11 May 2026

Revision of the Cybersecurity Act

ESMIG's position on the trusted ICT supply chain framework

ESMIG strongly welcomes the revised Cybersecurity Act (CSA), presented by the European Commission on 20 January 2026, and particularly the new trusted ICT supply chain framework with its provisions on de-risking ICT supply chains. Cybersecurity is no longer only a technical compliance issue but a matter of critical infrastructure resilience and economic security, especially in the current geopolitical context. By introducing the concept of "high-risk suppliers", the revision of the CSA paves the way for greater scrutiny in the protection of Europe's critical infrastructure.

The Advanced Metering Infrastructure (AMI), comprising smart meters and supporting communication and data systems[1], is part of the smart grid critical infrastructure. As the interface between the consumer and the grid, smart meters control energy flows, manage sensitive consumption data, and can be remotely accessed. Allowing suppliers linked to

[1] Smart meters are an integral component of modern electricity systems and form part of Advanced Metering Infrastructure (AMI), which relies on large-scale, interconnected ICT infrastructures for metering, communication, remote management, and system control. Due to its scale of deployment, long operational lifecycles, and dependence on centralized governance for software updates, cryptographic key management, and remote access, AMI is exposed to systemic cybersecurity and non-technical risks.

high-risk third countries to access the internal market, and creating external technology vendor dependencies, can create long-term vulnerabilities for Europe's critical infrastructure and pose a direct threat to Europe's energy security and strategic autonomy.

The smart metering sector is therefore a key test case. With around 300 million smart meters projected to be deployed across the EU27+3 (United Kingdom, Norway and Switzerland) by 2030[2], procurement decisions made today could lock in dependencies on potentially high-risk third-country suppliers, with associated non-technical cyber and geopolitical risks, for 15 years or more.

Both in its Policy Manifesto (May 2024) and its Position Paper on Fair Competition (June 2025), ESMIG has consistently called for the identification and, where necessary, exclusion of high-risk suppliers from EU critical energy infrastructure procurement. The revised CSA's trusted ICT supply chain framework is the most concrete legislative response to this call. We therefore strongly welcome the provisions laid out in Articles 98 to 107 and Articles 112 to 115 of the revised CSA.

ESMIG proposes a set of changes to the CSA's trusted ICT supply chain framework to pursue the following three objectives:

- First, to ensure that the framework is fit for purpose to reflect the concerns relating to AMI.
- Second, to strengthen key procedural provisions so that the framework is effective and cannot be delayed or circumvented: ESMIG has seen how procurement timelines move faster than regulatory processes, and some amendments address this directly.
- Third, to ensure mitigation measures are calibrated to the specific risk profile of AMI, including software and firmware integrity, remote management architecture, and cryptographic key control. These risk vectors, absent from the current text, are central to the cybersecurity of large-scale smart metering deployment.

ESMIG recognises that the revised CSA operates alongside other key instruments for the smart meting sector — the Foreign Subsidies Regulation, the Net-Zero Industry Act, the Industrial Accelerator Act and the upcoming review of the EU Public Procurement Directives

[2] Berg Insight, *Smart Metering in Europe, 19th Edition* (Berg Insight, March 2025), https://media.berginsight.com/2025/03/20120551/bi-sm19-ps.pdf

— on which ESMIG has separately issued its position. The CSA's supply chain provisions and focus on ownership and control of entities are however the most direct and powerful tool yet to address non-technical cybersecurity risks. These risks increasingly pose a concern, also in light of market distortions due to the absence of a true international level-playing field which ESMIG has called the EU to address.[3]

A coherent, cross-instrument approach is ultimately needed. The following changes proposed by ESMIG are intended to ensure that the CSA contributes as effectively as possible to this broader framework:

- **Explicit inclusion of electricity grid digitalisation technologies.** The CSA should clarify in Recital 133 that referenced 'electricity supply systems' explicitly include electricity grid technologies and technologies to digitalise the grid. This provides clarity that cybersecurity de-risking measures apply consistently to smart electricity grid infrastructures, including advanced metering infrastructures and smart metering systems, and support coherent supervision across Member States.
- **Accountability for delays in completing security risk assessments.** While Article 99 provides for a six-month deadline for completing coordinated security risk assessments, it does not establish any obligations or consequences in the event of delays. Given the urgency of cybersecurity threats and the potential geopolitical pressure against the implementation of the supply chain provisions, ESMIG proposes to introduce three safeguards where the Commission fails to meet the deadline:
  (a) an obligation to report to the European Parliament and Council on the reasons for the delay;
  (b) a precautionary measure whereby the ICT supply chain assets identified in the request are temporarily treated as high-risk until the assessment is complete; and
  (c) a possibility for the NIS Cooperation Group, in consultation with ENISA, to adopt a provisional assessment pending completion of the full assessment.
- **Additional criterion for designating third countries posing cybersecurity concerns.** While Article 100 establishes criteria for identifying a third country as potentially posing cybersecurity risks, it does not sufficiently address all forms of

[3] European providers of smart energy solutions have been confronted for years with unfair competition from some third-country suppliers whose artificially low prices, possibly underpinned by third-country subsidies and export credits, have allowed some third-country suppliers to gain a significant and growing foothold in the EU market.

interference that a third country may exert. ESMIG proposes introducing an additional criterion covering situations in which a third country exercises decisive influence over an entity, through laws, regulations or established practices that allow that State to control, access or require disclosure of critical data, vulnerabilities or sensitive information related to digital infrastructure. This broadens the scope for identifying when a third country may pose a non-technical cybersecurity risk.

- **Differentiated treatment of new procurement and installed equipment.** This ensures that prohibitions and mitigation measures are applied in a proportionate and operationally feasible manner by distinguishing between new procurement — subject to immediate prohibition from the date of entry into force of the relevant implementing act — and ICT components already installed or integrated in key ICT assets, which shall be subject to risk-based mitigation measures and phase-out obligations on a timeline established by the Commission. In establishing that timeline, the Commission shall consider the residual operational lifecycle of the relevant assets and the availability of replacement supply from non-high-risk suppliers. This provides legal certainty for immediate de-risking of future investments while allowing for phased replacement of existing systems, thereby safeguarding continuity of essential services.
- **Strengthened supervisory powers for procurement and operational compliance.** ESMIG proposes to clarify in Article 114 the supervisory powers of competent authorities by specifying that requests for supplier information may cover elements necessary to assess dependency, control or exposure to non-technical risks in the procurement and operation of electricity grid technologies or technologies to digitalise the grid. This is particularly important for smart metering and AMI systems, where supply-chain risks are determined at procurement stage and through system-level dependencies, and where effective supervision requires the ability to assess the full picture of vendor control and access arrangements.

The revision of the CSA presents a critical opportunity to enhance cybersecurity resilience across the Union. By addressing the issues outlined above, the European Commission can create a stronger and more resilient framework for businesses and citizens. We encourage the Commission to consider these recommendations and look forward to contributing to the development of effective and comprehensive legislation.