The European Commission's New Cybersecurity Package

Review

January 2026

H/ADVISORS

The Cybersecurity Package: An Overview

On 20 January 2026, the European Commission published its new Cybersecurity Package, composed of a revised Cybersecurity Act, together with targeted amendments to the Directive on a high common level of cybersecurity (NIS2), which sets cybersecurity requirements for sectors of high criticality (e.g. financial institutions, the energy sector, transport, etc.).

The Package is based on four key pillars:

- **Revising the European Cybersecurity Certification Framework**, ensuring that future cybersecurity certification schemes are adopted faster and with greater transparency.
- **Reviewing the role of the European Union Agency for Cybersecurity (ENISA),** providing it with a broader mandate and scope of action.
- **Securing supply chains** by creating a list of high-risk vendors and setting up specific restrictions for such actors.
- **Simplifying the compliance burden** for entities under NIS2.

Overall Significance

The file sets up a regime for high-risk vendors from risky third countries - clearly aimed at reducing dependency on actors such as China, rather than Western partners - which will be restricted from several opportunities, including:

- Participation in European standardisation activities;
- Participation in public procurement processes for key ICT assets;
- Participation in Union funding programmes that support the provision of ICT components used in critical ICT assets;
- Limitations on the provision of ICT services and components to certain important and essential entities under NIS2 (with specifics to be defined on a sectoral basis).

The Package also establishes a new framework for cybersecurity certification schemes, including plans for a certification scheme for entities, aimed at simplifying compliance. Although schemes remain voluntary, they may be made mandatory through other legislation, including under NIS2, making certification a strategic asset. As high-risk vendors are barred from such schemes, the review poses an almost existential threat to these entities.

Scope

The file is primarily relevant to:

- **ICT service providers,** not only those providing cybersecurity services or products, but any entity providing services to important or essential entities under NIS2;
- **Important or essential entities under NIS2,** which may use cybersecurity certification schemes to meet compliance requirements and will have to abide by the new restrictions on high-risk vendors;
- **ICT providers from high-risk third countries,** which are on track to be barred from significant European market opportunities.

In More Detail

Supply Chains

- **Non-technical risk defined:** A precise definition is introduced for "non-technical cybersecurity risk," clarifying that it refers specifically to suppliers subject to influence by a third country. This makes it easier to distinguish between technical and non-technical requirements.
- **High-risk vendors:** A process is established for designating high-risk vendors in the European Union, linking them to specific third countries. Countries are to be assessed, inter alia, on the basis of the existence or absence of "democratic controls." While the definition is clearly aimed at China at present, it could in the future be used to capture a wider range of states.
- **Clear prohibitions for high-risk vendors:** High-risk vendors are barred from public procurement for ICT in key assets, from participation in certain funding programmes, and from obtaining cybersecurity certification schemes.
- **Member State variations:** This regime is without prejudice to Member States putting in place more stringent supply-chain rules.
- **New rules for digital networks:** Key ICT assets for mobile, fixed, and satellite electronic communications networks must phase out components supplied by high-risk vendors within 36 months of publication of the revised Cybersecurity Act.

Cybersecurity Certification Schemes

- **Revised certification framework**: Timelines within schemes are clarified and delimited; procedures for maintenance and withdrawal are clearly defined; and the scope of schemes is explicitly limited to technical requirements.
- **High-risk vendors:** High-risk vendors are banned from accessing cybersecurity certification schemes.
- **Cybersecurity skills:** A new framework is created for the certification of cybersecurity skills, aimed at ensuring workforce mobility and cross-border recognition.
- **International recognition:** The European Commission is empowered to adopt implementing acts for mutual recognition.

Simplification of Compliance

Under the targeted amendments to NIS2:

- The Commission is to develop guidelines on supply-chain management;
- A new reporting requirement is introduced for ransomware incidents;
- ENISA is tasked with carrying out a cross-border risk assessment relating to NIS2 entities, focusing on exposures such as concentration risk.

Next Steps

The file will now go through the legislative procedure in the European Parliament and the Council. As currently drafted, the revised Cybersecurity Act is expected to enter into force the day following its publication and to become directly applicable across Member States.

The file is expected to be controversial, both among industry stakeholders and policymakers.

On the Council side, the new responsibilities assigned to ENISA are unlikely to be warmly received, as Member States have increasingly expressed concerns about what they see as the Agency encroaching on national competences.

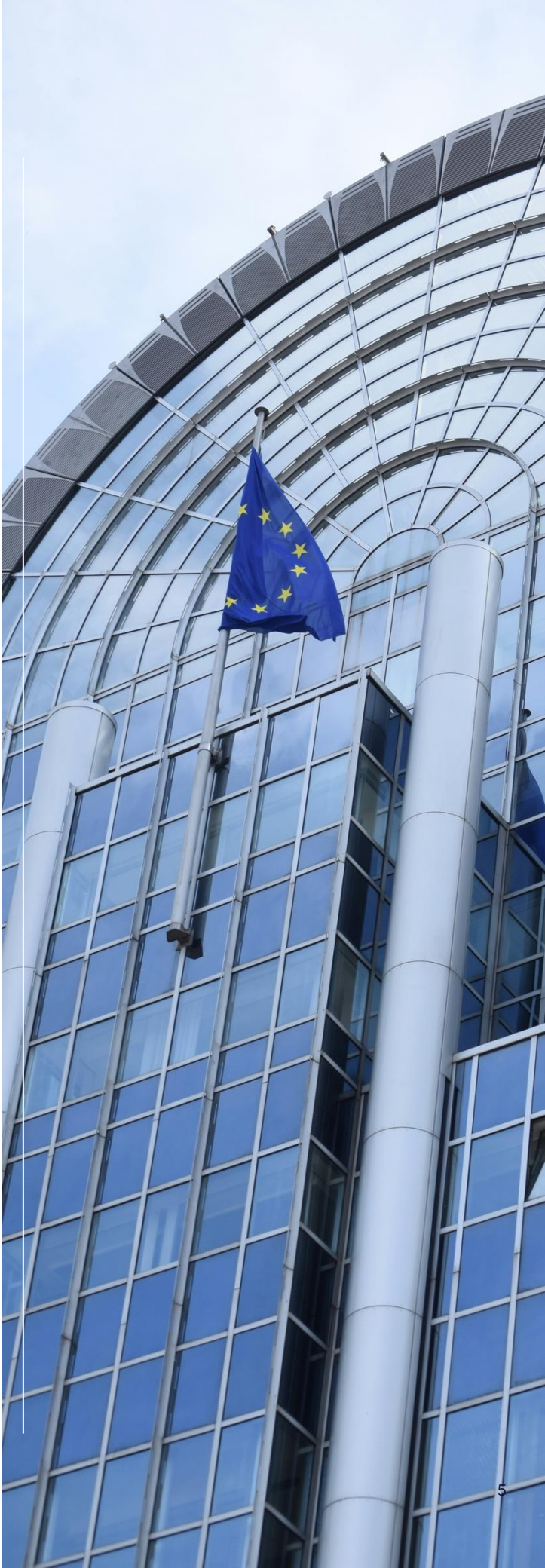
The European Parliament, while unlikely to oppose the designation of high-risk entities per se, may seek increased transparency in the designation process in order to prevent perceived Commission overreach.

For industry, pushback is likely to focus on supply-chain risk provisions, particularly the restrictions on the provision of services to NIS2 entities.

If you have any inquiries, please contact the team in Brussels.

Helena Walsh, CEO
helena.walsh@h-advisors.global

Cristina da Costa Ferreira, Consultant
cristina.da-costa-ferreira@h-advisors.global



Thank you

H/ADVISORS