DIGITALEUROPE

8 FEBRUARY 2022

Harmonising cyber protection across Europe: The digital industry's basic asks for the NIS2 trilogues

Executive summary

Trilogue negotiations for a reformed EU framework for the security of network and information systems (NIS2) will set the basis for Europe's cybersecurity efforts in the years ahead.[1] With an expanded scope covering more sectors, the end goal should be to build on the current framework, remedy its shortcomings and ensure effective compliance.[2]

Crucially, the final NIS2 must ensure that practical implementation will meet the ambitions it sets. We should not rush to establish rules that entities and authorities will struggle to follow – rather, we should build incrementally to steadily improve Europe's cybersecurity capabilities over time.

Current estimates put Europe's cyber workforce shortage at almost 200,000.[3] Unrealistic compliance demands placed on entities will not only not be met, but will actively work against genuine efforts to increase cybersecurity.

Co-legislators should therefore aim to:

- Provide a **clear list of essential and important entities** – with a full exclusion for SMEs subject to risk-based exceptions[4] and for activities

[1] COM/2020/823 final.

[2] In this paper we focus on areas where compromise and additional improvements appear possible in light of legislative discussions in the European Parliament and the Council so far. Our more detailed position on the whole proposal is available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/03/DIGITALEUROPE-position-on-NIS2-Directive.pdf.

[3] (ISC)² Cybersecurity Workforce Study 2021, available at https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

[4] Such as being the sole provider of a critical service for a Member State or the significant impact of potential service disruption on a Member State's economy.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

outside Europe – **minimising Member States' discretion** to deviate from such list;

- Require that **only confirmed, significant incidents be reported**, as opposed to mere 'threats,' with predefined parameters to determine significance;
- Consider a **72-hour notification timeline**, or absent this that the **24-deadline** be limited to incidents that significantly disrupt **service availability** as in the Parliament's version;
- Give precedence to an **EU-level process for making cybersecurity certification schemes mandatory**, as opposed to a fragmented national approach. Such process should defend the system **established under the Cybersecurity Act**,[5] ensuring **strong market analysis of existing schemes**. This process is quintessential to successful certification schemes, which should as a rule remain voluntary;
- Guarantee **strong alignment with existing international and European standards** for the European Commission's technical and methodological specifications as well as ENISA's technical guidelines; and
- Devote a specific article to the relationship with **sector-specific laws**, tasking the Commission to **periodically review the equivalence of risk management and incident notification obligations** to establish their precedence over NIS2.

[5] Regulation (EU) 2019/881.

Table of contents

Scope

Alignment on institutional design and enforcement is key to avoiding fragmentation in the operation of the internal market. Among the principal goals of the NIS reform is to remedy the wide divergence in how Member States have identified critical entities under the current Directive.[6] The final NIS2 should therefore be unambiguous about what entities it covers and minimise discretion for Member States.[7]

Essential and important entities

A **clear distinction between essential and important entities** should be established. This is achieved in the Commission's proposal, as well as **in the Parliament's version**, by listing the entities belonging to each category in Annexes I and II, respectively.

While the Council has brought more clarity to parts of Art. 2,[8] the introduction of Art. 2bis makes the identification of entities falling in each category more untransparent and discretionary for Member States. This is compounded by Art. 2a, which removes Member States' obligation to notify the Commission of their list of identified entities,[9] replacing it with a more generic obligation to notify 'relevant information.' Objective, primarily technical criteria should guide Member States' identification of covered entities.

Territorial scope

The **Parliament text** has clarified under Art. 2(1) that it is **only services provided, and activities carried out, in the Union** that fall under the NIS2 scope.

This clarification is particularly important considering the inclusion of manufacturing among important entities. Non-EU entities should not fall into

[6] Directive (EU) 2016/1148.

[7] In this paper we do not cover ongoing concerns regarding the broad and overlapping definitions that are included in the text, which were largely retained by both co-legislators. For more on these concerns, notably regarding cloud computing or data centre services, see pp. 4-5 of our original position.

[8] Notably, the inclusion of public administration entities (Art. 2(2a)), the requirement for entities being the only providers in a Member State to perform services used for critical societal or economic activities (Art. 2(2)(c)), the need for the impact from potential disruptions to be significant (Arts 2(2)(d) and (e)) and the exclusions provided for in Arts 2(3a)–(3b), except for Art. 2(3a)(2), which runs the risk of excluding too many public entities only remotely linked to the judiciary, parliaments or central banks.

[9] This obligation is kept and strengthened in the Parliament's Art. 2(2), first paragraph a.

scope, although they may come into consideration under EU entities' supply-chain obligations.[10]

SMEs

We urge the co-legislators to establish a **full exclusion for SMEs**, not just micro and small businesses. Such exclusion should only be **overridden by strict conditions** linked to an SME's critical role in light of the services it provides or its position in a given Member State.

These conditions for criticality, which reflect a risk-based approach, are laid down **under Art. 2(2)** and are sufficient to determine what SMEs should be brought into scope. Any further specifications as to size, including those under the Council's Art. 2bis, are redundant at best and grant unnecessary discretion to Member States.

Reporting obligations

Significant incidents

Notifications should be reserved for **confirmed, significant incidents**. We thus warmly support both co-legislators' **deletion of 'cyber threats'** from the reporting obligations under Art. 20(2), in favour of a voluntary, more actionable notification to potentially affected recipients to help them prevent threats from materialising.

In addition, we welcome the Parliament's reintroduction under Art. 20(3) of a list of **parameters to determine significance** – including number of affected recipients, duration and geographical spread, impact on service functioning and continuity, and impact on economic and societal activities – reflective of the approach taken under Art. 16(4) of the current NIS.

Notification timeline

Entities' resources should **focus on mitigating incidents** in the crucial phases of their emergence. Unfortunately, the proposal requires incident notifications within 24 hours, which will force entities to divert excessive resources away from mitigation towards legal compliance. This is especially true for SMEs that may fall into scope.

For this reason, the time allowed to notify authorities should be aligned with the personal data breach notification regime in the General Data Protection

[10] Art. 18(2)(d) of the proposal.

Regulation,[11] which sets a **72-hour deadline**. Similarly, allowing entities to submit their **final reports 90 days** after the initial notification, as opposed to one month in the proposal, would give entities more time to produce a meaningful report.

Absent these ideal timelines, the final text should converge around **the Parliament's position**, which specifies that the **initial 24-hour notification** should be reserved for incidents that significantly disrupt **service availability**, with other incidents having to be notified within 72 hours instead.

In order to facilitate reporting, we also strongly support the **Parliament's Art. 20(4a)**, which makes the establishment of a **single entry point for all NIS2 notifications obligatory for Member States**, as opposed to merely optional, in order to avoid national fragmentation of crucial information flows.

Main establishment

We urge co-legislators to provide a clear main establishment criterion in the final NIS2. The main establishment should be considered **an entity's place of central administration in the Union**. By contrast, the current criterion centred around where risk management decisions are taken – let alone 'predominantly' taken, as in the Council version – will make it too unclear for companies to know what authorities they will be supervised by.

We also invite co-legislators to **include number-independent interpersonal communications services (NI-ICS)** to the entities subject to main establishment under Art. 24.[12] NI-ICS are inherently cross-border in nature and their inclusion would fulfil the proposal's objective 'to ensure that such entities do not face a multitude of different legal requirements, as they provide services across borders to a particularly high extent.'[13]

Vulnerability disclosure

We welcome the co-legislators' efforts in Recital 31 and Art. 6(2) to align the proposed vulnerability registry maintained by ENISA with the **long-established CVE Program**.[14]

Similarly, we support the Parliament's stance at Art. 6(1) that **CSIRTs' coordinating role in vulnerability disclosure** should only be '**upon the**

[11] Art. 33, Regulation (EU) 2016/679.

[12] As defined in Art. 2(7), Directive (EU) 2018/1972.

[13] P. 11 of the explanatory memorandum.

[14] https://cve.mitre.org/.

request of the reporting entity,' combined with the Council's clarification of the voluntary nature of coordinated vulnerability disclosure in Art. 5(2)(c). As a rule, CSIRT engagement in multi-party cases should focus on cases not coordinated by the vulnerability owner, who is usually best positioned to lead the coordination.

Mandatory certification

The multiplication of Member State mandates for the use of cybersecurity certification schemes to demonstrate compliance with NIS2 should be avoided, as it will only work against the objective of a harmonised high level of cybersecurity across Europe. Instead, **certification schemes should only be made mandatory after careful assessment at European level** by the European Commission following the **process established under the Cybersecurity Act**.

While a strong EU-level process is vital, the Commission has proposed in Art. 21(3) that it should be allowed to request preparation of a scheme in cases where it determines a scheme should be mandatory but no such scheme exists. This circumvents Art. 56(3) of the Cybersecurity Act, which requires the Commission to carry out a thorough assessment of *existing* schemes before they can be made mandatory. This assessment is quintessential to successful certification schemes, which should as a rule remain voluntary.

Art. 21(3) should therefore be **deleted**, and **complete reference** should be made to the assessment procedure set out under **the Cybersecurity Act's Art. 56(3)**.

The Council has reintroduced *some* of the elements stipulated in the Cybersecurity Act under its version of Art. 21(2),[15] but it contradictorily still allows the Commission to circumvent an assessment of those very elements by retaining Art. 21(3).

In addition, the Council allows the Commission to make schemes mandatory based on implementing acts, which receive lower scrutiny. From this perspective, we support the Parliament's position that such decisions should be adopted via **delegated acts**.

[15] Under Art. 56(3) of the Cybersecurity Act, these include: cost-benefit impact on manufacturers, providers and users; existence and implementation of relevant Member State and third-country law; an open, transparent and inclusive consultation process; implementation deadlines, transitional measures and periods; and efficient transition from voluntary to mandatory certification.

Risk management

Standards

Strong engagement with businesses on setting technical standards and certifications in the context of new and emerging technologies is vital, and central to the EU's better regulation principles.[16]

We support the Council's position at Art. 18(5), reflective of the original proposal, to stipulate that the Commission's implementing acts laying out technical and methodological specifications should **follow existing international and European standards**, as well as relevant technical specifications.

We also welcome the Council's **inclusion of ENISA** – in addition to the Cooperation Group pursuant to Art. 14(4)(d) – in the process for adopting such implementing acts. **ENISA's role** in drawing up technical guidelines based on existing international and European standards for compliance with Art. 18 is also rightly reflected in **Art. 22(2)**.

Finally, we support the **Parliament's Art. 22(2a)**, which tasks the Commission to **promote the uptake and continued update of existing standards** for compliance.

Encryption, authentication and secure communications

We welcome the co-legislators' clarifications in Art. 18(2)(g) to the effect that cryptography and encryption should **not be mandatory**.

The Parliament stipulates they should be used only 'where appropriate,' while the Council proposes entities should put in place a policy on their use. Given the central role cryptography and encryption can play in securing data and service integrity, we support this latter requirement.

Similarly, we support the Parliament's requirement for the 'use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems,' which should apply 'where appropriate.'

[16] See *'Better regulation' toolbox – November 2021 edition*, available at https://ec.europa.eu/info/sites/default/files/br_toolbox-nov_2021_en_0.pdf.

Link with sector-specific laws

Clarity on the **relationship between NIS2 and the growing number of other laws** setting out cybersecurity obligations on entities is necessary in order to avoid conflicting requirements and facilitate compliance efforts. This has been particularly evident given parallel discussions on the proposed Regulation on digital operational resilience for the financial sector (DORA),[17] but is not limited to the DORA proposal.

We welcome the Council's work to expand on this aspect under the **new Art. 2b**, tasking the Commission to **periodically review the equivalence of risk management and incident notification obligations** under sector-specific laws in order to establish their precedence over NIS2. These provisions are reflected in the Council's Recitals 12a and 12aa, while Recital 12aaa should also include NIS2 risk management and incident notification obligations among the elements that future sector-specific legislation should take into account. Similarly, Recital 12ab should incorporate the need to avoid overlapping risk management obligations, similar to the current language on reporting.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

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

Zoey Stambolliu

Manager for Infrastructure and Security Policy

zoey.stambolliu@digitaleurope.org / +32 498 88 63 05

[17] COM/2020/595 final. Our position on the DORA proposal is available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/02/DIGITALEUROPE%E2%80%99s-response-for-the-Commission%E2%80%99s-public-consultation-on-the-Digital-Operational-Resilience-of-Financial-Services-DORA-legislative-proposal.pdf.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK