecurity Risk Assessments as a Measurable System

The guidance appropriately centers cybersecurity risk assessments as the primary mechanism for demonstrating compliance. However, as currently framed, these assessments are largely firm-specific, context-dependent, and narrative-driven. Without a degree of standardization, these assessments risk becoming compliance artifacts rather than tools for systemic insight and improvement.

The Commission may wish to encourage the use of structured, machine-usable formats for key elements of risk assessments—such as common metadata, standardized risk categories, and consistent representations of likelihood, impact, and mitigation measures. Such structuring would not require full harmonization of methodologies, but would enable aggregation, comparability, and analysis across products and sectors. This, in turn, would

support the identification of systemic risk patterns and strengthen the effectiveness of market surveillance and policy development. As such, we recommend that the Commission:

- Encourage or define a standardized structure for cybersecurity risk assessments, including common taxonomies for:
    - risk categories, with special consideration for specifying 'risk to whom' (e.g., business versus their customers versus the downstream public)
    - mechanisms for measuring this risk
    - mitigation types
- Promote comparability across products and manufacturers, enabling aggregation and analysis at the ecosystem level
- Clarify expectations for how risk assessments should be updated and versioned over time

2. Establishing Mechanisms for Aggregating Vulnerability and Incident Data

The guidance references vulnerability handling and reporting obligations, which are essential. However, these processes currently function primarily at the level of individual firms and incidents. Aggregation, therefore, is essential for moving from reactive response toward proactive risk reduction at scale. As such, we recommend that the Commission:

- Establish or signal intent toward aggregation of vulnerability and incident data across products and sectors
- Encourage machine-usable structured reporting formats that enable:
    - identification of recurring failure patterns
    - tracking of defect classes and insecure defaults
- Consider periodic publication of system-level analyses (e.g., recurring vulnerability patterns, common failure modes)

3. Creating Feedback Loops into Design and Baseline Expectations

A core strength of mature safety systems (e.g., automotive, aviation) is the existence of feedback loops from real-world failures into evolving design expectations; however, the current guidance does not yet clearly articulate such a loop. We propose the CRA functions not only as a compliance regime, but also as a continuous improvement system for software safety. As such, we recommend that the Commission:

- Explicitly state that insights derived from vulnerability and incident data should inform evolving baseline cybersecurity expectations
- Link data collected through CRA processes to:
    - future guidance updates

    - harmonized standards
    - procurement expectations

4. Advancing Independent Testing and Benchmarking Capacity

The effectiveness of market surveillance will depend significantly on the ability to validate product security in practice. Over time, such capabilities could enable more transparent, evidence-based assessments of product security, strengthening both enforcement and market incentives. While the guidance references enforcement and assessment, it does not yet define a clear vision for technical testing infrastructure. As such, we recommend that the Commission:

- Support the development of standing independent testing and evaluation capabilities for products with digital elements, focused on systemic software risk to customers and the downstream public
- Encourage the creation of standardized testing methodologies aligned with CRA requirements
- Explore mechanisms for public and comparative benchmarking of product security

5. Guardrails on Interoperability and Legacy Constraints

The guidance appropriately recognizes that interoperability requirements and legacy systems may limit the immediate adoption of state-of-the-art security measures. However, without additional guardrails, this flexibility risks becoming a persistent justification for insecure configurations or delay of implementation of customer safety mechanisms which will undermine long-term security outcomes. As such we recommend that the Commission:

- Require that such exceptions be accompanied by:
    - clear documentation of constraints
    - risk mitigation measures customers can implement, as well as the time, money, and resources required
    - time-bound plans or conditions under which constraints can be reduced
- Encourage periodic reassessment of whether such constraints remain necessary

6. Clarifying Responsibilities for Open Source Dependencies

The guidance provides helpful clarification on when free and open-source software falls within scope. However, modern software systems frequently rely on extensive open source dependencies. The Commission should consider additional elements to help address

systemic risk introduced through widely shared components. As such, we recommend that the Commission:

- Reinforce expectations that manufacturers are responsible for:
    - assessing and managing risks associated with incorporated open source components
- Encourage visibility into dependencies and associated risks to owners/operators, consistent with broader supply chain security practices

7. Clarifying the Treatment of AI Systems as Software Within the CRA Framework

The Commission may wish to further clarify the application of the CRA to artificial intelligence systems, starting from the premise that AI systems are software and should be treated as such within the scope of products with digital elements.

While the EU Artificial Intelligence Act establishes a complementary framework focused on model behavior and risk, AI systems are, in practice, implemented, deployed, and maintained as software products. As such, they inherit the same classes of vulnerabilities, insecure dependencies, and lifecycle risks that the CRA is designed to address. At the same time, AI-enabled systems introduce characteristics that may stress existing CRA constructs, including:

- Highly dynamic behavior and frequent updates
- Reliance on external models, datasets, and third-party services
- Expanded attack surfaces (e.g., model interfaces, prompt injection pathways, agentic workflows)

We recommend that the Commission clarify how core CRA obligations, particularly cybersecurity risk assessments, vulnerability handling, and lifecycle responsibilities, should be applied to AI systems in light of these characteristics. This includes ensuring that:

- Risk assessments explicitly account for AI-specific attack vectors and dependency risks
- Vulnerability handling processes incorporate model-level and data pipeline vulnerabilities
- Updates and modifications to AI systems are evaluated consistently within the CRA's framework for substantial modification

Clarifying this interplay will help ensure that AI systems are not treated as an exception to software security expectations, but rather as a category of software that reinforces the need for robust, evidence-based, and lifecycle-oriented security practices.

Conclusion

The CRA represents a significant and necessary shift toward treating software as a domain with safety implications and corresponding accountability. The draft guidance takes important steps in operationalizing that shift. To fully realize its potential, we encourage the Commission to strengthen the guidance in ways that:

- Enable measurement and comparability
- Support aggregation and analysis of system-wide data
- Establish feedback loops from failure to design
- Build the foundation for independent testing and benchmarking

These elements are critical to ensuring that the CRA evolves into a sustainable software safety system, one that not only enforces compliance, but also drives sustained improvements in software security outcomes across the market.

We would welcome the opportunity to engage further with the Commission on these issues and to support ongoing efforts to strengthen the evidence base and institutional infrastructure for software safety.

Respectfully submitted,

Lauren Zabierek, CEO and Co-Founder | lauren@softwaresafety.org
Bob Lord, Chief Strategy Officer and Co-Founder | lord@softwaresafety.org
Software Safety Institute