CECIP European Weighing Industry

Cybersecurity Updates without Breaking Conformity - Secure by Design, Compliant by Law

CECIP supports the objectives of the Cyber Resilience Act (CRA) and the Commission's efforts to provide practical guidance for its implementation. For weighing instruments and other legally regulated measuring instruments under Directive 2014/31/EU (NAWID) and Directive 2014/32/EU (MID), manufacturers face a risk of conflicting obligations: The CRA drives timely vulnerability remediation and frequent security updates over the product lifecycle, while legal metrology frameworks impose strict controls on changes to legally relevant software, including type examination maintenance and (In some cases) reverification before deployment in the field. This paper sets out CECIP's key concerns and proposes targeted clarifications for the Commission guidance to ensure cybersecurity obligations can be met without undermining legal metrology controls and trust in measurement.

30th March 2026

1. Purpose and context

The CRA establishes horizontal cybersecurity requirements for products with digital elements and emphasizes lifecycle obligations, including vulnerability handling, secure updateability, and risk-based compliance. CECIP members already integrate cybersecurity practices into the design and lifecycle management of weighing instruments, in line with software controls required under legal metrology directives. CECIP has no concerns with the objectives of the CRA but how its expectations interact in practice with the legal metrology regime governing conformity and software change control for verified measuring instruments.

CECIP's central message is straightforward: CRA compliance must be achievable without forcing manufacturers into legal uncertainty or procedural deadlocks under MID/NAWID—especially software updates after-market placement.

2. The core tension: lifecycle cybersecurity vs. metrological change control

2.1 CRA expectations

The CRA's logic is lifecycle-oriented: Manufacturers must ensure an appropriate level of cybersecurity based on risks, maintain vulnerability handling processes, and remediate vulnerabilities throughout the support period. This will, in practice, increase the frequency of cybersecurity-related software updates.

2.2 Legal metrology constraints (MID/NAWID practice)

For weighing instruments, software changes are not neutral maintenance actions. Many components are legally relevant or interact with legally relevant functions. Where a change affects legally relevant software - or cannot be excluded from doing so - legal metrology practice typically requires controlled procedures (e.g., notified body involvement, certificate maintenance, and in some cases reverification before deployment to instruments in use).
Resulting risk: CRA may require remediation quickly, while MID/NAWID can restrict or delay deployment - creating the possibility of noncompliance on one side or the other without clear interpretative guidance.

3. Key concerns based on industry experience

3.1 CRA drives more frequent updates; MID/NAWID limit when updates are allowed
The CRA increases the need for frequent security updates, while MID/NAWID impose strict controls on software changes - especially where legally relevant software is concerned - often requiring formal assessment before rollout. Without explicit clarification, stakeholders may assume CRA implies immediate deployment, while legal metrology may prohibit deployment until conformity steps are completed.

3.2 CRA may require updates even when metrology is not affected
Cybersecurity patches may be required even if essential metrological requirements are untouched. This expands the practical trigger for change beyond traditional legal metrology logic and creates uncertainty when metrological procedures must be initiated for cybersecurity-motivated updates.

3.3 Separation of legally relevant vs. non-relevant software becomes critical (and harder)
Legal metrology relies on software separation to permit changes to nonrelevant software without affecting the legally relevant part CRA driven updates often target operating system layers, libraries, or communication stacks which will inevitably lead to an interaction with legally relevant modules, raising the risk that cybersecurity changes inadvertently trigger metrological reassessment.

3.4 Timing mismatch: “timely remediation” vs. slower conformity workflows
CRA remediation expectations can be short, while conformity workflows (notified body review, documentation updates, and potentially reverification instruments already in the field) often take weeks or even months. Manufacturers need a recognized, compliant pathway when immediate patch deployment is legally constrained.

4. “Substantial modification” and software updates: Avoid misinterpretation for legal metrology

The CRA guidance explains “substantial modification” and indicates that security updates are generally not to be treated as substantial modifications under CRA criteria. CECIP notes that this CRA concept does not map one-to-one onto legal metrology practice. Even a security motivated change can be treated as metrologically relevant if it affects, or may affect, legally relevant software or its environment.

CECIP request: The guidance should explicitly clarify that CRA terminology (Including “substantial modification”) does not prejudge whether a change triggers legal metrology procedure under MID/NAWID.

5. What DG GROW should clarify in the final CRA guidance (CECIP recommendations)

- Explicit compatibility statement (CRA ↔ MID/NAWID change control); Clarify that CRA obligations on vulnerability remediation and software updates must be fulfilled in a manner compatible with MID/NAWID change control requirements for legally relevant software and verified instruments, including certificate maintenance and any required legal metrology steps prior to deployment.

- Legally constrained deployment: Recognition of interim mitigation measures: Clarify that where immediate patch deployment cannot be delivered because of MID/NAWID procedures, manufacturers may apply interim compensating measures (e.g., exposure reduction, configuration hardening, operational restrictions, user instructions) while completing required conformity steps, without being presumed noncompliant under CRA solely due to the deployment constraint.

- Software separation and impact assessment as a practical bridge Encourage architectures and documentation practices that support robust separation between legally relevant and nonrelevant software and enable transparent impact analysis for each cybersecurity update - recognizing that CRA driven patches may affect OS/libraries/communications components that interact with legally relevant functions.

- Avoid implied bypass of legal metrology controls Clarify that CRA guidance does not imply cybersecurity updates may be deployed in the field without respecting applicable MID/NAWID certificate maintenance, notified body processes, and (where applicable) reverification requirements if legally relevant software is impacted or cannot be excluded from impact.

- Interplay section: Explicitly cover legal metrology (MID/NAWID) in the guidance narrative. Include an explicit reference to legal metrology (NAWID/MID and

associated national verification regimes) within the “interplay with other legislation” part of the guidance to support harmonized interpretation and enforcement across Member States.

CECIP supports the CRA’s cybersecurity objectives and is ready to provide practical examples from the weighing industry to support workable, harmonized implementation. Clear and targeted guidance on CRA–MID/NAWID interplay will enable both policy goals: High cybersecurity throughout the lifecycle of connected products and continued trust in legally controlled measurement across the Internal Market.