DIGITALEUROPE

12 MAY 2026

EU cybersecurity rules: fixing certification, supply chains and critical entities

Executive summary

In the recent years, the EU has built one of the world's most ambitious regulatory frameworks for cybersecurity, driven by rising cybersecurity risks. The challenge the newly proposed cybersecurity package must meet is to make it work in practice.

The Cybersecurity Act 2 (CSA2) should position ENISA as a trusted EU coordination hub and make the European cybersecurity certification framework useful.[1] With a hardened state of international affairs, the ICT supply chain security framework is a positive step to mitigate non-technical risks; the current proposal, however, can result in far-reaching measures and must lay out a clearer, more predictable procedure, including stakeholder involvement.

Targeted amendments to the NIS2 Directive respond minimally to deep concerns industry has raised over the past years and are welcome.[2] More rigorous harmonisation is needed to simplify different national rules on scope, stricter national requirements, multiple supervisory authorities, varying conformity assessment obligations and inconsistent compliance timelines.

On ENISA's role:

- ENISA should conduct impact assessments for, and coordinate the implementation of, all relevant EU legislation to help develop a more coherent EU cybersecurity framework.
- The expanded role in mutual assistance should safeguard the strong partnership with industry.
- ENISA should support EU cybersecurity standardisation by advising and coordinating within existing standardisation processes, avoiding parallel technical specifications that would weaken harmonised standards and international alignment.

On the European cybersecurity certification framework:

- Schemes should remain voluntary and provide evidence of compliance with EU legislation to ensure they play a meaningful role.
- Mature international and European standards should be used wherever possible, with new schemes developed only to fill clear gaps.

[1] COM(2026) 11.

[2] COM(2026) 13.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

- A meaningful advisory structure should replace the misused Stakeholder Cybersecurity Certification Group (SCCG) to improve transparency and quality.
- Any extension profiles to schemes should be technical, proportionate, justified by specific uncovered risks and designed to avoid national overlays or market access barriers.

On the ICT supply chain security framework:

- ICT supply chain measures should remain proportionate, applying only where clearly identified non-technical cybersecurity risks cannot be mitigated through existing EU rules, and where impacts have been thoroughly assessed.
- A structured consultation mechanism with affected companies should be introduced, to ensure risks are properly understood, measures are feasible and unintended market disruption is avoided.
- Risk assessments and high-risk designations changes should follow a clear, evidence-based process with clear criteria, thresholds, timelines and meaningful Member State involvement.

On NIS2:

- NIS2 should be further harmonised across all entities, including scope, size thresholds, incident reporting, classification, main establishment rules and conformity assessment requirements.
- Scope should focus on core business activities only, excluding ancillary operations, to avoid disproportionate obligations.

Table of contents

Cybersecurity Act 2

ENISA's mandate

The expansion of ENISA's role within the cybersecurity framework is necessary. Particularly, its systemic advisory role in the development and consistent implementation of EU cybersecurity policy is key to ensure a streamlined framework across the bloc. To become a genuine operational hub at EU level, several adjustments are needed.

Security impact assessments

Nearly all legislation directly or indirectly affects digital systems and cyber infrastructure. Without careful consideration, new laws can unintentionally expand attack surfaces, create new vulnerabilities and weaken Europe's cybersecurity.

ENISA should therefore conduct mandatory, independent cybersecurity impact assessments for all relevant new EU legislation, including its implementation and enforcement. This would help identify cyber risks from the start, avoid unduly compliance burdens and support a more coherent EU cybersecurity framework.

Mutual assistance

The proposed NIS2 amendments give ENISA a greater enforcement role in mutual assistance, allowing it to participate in joint supervisory actions for entities operating across multiple Member States.[3]

ENISA is seen by industry as a trusted partner. Granting it enforcement powers could discourage companies from reporting incidents openly and undermine the existing public-private partnership model at large. The strong, partnership-based approach we currently have should be preserved.

Standardisation

ENISA's involvement in technical standardisation activities should support, not replace or weaken, the work of the European standardisation organisations (ESOs) and international standardisation bodies. Harmonised standards remain the most favourable route for demonstrating compliance and ensuring consistency across Member States. Any bottlenecks in their development, including delays in standardisation requests, limited resources and weak international alignment, should be addressed in a broader reform of Europe's standardisation framework.[4]

ENISA can assist the Commission by assessing draft harmonised standards and acting as a bridge between policymakers and the standardisation community. However, the drafting of technical specifications, which could be *de facto* common specifications, in support of EU legislation should remain with ESOs. They have established, transparent and inclusive processes, strong links with international bodies such as ISO and IEC, and the technical expertise needed to build market-relevant consensus. Allowing ENISA to develop

[3] Art. 37(a) of the proposal.

[4] See DIGITALEUROPE, A European standardisation system fit for global influence, available at https://cdn.digitaleurope.org/uploads/2025/11/A-European-standardisation-system-fit-for-global-influence.pdf.

alternative technical specifications, including for cybersecurity certification schemes, risks duplicating work, weakening stakeholder balance and creating parallel standards.

The Commission's proposal allows ENISA to participate in standardisation activities, including by drafting contributions, whilst also tasking it with helping the Commission assess draft harmonised standards. This creates a conflict of interest. The legal text should reflect Recital 41 unequivocally: ENISA should not help draft standards it is later responsible for assessing, to prevent it from grading its own homework.[5]

A clear separation must be maintained between legislation, standard-setting and conformity assessment. ENISA, the Commission, ESOs and other stakeholders should cooperate in a transparent way to preserve checks and balances and ensure high-quality technical outcomes.

The Standardisation Regulation already allows, through a transparent process involving a Multi-Stakeholder Platform (MSP), the identification of ICT technical specifications developed by recognised standards developing organisations.[6] At present, this mechanism is limited to public procurement. Extending it to regulatory compliance would give companies an additional, industry-driven pathway to demonstrate conformity where harmonised standards are not yet available, whilst preserving the primacy of harmonised standards. This could find support from industry, provided two conditions are met:

1. It enables quick recognition of relevant international standards and technical specifications; and
2. It operates through the MSP, ensuring transparency, inclusiveness and continuity, rather than establishing a separate expert group. As an MSP member, ENISA would be well placed to lead the cybersecurity-specific work within this framework.

The Network Code on Cybersecurity (NCCS)

The NCCS is a sector-specific delegated regulation on cybersecurity for cross-border electricity flows.[7] Whilst it complements NIS2, the CSA2 should further harmonise its implementation. A stronger ENISA could support the NCCS through threat intelligence sharing, best-practice guidance, pan-European coordination and, eventually, EU-wide network codes.

European cybersecurity certification framework

Changes to render the certification framework effective are most welcome. Certification should be a practical tool to simplify compliance with cybersecurity requirements and strengthen trust in certified entities. Several outstanding issues still must be resolved to make sure certification is genuinely useful to all parties.

By focusing the certification framework on the technical integrity of ICT products and services, and addressing non-technical risks separately, a consistent and objective certification process is safeguarded.

Voluntary certification and legal certainty

European cybersecurity certification schemes should be a trusted tool for demonstrating compliance. Where an entity chooses to certify a product, service or process under an EU scheme, that certificate should be

[5] Art. 18(7) attempts to mitigate this conflict of interest but is vague.

[6] Regulation (EU) No 1025/2012.

[7] Commission Delegated Regulation (EU) 2024/1366.

accepted as fully sufficient evidence of meeting the relevant legal requirements, without additional or duplicative national demands. The CSA2 should prevent Member States from introducing national schemes that are more stringent than EU-level schemes.

To deliver this simplification, the use of schemes must remain voluntary, including under the CRA and NIS2. Currently, the Commission's proposal leaves the possibility for Member States to mandate schemes, which will only add burden and fragmentation.

Schemes should remain flexible enough for complex or legacy hardware. Where requirements are overly rigid or technically incompatible, companies may be unable to achieve certification without disproportionate cost or redesign, effectively blocking compliant products from the market. Ultimately, an entity itself should decide if certification is the most appropriate compliance pathway.

Clearly delineate the use of extension profiles

Extension profiles add security requirements beyond the core scheme. They should be narrowly defined and used only in clearly justified cases.

Any extension profile should address a specific technical risk that is explicitly not adequately covered by other requirements. It should build on existing assurance levels to avoid parallel or divergent requirements and remain strictly technical in nature.

An extension profile should be a minimal and proportionate delta from the highest assurance level, defined at EU level under ENISA's technical lead. Strong safeguards are needed to ensure they do not turn into market access conditions in individual Member States.

Build on international and European standards

European cybersecurity certification schemes should be built around mature European and international standards. Certification schemes should fill gaps only where no suitable standard exists, and should not duplicate, contradict or dilute recognised frameworks such as ISO/IEC-based standards.

This is essential for competitiveness. Digitally enabled products are often mass produced and depend on predictable, scalable requirements. Certification also creates significant costs, from product design changes to documentation, tooling, audit evidence and third-party assessment. Where entities already hold internationally recognised certifications covering equivalent requirements, EU schemes should provide a presumption of conformity or a reduced assessment scope.

Focus cyber posture certification on specific business activities or services

Harmonising risk management measures under NIS2 is central to making EU cybersecurity requirements manageable. However, before any cyber posture certification scheme is developed, existing international and European standards should be leveraged to avoid duplicating existing and well-functioning mechanisms.[8]

[8] Cybersecurity schemes for critical infrastructure, such as data centres, should also be mutually recognised across Member States. Additional national requirements should be strictly limited to avoid fragmentation, redundant infrastructure and inefficient use of scarce resources such as microchips

Ultimately, if a cyber posture scheme is deemed necessary to fill any gaps, it should focus on specific business activities, services, assets and functions, rather than applying to an entire organisation by default. This would better align the certification with NIS2. This is especially important for large, diversified companies, where one business unit may provide NIS2-regulated services whilst another may offer lower-risk consumer services.

Clarify expectations for verification of technical documentation at higher assurance levels

Higher assurance levels, such as 'substantial' and 'high,' are intended to generate greater confidence in the security of certified products. However, Recital 103 should be clarified to avoid suggesting that all security-relevant properties described in technical documentation must be exhaustively verified. Such an interpretation would make certification disproportionately complex and costly, especially for highly sophisticated or frequently updated systems.

Ensure transparency of technical specifications

Technical specifications underpinning European cybersecurity certification schemes should, by default, be publicly available to ensure transparency, predictability and market trust.

Any cases of restricted access should be clearly justified, and in all circumstances, provision of those details should be made free of charge. Certification schemes should not rely on non-public or restricted technical specifications as mandatory elements, as this would undermine legal certainty, equal access and effective market participation. Where genuinely sensitive information is identified, this could instead be handled through separate, non-binding advisory mechanisms with controlled access for relevant authorities and operators, without forming part of the certification criteria themselves.

Introduce meaningful stakeholder consultation

Schemes won't be practical and implementable without meaningful stakeholder consultation. Regrettably, the body introduced by the CSA to this end, the SCCG, was not involved effectively in the framework and in individual schemes and has now been deleted entirely. The proposed European Cybersecurity Certification Assembly, meeting only annually, cannot be fit for this purpose. The certification framework should include a permanent advisory structure with strong industry participation, greater transparency on draft schemes and decision-making timelines, and the ability to issue non-binding opinions. Existing models, such as the CRA Expert Group, could provide a useful example.

Transitional provisions

Existing certificates issued under national schemes should remain valid until their expiry date. This 'grandfathering' approach protects past investments and provides legal certainty for vendors.[9]

The phase-out of national schemes should depend on the readiness of the European certification ecosystem and be based on clear timelines, to be reflected in Art. 86(1).

---

and clean energy. This would support secure, resilient and resource-efficient deployment across Europe.

[9] Art. 86(3) of the proposal.

Moving beyond IT security: certification for industrial products, systems, processes and services

There is currently no EU-wide certification framework that adequately reflects the risks, architectures and operational realities of industrial environments. The certification roadmap should therefore include targeted schemes for industrial products, systems, processes and services where there is clear added value and appropriate standards do not exist yet. This is without prejudice to the fact that harmonised standards remain the preferred tool for compliance with market access legislation.[10]

These schemes should be based on recognised sector-specific international standards.[11] This would support international recognition of European products and strengthen their competitiveness in non-EU markets. Specifically, ENISA should be tasked with supporting existing, and where absent, developing:

- A certification for industrial products;
- A certification for industrial systems based on EN IEC 62443-3-3;
- A certification for security processes (secure development lifecycle) based on IEC 62443 /EN IEC 62443-4-1;
- And a certification for service providers based on IEC 62443 /EN IEC 62443-2-4.

Certification should reflect modern realities

In addition, certification must reflect the realities of modern software development.[12] Static recertification cycles can create a 'security paradox,' where a certified product becomes outdated whilst a more secure patched version lacks certification. Certification should evolve towards a continuous conformity model that accounts for updates, patches and vulnerability management, making it a market-oriented, meaningful indicator of security rather than a barrier to innovation.[13]

ICT supply chain security

Rapidly evolving cyber threats justify appropriate security measures. On the one hand, technical risks are rightly addressed by, amongst others, NIS2, the CRA and DORA.[14] On the other hand, a macro-level European approach to strengthening ICT supply chain security across critical sectors addresses the growing need to tackle non-technical vulnerabilities linked to suppliers who present elevated risk profiles.

The creation of an ICT supply chain security framework, separate from technical certification and anchored in risk-driven methodology, is a significant step forward. An EU-wide approach minimises fragmentation and provides more predictable conditions. However, as its scope expands to a wide range of companies,

[10] Such as the Cyber Resilience Act (CRA, Regulation (EU) 2024/2847) and the Medical Devices Regulation (MDR, Regulation (EU) 2017/745).

[11] In particular, the EN IEC 62443 series for industrial control systems and supervisory control and data acquisition.

[12] The common criteria–based Cybersecurity Certification (EUCC) scheme, specifically.

[13] Moreover, such certification should integrate best practices and data from critical open source mechanisms such as a Software Bill of Materials (SBOM) for component dependencies, as well as Coordinated Vulnerability Disclosure (CVD).

[14] Regulation (EU) 2022/2554.

proportionality must remain central. Measures should not go beyond what is necessary to mitigate structural, non-technical cybersecurity risks in critical supply chains.

In this context, several issues require further attention.

Proportionality

Restricting or banning high-risk vendors is a justified measure when the underlying risk cannot be effectively mitigated with technical measures prescribed in comprehensive operational resilience and product security requirements under EU law.

The CSA2 proposal rightfully states that any mitigating measures should be based on the assessment of risks and dependencies, including the potential economic and societal impact of such measures on the entities concerned. Where non-technical risks demand non-technical responses, the design of such measures must preserve both security and market stability:

- The availability and maturity of trusted alternative vendors or technologies should be confirmed before any restrictions take effect.
- Transition periods must be sufficient, reflecting operational continuity requirements, economic consequences and technical feasibility.
- Economic impact assessments must capture the full scope of associated costs. This includes contractual obligations, the lifecycle of affected components within key ICT assets and the reconfiguration of multilayered ICT supply architectures. Interventions should be reserved for situations involving clearly identified and active cybersecurity threats, where the gravity of the security risk demonstrably outweighs the potential consequences of market disruption.
- To ensure such powers remain exceptional and proportionate in their application, interventions must take place within well-defined boundaries: subject to clear thresholds, proper justifications and directly linked to concrete security threats.
- The CSA2 should be consistent with existing EU legislation. For instance, the CRA already offers a useful approach allowing authorities to address non-technical risks to products, done through targeted, proportionate measures rather than high-risk supplier designation.[15]
- To ease compliance for impacted entities, support measures should be made available, e.g. eligibility to apply for funding support under the EU Competitiveness Fund under the next Multi-annual Financial Framework.

Non-EU operations

The geographic reach of mitigation measures should not disadvantage European companies. Any restrictions addressing operations outside the EU would put European entities at a competitive disadvantage compared to entities not in scope of the CSA2 but operating in the same markets. This is particularly relevant in cases where a supplier, designated as high-risk in the EU, may be the sole available

[15] Art. 57 CRA.

or appropriate option in the local market. Non-EU operations should therefore be excluded from mitigation measures.

In addition, by design, the CSA2 mirrors the NIS2 entity-based logic, applying to organisations carrying out activities within the EU. This includes manufacturing activities, but not the product of the manufacturing activity. As a result, products manufactured outside the EU, but sold on the EU single market, fall outside the trusted ICT supply chain framework entirely. This could lead to competitive distortions.

A transparent, appropriate procedure

The cornerstones of the ICT supply chain security framework are: 1) the active involvement of Member States, mainly through coordinated risk assessments in the NIS Cooperation Group and their role in the comitology procedure to adopt implementing acts; and 2) the criteria used to identify non-technical risks.

1. Security risk assessments and the role of Member States

Security risk assessments play a central role. However, the operational conditions they are subjected to should be more precisely defined:

- Currently, there are no clearly defined criteria to decide when a coordinated risk assessment would be appropriate. Particularly the circumstances leading to Commission-led risk assessments should be clarified to ensure this avenue is reserved for genuinely high-priority risks.[16] Terms such as 'significant cyber threat' and 'sufficient reason to believe' require clear definitions.[17]
- Member State participation, particularly through the NIS Cooperation Group, should remain embedded in the process, with any departure from this model requiring compelling justification. The circumstances under which the Commission may act independently of the NIS Cooperation Group should be introduced in Art. 99(3).
- The threshold initiating a resourceful coordinated risk assessment in the NIS Cooperation Group – currently set at three Member States or the Commission – risks overuse and should be increased.
- The proposal does not appear to require a comprehensive technical and economic review of potential consequences prior to designations of 'third countries posing cybersecurity concerns,' nor does it foresee accompanying impact assessments.[18] Introducing such safeguards would help ensure that designation decisions rest on robust analysis and a clear understanding of their broader implications.

[16] Art. 99(3) of the proposal.

[17] Art. 100(1) sets out elements that the Commission shall take into account when verifying a risk posed by a third country. This among others includes third parties requiring entities to report vulnerabilities before being known to have been exploited. To prevent a vulnerability being interpreted by security researchers as 'actively exploited' against the intentions of the proposal, it should be specified the exploitation is malicious – the same manner the Cyber Resilience Act does in Art. 3(42). As written, third countries posing cybersecurity concerns could circumvent CSA2 criteria by simply requiring vulnerability reports to include a proof-of-concept, which the current proposal might interpret as having been actively exploited.

[18] Art. 100 of the proposal.

- A defined completion timeline, mirroring the six-month limit in Art. 99(2), should also be introduced in Art. 99(3) to improve predictability.
- The Commission should not have unilateral discretion to extend or amend the list of high-risk entities. Any such modification must be subject to meaningful involvement of Member States. Without such a safeguard, each addition of a new high-risk supplier would trigger a fresh round of legislative adoption, creating a cycle of recurring obligations and generating significant legal uncertainty for entities seeking to understand the scope and intensity of their compliance requirements.

The right balance between timely intervention, fidelity to the objective and evidence-based criteria is essential to the framework's credibility.

2. Criteria for the designation of high-risk suppliers

The Commission may introduce far-reaching requirements for entities in critical sectors, including measures that significantly restrict certain technologies or service models, such as remote data processing.

Whilst such measures may reflect concerns about dependency, resilience or systemic exposure, they could result in suppliers being treated as 'high risk' even where they demonstrate strong cybersecurity practices and have no link to countries posing cybersecurity concerns.

The proposal should therefore clearly distinguish between: 1) risks linked to countries of cybersecurity concern, where state intent or behaviour may undermine Europe's security; and 2) broader supply chain risks, such as technological lock-in or excessive supplier dependency. These categories raise different policy challenges. Dependency risks should be addressed through proportionate, supplier-neutral tools and structured dialogue with regulators, rather than by conflating them with malign state behaviour.

Furthermore, laying down a clear relationship between a supplier's relationship with a third country of concern is key. The following should be taken into account:

- The CSA2 allows the Commission to consider a company's 'place of establishment,' but the term should be clarified in alignment with existing EU cybersecurity law.[19]
- It also refers to a company being 'controlled by a third country.' This should apply only where a company is subject to undue foreign influence that creates a specific security risk, compromises its operational independence or affects the integrity of its services. Its use should be limited to jurisdictions lacking independent judicial oversight or meaningful right of appeal.

Structured consultation with affected entities

Where risks are identified, operational realities should inform any mitigation measures. A structured consultation mechanism with the companies implementing the measures should be created to ensure the concerns are mutually understood and mitigation measures are satisfactory.

Such consultation would enable suppliers to understand the specific resilience concerns identified by the Commission and to provide evidence-based input on whether those risks can be mitigated through technical, operational or governance safeguards – such as diversification strategies, portability measures,

[19] 'Place of establishment' could be designated based on headquarters, staff, operational facilities or tax registration, amongst others.

contractual controls, transparency commitments or enhanced oversight – before more restrictive outcomes are considered the only effective solution.

In addition, uniform mitigation measures across all entities could create significant challenges. What is feasible and appropriate in one context may be unworkable, or even create new risks, in another. Entities differ considerably in their system architectures and risk profiles, and any framework that fails to account for this diversity risks imposing requirements that are ill-suited to the environments in which they must be implemented.

A consultation mechanism is essential to ensure that mitigation measures are proportionate and feasible, improve predictability for companies in scope, and avoid unintended market consequences.

Trusted partners

The ICT supply chain security framework only focuses on the identification of untrusted partners. As a balance, it should also recognise partners whose governance and security systems are aligned with the EU's objectives.

A 'trusted partner' notion could be factored into future risk assessments, treating companies from trusted countries as lower baseline risk. Access to high-quality, trusted IT solutions and cybersecurity services remains essential to maintaining a high level of cybersecurity in the EU.

Amendments to the NIS2 Directive

NIS2 is a cornerstone of Europe's cybersecurity, but divergent national transposition is creating fragmentation. Entities now face different rules on scope, stricter national requirements, multiple supervisory authorities, varying conformity assessment obligations and inconsistent compliance timelines.

The Commission's efforts to reduce the compliance burden on NIS2 entities are welcome, but further harmonisation is needed. The Commission should support consistent transposition and provide clear, up-to-date guidance on how entities should navigate the Directive, implementing rules, national transpositions and proposed amendments.

Scope

Core business activity

The NIS2 Directive should establish the concept of core business activity, following in the footsteps of some Member States.[20] This is strictly needed to ensure legal certainty, uniform application across the EU and proportionality.

The aim is to create a clear *de minimis* rule. All ancillary business operations should be excluded from NIS2. This should apply, in particular, to entities whose primary business operations fall outside the NIS2 scope, but who risk inadvertently becoming regulated simply for having ancillary, small-scale operations under the NIS2 scope. The same goes for services that are exclusively provided within a group. This would avoid

[20] For example, the German implementation (BSIG) attempted to address this via a 'negligible activity' threshold.

disproportionate inclusion of non-critical entities that use IT services provided by one entity (e.g. the headquarter) to other entities of the group.

A clearly defined focus on core business activities allows supervisory and compliance efforts to focus on genuinely critical activities where cybersecurity risks have societal relevance. In addition, this clear but relieving step contributes directly to the EU's simplification agenda by reducing unnecessary regulatory complexity and administrative burden.

For the same reasons, the definition of 'research organisation' should be clarified to exclude companies that conduct R&D only as part of developing or improving their own commercial products, services or processes. Internal or ancillary R&D should not, by itself, bring an entity within the scope of NIS2.

Size cap

Moreover, the size cap imposed by NIS2 must be harmonised at EU level. This is illustrated by Hungary, where national transposition law sets out that companies with 50+ employees in sectors of high criticality (Annex I) are designated as essential entity; the Commission's new proposal raises this criterion from 250+ to 750+ employees. Deviations should only be permitted where the national company size distribution substantiates a lower threshold, for instance where smaller firms carry a disproportionate share of national resilience.

Harmonisation

The introduction of a principle of 'maximum harmonisation' for NIS2 sectors, where EU implementing acts are adopted under Art. 21(5), is welcome. However, this does not solve the fragmentation of multiple national frameworks for the other sectors. Other national divergences related to incident reporting, scope and classification still create market fragmentation. The maximum harmonisation principle should therefore be extended to all NIS2 entities.

'One set of measures for one law'

To significantly reduce the administrative burden for most entities, the principle of 'one set of measures for one law,' with EU-wide options to obtain presumption of conformity, should be guaranteed for all NIS2 entities. Importantly, the principle of main establishment must be consistently applied in all Member States to avoid erosion of its intended function and should be extended to all NIS2 entities.[21]

The amendments enabling a presumption of conformity with the NIS2 requirements would be a positive step and of major help down the line.[22] In any case, the method should be harmonised and based on existing and proven evidence to not reinvent the wheel. ISO/IEC 27001 is a technology neutral and sector unspecific tool that should be recognised to that end, whilst remaining strictly voluntary.

[21] Some Member States interpret Art. 26 NIS2 to require each individual legal entity to be compliant with NIS2 requirements, meaning each subsidiary would have to comply with specific, diverging national NIS2 requirements. It should be specified to be at group level to avoid fragmentation and duplicative burden. The same logic should apply to registration obligations for corporate, cross-border groups.

[22] Art. 5(9) of the proposal.

A mutual recognition policy for NIS2 compliance audits, allowing compliance through European or international standards, will be needed in the interim to bridge the gap, as it will likely take years before the method enabling presumption of conformity is in place.[23] Executing multiple conformity assessments and external audits for a single corporate entity in scope brings a significant cost.

Finally, although partially tackled by the digital omnibus, the issue of fragmented reporting regimes remains significant. The harmonisation of reporting obligations should go beyond the creation of the single entry point and define a harmonised timeline to the General Data Protection Regulation's 72-hour standard, a unique incident definition and horizontal threshold to be used across relevant reporting regimes.[24]

Ransomware data collection

Under the proposal, Member States are required to collect data related to significant incidents caused by a ransomware attack, such as whether the victim entity received a ransom demand and by whom, and whether it was paid and to whom.[25] There should be a clear guardrail to not expose entities to any negative ramifications or additional liabilities following the reporting of such information.

The scope of reporting should also be narrowed and aligned with approaches in like-minded jurisdictions such as Australia and the United States. NIS2 entities should not be required to report ransom or extortion demands where no payment was made. The main systemic risk lies in ransom payments that fuel the ransomware ecosystem, not in the mere existence of demands.

In addition, given the potentially highly sensitive financial and operational nature of this data, this mechanism should not be expanded into a systematic or automatic reporting obligation. Any reporting framework should require only minimal, necessary data, protect it with strict confidentiality and use it solely to generate actionable threat intelligence for CSIRTs and national authorities. This would keep the mechanism lightweight and avoid diverting resources from incident response and recovery.

PQC migration

The proposal rightly requires Member States to adopt policies for the migration to post-quantum cryptography (PQC) as part of their national cybersecurity strategy. As much as possible, Member States should build on existing PQC standards. Government agencies have already set quantum-resistance requirements to be followed by technology vendors used in national or government security systems, such as NSA's CNSA 2.0 and NIST PQC standardisation process in the US.[26]

---

[23] In the case of certification schemes, given the existing timelines for the current requested ones, there is an anticipation that developing certification for organisational matters, which represents a distinct area of expertise, will require additional time and resources.

[24] See DIGITALEUROPE, *Digital omnibus: a first step and what must come next, now*, available at https://cdn.digitaleurope.org/uploads/2026/02/Digital-omnibus-a-first-step-and-what-must-come-next-now.pdf.

[25] Art. 5(8) of the proposal.

[26] See: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF and https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4, respectively.

These national roadmaps mandate actionable guidance and concrete support measures to help entities accurately assess their cryptographic inventory and exposure, thereby facilitating a secure, coordinated and timely migration to PQC across the Union's digital applications and networks.

Commission guidelines for supply-chain information requests

The proposal mentions that the Commission should develop guidelines to recommend 'an appropriate level of detail, structure and format' for information requests passed by essential and important entities to their suppliers, especially for the supplier monitoring activity currently suffering a huge diversity.[27]

This could become a useful cross-sector standard but must be developed with strong industry input to avoid disproportionate burdens. It should also align with existing international guidance, and where no suitable standard exists, the ESOs could develop a European standard or technical specification.[28]

FOR MORE INFORMATION, PLEASE CONTACT:

Sid Hollman

Policy Manager for Cybersecurity

sid.hollman@digitaleurope.org / +32 491 37 28 73

Hanna Harrison

Associate Director for Resilience & Critical Infrastructure

hanna.harrison@digitaleurope.org / +32 494 03 32 14

Alberto Di Felice

Policy and Legal Counsel

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[28] See, for instance, the Manufacturer Disclosure Statement for Medical Device Security (MSD2).

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European digitalizing businesses across multiple sectors and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents, investment and technology companies. Together with our members, we shape the industry policy positions on all relevant policy matters and contribute to its development and implementation. Our membership represents over 56,000 businesses who operate and invest in Europe. It includes corporations and scale-ups which are global leaders in their field of activity, as well as national trade associations from across 30+ European countries.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20