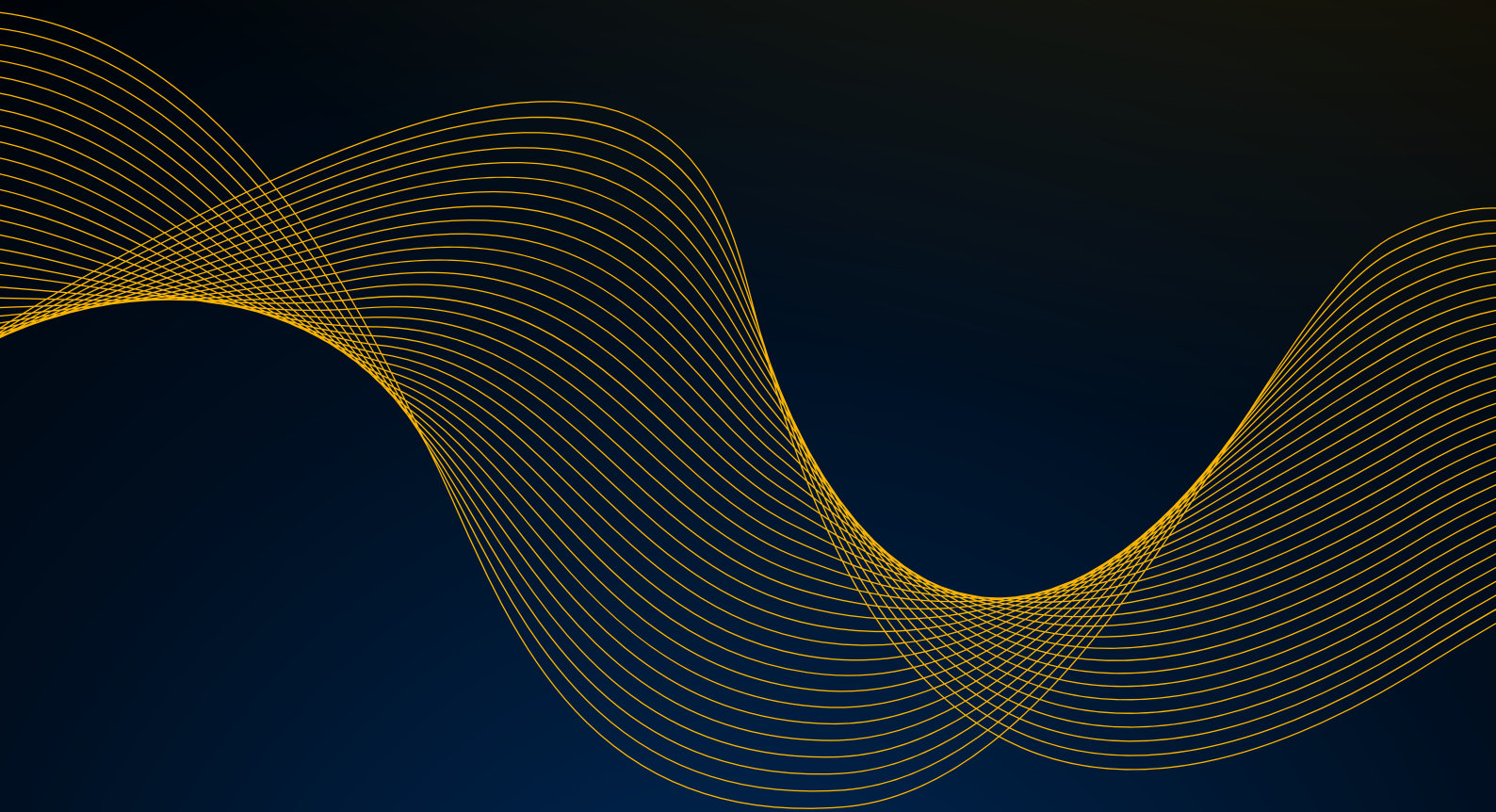
cecimo
European Association of Manufacturing Technologies

CECIMO'S POSITION ON THE REVISION OF THE EUROPEAN CYBERSECURITY ACT

JUNE 2025



CECIMO POSTION PAPER

www.cecimo.eu

CECIMO - representing European Manufacturing Technologies – welcomes the European Commission's initiative to revise the Cybersecurity Act (Regulation (EU) 2019/881). As set out in our 2022 publication, *Cybersecurity for the Machine Tool Industry*, the growing digitalisation of industrial equipment and processes has significantly increased both technical and business risks. Machine tool builders now operate in a cyber threat landscape where attacks can endanger data, disrupt operations, affect safety, and jeopardise intellectual property.

We strongly support the Commission's goals of strengthening cyber resilience, enhancing the operational role of ENISA and simplifying the EU's cybersecurity framework, in line with the 2025 EU Work Programme and the ProtectEU Strategy. It is essential for the machine tool industry that the revised Act reflects the realities of manufacturing, particularly for SMEs operating in complex, interconnected supply chains and managing long-life, high-value industrial equipment.

Drawing on the priorities outlined in our sectoral paper and feedback from our members, we submit the following targeted recommendations.

Recommendations

1.Strengthening ENISA's role in sectoral engagement and standardisation

ENISA should be given a clearer mandate to engage directly with the manufacturing sector through dedicated groups focused on operational technology (OT). These groups should address the specific cybersecurity challenges associated with industrial hardware and software systems. ENISA's guidance should go beyond traditional IT to provide bespoke threat intelligence, incident response and technical advice relevant to factory floor realities.

ENISA should also play a stronger role in coordinating inclusive EU-wide standardisation efforts to ensure that all Member States, both large and small, are equally represented and able to contribute to developing cybersecurity standards. Cybersecurity standards and norms risk reflecting only the perspectives of larger Member States with greater institutional capacity. Currently, larger Member States are disproportionately represented in technical working groups, which leads to the development of standards that favour national interests. For example, larger European economies reportedly allocate more experts to CRA standardisation processes, whereas smaller Member States often contribute none or just one expert. To avoid this imbalance, ENISA must be given more resources to coordinate inclusive, pan-European standardisation efforts together with industry associations and SMEs to ensure operational relevance across all Member States.

2. Simplifying and harmonising EU cybersecurity regulations

To ensure effective and sustainable compliance, the revision of the Cybersecurity Act must clearly define its relationship with other key EU regulations, including the Cyber Resilience Act (CRA), the NIS2 Directive, the AI Act, the GDPR, and the Machinery Regulation. While each framework has its own objectives, their overlapping provisions and conflicting interpretations create legal uncertainty, raise compliance costs, and hinder innovation, particularly for SMEs. CECIMO therefore urges the adoption of a harmonised approach that includes clear guidance on how these regulations interact, tools to map legal obligations, and practical resources adapted to business needs.

Additionally, European SMEs are at risk of being excluded from the EU market altogether due to the legal uncertainty and compliance burden imposed by regulations such as CRA, CSA and NIS2. This creates an uneven playing field, in which non-EU manufacturers, who are often able to bypass EU rules and benefit from limited market surveillance, can flood the market with non-compliant products.

As we have seen in the consumer space with platforms such as Shein and Temu, a similar threat is emerging at the B2B level. Without stronger enforcement and clarity, compliant EU companies could lose market share to competitors who do not follow the same rules.

CECIMO is also calling for the creation of a centralised EU platform, managed by ENISA, that would consolidate incident reporting, regulatory guidance, and compliance support. This platform would enable businesses to submit cybersecurity incident reports once only, automatically notifying the relevant national authorities and eliminating redundant reporting obligations while improving cross-border coordination. It would also provide a digital gateway for tracking compliance deadlines, receiving real-time alerts, and accessing up-to-date, sector-specific guidance.

A streamlined system like this is essential for reducing administrative burdens and avoiding a fragmented or two-speed regulatory environment. SMEs, in particular, often lack the resources to manage complex compliance requirements. The Cybersecurity Act should evolve into a coherent framework that integrates smoothly with related regulations while acknowledging the operational realities of businesses of different sizes. A one-size-fits-all approach would impose excessive costs on smaller firms and risk widening the gap between large companies and SMEs in terms of cybersecurity readiness. A system tailored to SMEs and delivered through a single, reliable contact point, would ensure fair access to compliance tools, support secure digital adoption, and strengthen cybersecurity resilience across the EU industrial landscape.

3. Making certification more practical and flexible

The current certification system needs to be practical, reliable and flexible because machine tools are complex, composed of many subsystems (e.g. HMIs, hydraulic units, third-party add-ons), and often in use for decades. Certification should continue to be voluntary and allow for component-level approval and support upgrades to legacy machines. Certification schemes should also align with standards such as ISO/IEC 62443, focusing on the cybersecurity of industrial automation. Simplifying conformity assessments through self-assessment options for lower-risk systems would reduce administrative burdens and empower manufacturers, who understand their own products best.

4. Improving cybersecurity across industrial supply chains

Modern machine tool operations rely on a complex network of original equipment manufacturers (OEMs), integrators, software vendors and users. Weak cybersecurity practices anywhere in this chain increase risk for all interconnected partners and subcontractors. We support the CSA revision's focus on supply chain security and recommend that ENISA provides sector-specific tools such as standardised risk assessments, a software bill of materials (SBOM) adapted for manufacturing and practical threat models based on real production scenarios.

In addition, recent discussions around the CRA have brought up a critical timing issue. OEMs often stock components that may not comply with the new cybersecurity rules by the time they come into effect. Meanwhile, suppliers may use the entire transition period to make their products compliant, leaving OEMs with the choice of either ensuring conformity themselves, which many are not equipped to do, or delaying production until compliant parts are available. To avoid supply chain disruptions, a two-tier or multiple-tier transition period could be useful, allowing for a more flexible transition period with different phases that reflect the practical realities of industrial supply chains.

5. Creating centralised EU contact points for companies' support

In parallel, we advocate for the creation of a permanent, dedicated support service, such as an email helpdesk or telephone line, where companies can seek practical, trustworthy guidance on compliance with the CRA and related regulations.

This service could be overseen by ENISA or a competent authority and be accessible long-term, not just during the rollout phase. SMEs in particular would benefit from such support, as they often lack the internal resources to interpret complex legislation. By providing authoritative advice with legal standing, this service would help ensure consistent understanding of cybersecurity obligations across the EU, reduce compliance risks, and foster greater confidence in regulatory implementation.

6. Providing free, practical cybersecurity training

Workforce training, especially for operators and technicians, is a critical weak spot as skills shortages and a lack of basic cybersecurity awareness pose significant risks. ENISA should collaborate with industries to develop modular training programmes, tailored to sector-specific needs and interactive exercises on topics such as phishing, password security and machine updates. These resources should be distributed through national associations and linked with broader skills development programmes to ensure relevant and accessible training across all Member States.

Revising the Cybersecurity Act is an opportunity to create a stronger, more secure industrial Europe. However, to succeed, it must be shaped around technical realities and different sectors, such as advanced manufacturing. This requires adopting smarter, more flexible certification processes, investing in targeted training, supporting sector-specific implementation and providing practical tools to help SMEs comply without creating an unnecessary burden. With the right approach, the updated Act could safeguard Europe's industrial future by making it more secure, competitive and inclusive for companies of all sizes.

For more information please contact:

Name	**Olha HUNCHAK,** **Technical and Digital Policy Manager.**
Email	**olha.hunchak@cecimo.eu**

About CECIMO:

CECIMO is the European Association of Manufacturing Technologies. With a primary focus on machine tools and additive manufacturing technologies, we bring together 15 national associations representing approximately 1500 industrial enterprises in Europe (EU + UK+ EFTA + Türkiye), over 80% of which are SMEs. CECIMO covers 97% of the total machine tool production in Europe and about 1/3worldwide. It accounts for approximately 150,000 employees and a turnover of around 25.8 billion euros in 2024.

CECIMO Members

Austria: Metaltechnology Austria
Die MetalltechnischeIndustrie

Germany: VDW
Verein Deutscher
Werkzeugmaschinenfabriken e.V.

Sweden: MTAS
Machine and Tool Association of Sweden

Belgium: AGORIA
The Federation of Technology Industry

Italy: UCIMU
Associazione dei costruttori Italiani di macchine utensili robot e automazione

Switzerland: SWISSMEM
Die Schweizer Maschinen-, Elektro- und Metall-Industrie

Czech Republic: SST
Svazu Strojírenské Technologie

Netherlands: FPT-VIMAG
FederatieProductieTechnologie / Sectie VIMAG

Türkiye: MIB Makina
Imalatcilari Birligi

Denmark: The Manufacturing Industry
a part of the Confederation of Danish Industry

Portugal: AIMMAP
Associacão dos Industriais Metalúrgicos, Metalomecãnicos e Afins de Portugal

United Kingdom: MTA
The Manufacturing Technologies Association

Finland: Technology Industries of Finland

Spain: AFM Cluster
Asociación española de fabricantes de máquinas-herramienta, accesorios, componentes y herramientas

France: Evolis
Organisation professionnelle des biens d'équipement