Computer & Communications Industry Association
Tech Advocacy Since 1972

NIS2 Directive
CCIA Europe Comments

Executive summary

The Computer and Communications Industry Association ('**CCIA Europe**') welcomes the main objectives of the European Commission's ('**the Commission**') proposal for a revised Directive on the Security of Network and Information Systems ('**NIS2**').

In particular, CCIA Europe welcomes the Commission's efforts to consolidate and harmonise the existing NIS Directive[1] and to encourage further information sharing among stakeholders and Member States authorities. In particular, the Commission provides helpful improvements to the current EU cybersecurity rules, including the generalisation of the 'One-Stop-Shop' ('**OSS**') mechanism for most cross-border services falling in the scope of the Directive, and measures to facilitate coordinated vulnerability disclosure exchange across the EU. We are also encouraged to see the proposal maintains liability exemptions for entities reporting incidents.

However, CCIA Europe is concerned that the proposed NIS2 does not go far enough to also extend the OSS mechanism to electronic communications networks ('**ECNs**') or electronic communications services ('**ECS**'). CCIA Europe further believes that NIS2 goes too far in that it suggests broadly prescriptive and sometimes unclear rules to govern the security practices of a wide range of service providers. If everything is important, nothing is important, and we fear that the proposed approach risks diverting resources to compliance efforts instead of ensuring meaningful resiliency and security of entities' services throughout the Union.

CCIA Europe invites lawmakers to improve the proposal and:

- **Ensure legal clarity, consistency with EU laws, and harmonisation of scope.** Service providers should know if and when the rules apply, and which rules and oversight mechanism apply when multiple legislation apply to them.

- **Favour a risk-based approach focused on outcomes rather than compliance burden.** Obligations on essential and important entities should be clear, workable and commensurate to the risks their services are exposed to and the criticality of their service.

- **Ensure effective and proportionate oversight.** While the generalisation of the OSS mechanisms to most cross-border services should be welcomed, the proposal is a missed opportunity to ensure greater harmonisation across the EU as it fails to extend the OSS to over-the-top ('**OTT**') communications services. The fractured approach and the proposed enforcement powers appear disproportionate and are unlikely to address the root-cause of the current level of supervision identified by the Commission.

- Ensure that the EU's efforts to increase **vulnerability information sharing remain voluntary and build on international best practices.**

[1] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

1. Ensure Legal Clarity, Consistency with EU laws, and Harmonisation of Scope

Service providers should know if and when the NIS2 rules apply to them. This includes clarity on which rules and oversight mechanisms they are subject to, particularly when multiple legislative frameworks apply.

The proposed NIS2 goes some way in addressing the deficiencies and fragmentation of implementation observed under the current NIS framework. For instance, CCIA Europe supports the Commission's efforts to align the definitions of sectors in the NIS2 annexes that would minimise variation of implementation across Member States. Similarly, the harmonisation of the registration of entities with the European Union Agency for Cybersecurity ('**ENISA**') under Article 25, and requiring ENISA to forward entities' notification to the relevant single competent authority in the Union will remove entities' duplicative efforts and require better cooperation between competent authorities.

However, CCIA Europe considers that several aspects of the proposed NIS2 must be addressed to ensure as harmonised a scope as possible including consistency with recently adopted legislation, in particular:

i. Article 2 should clarify that **only external facing services (i.e. those offered directly to customers) should be in scope of the Directive.** Where an entity carries out operations in furtherance of providing its (or its wider group's) own services, those operations should fall outside the scope of NISD2 - notwithstanding whether or not a company's services are in scope of NIS2. For example, a company offering a video sharing service developed and built on its own servers should not have its "cloud computing", "data centres", or "content delivery network" operations covered in NIS2. CCIA Europe considers that it would be disproportionate to extend NIS2 obligations to an entire entity simply because it performs operations described in the proposal. We believe this clarification would also reflect parts of the proposal, including the notification of incidents "having a significant impact on the provision of their *service*" (Article 20(1)) .

ii. **Cloud computing services and data centres should be better defined in the proposal in line with international standards.**[2] Varying national interpretations and legal uncertainty would likely persist if this is not addressed.

iii. **Extend the OSS mechanism to all cross-border entities/digital infrastructures** (Annex I(8)). While the proposed NIS2 Directive helpfully proposes to establish an OSS mechanism for most entities providing cross-border services, it would not apply to trust service providers and electronic communications networks and services. While CCIA understands that Member States should have a margin of manoeuvre to oversee the network and information security practices of some essential services provided on a national basis, 27 oversight regimes for cross-border services conflict with the main objective of the EU's Single Market.

iv. **OSS jurisdictional criteria should be based on meaningful operational and managerial capabilities.** Article 24 specifies that entities subject to the OSS mechanism are under the jurisdiction of the Member State where they have their main establishment in the Union, described as where the headquarters of the entity are located, where the decisions on cybersecurity risk management are taken, or in the country where the company has the highest number of employees. We believe the latter criterion related to employment does not correspond to any security management rationale. The establishment that has operational and managerial capabilities to implement cybersecurity measures would be a more suitable alternative to identify the main establishment.

v. NIS2 should **avoid inconsistencies with the recently adopted European Electronic Communications Code ('EECC')**[3] for providers of electronic communications networks and services, including OTTs. CCIA Europe

[2] E.g. ISO/IEC 17788:2014 for a definition of cloud computing and ISO 22237-2:2018 for a definition of data centres
[3] Directive (EU) 2018/1972 establishing the European Electronic Communications Code

strongly supports extending the OSS mechanism to cross-border OTT services and repealing the relevant provisions of Article 40 EECC to avoid duplication and legal uncertainty. We also appreciate that maintaining certain precedents arising from the application of Article 40 and Article 41 EECC and associated guidelines[4] may be useful in the short-term (as per Recital 49). However, given the significant discrepancies between NIS2 and the EECC regarding the nature and thresholds of incidents which should be reported,[5] we think it is important to clarify that ENISA continues ensuring greater harmonisation regarding the application of cybersecurity obligations consistent with NIS2. Furthermore, it should be clear any national legislation that is inconsistent with NIS2 should be repealed. We raise further concerns regarding the incident reporting threshold and the security obligations of the NIS2 in section 2(B) further below. Finally, we urge lawmakers to ensure that nothing in the NIS2 proposal undermines encryption - including end-to-end ('**E2EE**'). While encryption should be promoted where appropriate, CCIA Europe cautions against mandating encryption as Recital 54 suggests. NIS2 should be technology-neutral and recognise that encryption is one of many other ways to ensure data integrity and prevent unauthorised data access.

vi. Similarly, **NIS2 should avoid circumventing the recently agreed Cybersecurity Act ('CSA')**[6] as is currently the case under Article 21. By allowing Member States to require essential and important entities to certify certain ICT products, services and processes, the proposed NIS2 effectively seeks to rewrite rules that the Council of the European Union (**'the Council'**), the European Parliament (**'the Parliament'**) and the Commission adopted a little over 2 years ago. As a reminder, the adoption and promotion of cybersecurity certifications under the CSA should primarily be carried out on a voluntary basis.[7] We raise further concerns regarding national mandatory certifications in section 2(C) below.

vii. Finally, CCIA Europe calls on lawmakers to **ensure consistencies for some of the services covered by both NIS2 and the proposed Regulation on Digital Operational Resilience for the Financial Sector** ('**DORA**')[8], e.g. on incident reporting thresholds, time of the initial incident notification, incident reporting templates, and supervisory competence. This is essential to avoid any disproportionate duplication or contradictions of obligations for service providers subject to both legislative frameworks.

2. A Risk-based Approach Focused on Outcomes Rather than Compliance

A) Differentiation between Essential and Important Entities

CCIA Europe notes that the proposal establishes the same rules for essential and important entities, and considerably extends the list of "essential entities" to a whole range of digital services. In both instances, the underlying premise seems to be that an online marketplace,[9] for example, and national electricity grids are equally critical to the functioning of

4 See for instance ENISA Guideline on Security Measures under the EECC from December 2020, available on https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

5 Article 2(42) EECC defines *security incident* as "an event having an actual adverse effect on the security of electronic communications network and services" while Article 4(5) NIS2 refers simply to *incidents* (not just security incidents) i.e. any event compromise the available, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via network and information systems". Article 20(2) and (3) in NIS2 also mandate entities to report *threats*;

6 Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

7 Article 56(2), Recital 91;

8 Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, and (EU) No 909/2014

9 Marketplaces are qualified as "important entities" under Annex II;

Europe's economy and society. The same goes for a cloud-based Customer Relationship Management (CRM) software provider[10] and drinking water suppliers.

CCIA Europe respectfully disputes the assumption that everything must be considered critical and be treated equally. Not only is this a significant departure from the recent NIS Directive, but such a broad brush regulatory approach fails to take into account objective criticality thresholds. Above all, the NIS2 approach stands at odds with good cybersecurity governance around risk prioritisation including effective threat mitigation. If everything is important, nothing is important.

Finally, it is not clear to what extent erecting the same obligations for all services would remedy the key shortcomings of the NIS Directive identified in the Impact Assessment[11] accompanying the NIS2 proposal, namely a lack of jurisdictional clarity and varying interpretations and implementation across Member States.[12]

CCIA Europe invites lawmakers to **maintain a risk-based approach to cybersecurity and ensure that the cybersecurity risk management and reporting obligations are commensurate to the level of risk *and* the criticality of the service**, based on objective criteria, greater use of empirical methods for determining categorisation and a process for either complete inclusion or exclusion to improve transparency of identification.

B) Incident and threat reporting

CCIA Europe believes that the primary objective of any incident reporting obligation should be about encouraging high quality reports that drive accountability, improvement in practices and benefits to end-users. (e.g. through appropriate mitigation, user awareness, improving standards, etc.). Conversely, we caution against notification requirements for the sole purpose of achieving more reporting, which may ultimately decrease cyber resilience, and serve only to confuse end-users and/or lead to notification fatigue. Similarly, any incident reporting obligation should be workable in practice, with clear triggering thresholds which a reporting entity can reasonably quantify.

CCIA Europe therefore invites lawmakers to:

i. **Focus on mandatory reporting of incidents which are truly significant** to avoid overburdening the notifying entities and the relevant authorities with inactionable or irrelevant reporting. **The significance threshold should be clear, pragmatic, and based on international standards.**[13] Article 23(3) currently envisages the reporting of incidents that have "the potential to cause substantial operational disruption or financial losses for the entity concerned", or have "the potential to affect other[s] [...] by causing considerable material or non-material losses". These thresholds are vague and unworkable in practice. In the vast majority of cases it is impossible to quantify the scale of effective financial losses of a cyber incident within 24 hours, let alone the *potential* financial losses that their customers may face.[14] Similarly, CCIA Europe cautions against reporting an incident that may cause non-material losses without clear detailed guidance on how such quantification should be performed.

---

10 A cloud-based CRM software would fall in the "cloud computing service" definition, and be categorised as an "essential entity" under Annex I;

11 SWD(2020) 345 final

12 The Impact Assessment provides ample evidence of NISD shortcomings specifically pointing to a lack of clarity of jurisdiction and varying interpretation, implementation and capabilities across the EU (section 2.2.2). CCIA Europe regrets the selective reading of studies and surveys used in the Impact Assessment to conclude that "key companies" are not taking enough cybersecurity measures (section 2.2.1) and skew towards additional regulation;

13 E.g. ISO/IEC 27035-2;

14 First deadline for reporting under Article 20(4)(a);

ii. **Ensure that mandatory incident reporting falls on the best placed entity when an incident involves multiple entities, similar to Article 16(5) of the current NIS Directive.** Given the broad scope of "essential entities", the proposed NIS2 would likely capture existing contractual relationships between an essential entity acting as a supplier / vendor, and another essential entity acting as the customer / user. In those cases, the customer / user is more likely to quantify the significance of the incident than the vendor. For example, an air carrier may use a third party cloud computing service for a range of purposes, from booking management to aircraft repair monitoring. As cloud computing remains by and large agnostic to the content they host, the cloud service provider will be unable to quantify the effect of an incident on one or more of its servers on that particular customer. Even if it were able to, this would effectively lead to double - and potentially incomplete - reporting from both affected entities, particularly where one entity may not be privy to the information that is more appropriately within the gift of the other entity.

iii. **Encourage *voluntary* information sharing of "threats" and "near misses"** and caution against mandating the reporting of such information. At present, the CSA loosely defines cyber threats as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons".[15] This is very wide in scope, and absent any specific and workable metrics, could lead to severe compliance difficulties at best, or misallocation of entities' and supervisory authorities' resources over a significant number of inactionable information.

iv. **Consider workable deadlines for reporting a significant incident, with a first notification in line with the General Data Protection Regulation ('GDPR')[16], and a final notification one month after the completion of the forensic analysis.** In the event of an incident, particularly a 'significant' incident that would warrant a mandatory reporting, entities should be expected to primarily focus on identifying the scale of the incident, containing and mitigating the incident. Instead, the two- (and sometimes three-) step process as described in Article 20(4) would direct entities' resources to comply with a notification obligation without bringing substantial value in terms of containment and impact mitigation. As per our comments above, the wide and vague scope of incidents that should be reported to the relevant authority are expected in practice to have a multiplier effect on the resource allocated purely for compliance purposes. At the same time, CCIA Europe recognises that notification is important, and we therefore recommend reformulating Article 20(4) to indicate a reporting timeline of "without undue delay and where feasible not later than 72 hours after having become aware of the incident" (consistent with Article 33(1) GDPR). Last but not least, expecting a full notification one month after the entity has become aware of the incident does not necessarily take into account the time necessary to investigate, let alone contain, sophisticated state-sponsored or otherwise similar cyber attacks. CCIA therefore recommends that the final notification be sent to the competent authority one month after the completion of the forensic analysis.

C) Cybersecurity risk management measures

i) General comments

Overall, CCIA Europe supports the comprehensive cybersecurity risk management measures set out in Article 18. However, we invite lawmakers to clarify that **implementing measures specifying the methodology and technical specifications of those risk management requirements should take utmost consideration of international standards and frameworks.** This clarification would ensure that the specified measures remain fit to address the security of global services and supply chains.

[15] Article 2(8) CSA
[16] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

ii) Supply chain security assessment should be based on objective, technical specifications

CCIA Europe generally welcomes the introduction of an obligation for entities to assess its supply chain security. However, and to the extent that the supply chain security assessment of the Cooperation Group are relevant for entities performing their obligations under Article 18(2)(d), CCIA Europe cautions against supply chain assessments which would consider "non-technical factors" (as per Article 19) and focus on supply chain areas based on subjective requirements such as those set out in Recital 47.

Instead, CCIA Europe recommends that the Coordination Group liaise with ENISA and relevant industry stakeholders to **produce specific, voluntary, principles-based supply chain security standards** with associated technical assessment criteria in line with international standards. The Coordination Group should then work closely with ENISA to **review top suppliers' self-attestations** to better understand the specific supply chains that present the most risk.

iii) Certifications should remain voluntary

As mentioned in section 1(vi) above, CCIA Europe is concerned that the proposed Article 21 deviates from the recently adopted CSA. **CCIA Europe believes the EU's certification approach should remain voluntary in line with international standards and frameworks**, and should avoid giving Member States carte blanche to require certification for entities to be able to demonstrate compliance with Article 18.

CCIA Europe is concerned that a mandatory obligation to structure security in alignment with a prescriptive standard as per the proposed Article 18 will lead to the implementation of security in a 'particular way', rather than to a 'particular level of assurance' – to the detriment of the security of systems.

This NIS2 covers a range of services and entities, operating across different national and global markets. It is challenging for any security standard to, on the one hand, be suitable in the vast majority of 'normal' cases, and simultaneously take into account the specific challenges that arise when providing specific "essential" or "important" services – in particular, when operating a pan-European, or global infrastructure.

Ultimately security is implemented through a series of controls, but it should not automatically be inferred that the presence of absence of specific controls, mean that one organisation is more or less secure than another. What is important is the outcome; that the security measures put in place by an entity are appropriate to the risks being faced. Assurance that appropriate security is in place can be carried out in a variety of ways, one of which is to verify the presence of specific controls, but this is not the only way. For example, the use of metrics of security-effectiveness can also demonstrate that appropriate measures are in place and operating effectively. We encourage the co-legislators to adopt an approach that is based on appropriate outcomes, rather than focusing on prescriptive adherence to fixed standards.

In other words, while certification schemes can help establish that an entity has put in place security controls, an entity may choose not to certify and still be able to implement the relevant standard(s) underlying said certification and/or other appropriate security measures commensurate to the risks it faces, and therefore comply with Article 18 requirements.

CCIA Europe calls on lawmakers to adopt an approach which recognises that *how* the relevant standard is met, and assured, is best determined by the entity itself and to be held accountable for those determinations. to favour security and resilience outcomes over process and compliance.

3. Ensure Effective and Proportionate Oversight

As stated before, CCIA Europe welcomes the Commission's efforts to consolidate and harmonise the existing NIS Directive and extend the OSS mechanism for most cross-border services falling in the scope of the draft NIS2. We strongly encourage lawmakers to extend this mechanism to all cross-border services, including trust services and electronic communications networks and services.

However, CCIA Europe is concerned that the proposal allows the national relevant authorities to perform extensive access to and audits of a whole new range of service providers now qualified as 'essential entities', at any given time, without any incident ever having taken place, without any justification, and without offering the entity any recourse for redress.

While CCIA Europe believes that the relevant authorities should be vested with the necessary powers to ensure compliance with NIS2, we consider that Article 29 and 30 are disproportionate vis-a-vis the thousands of new entities covered by NIS2 and that some enforcement powers may carry potential risks e.g. when systems or data used by several cloud customers are accessed in the course of an on-site audit.

Furthermore, the proposed Article 29 and 30 are unlikely to address the root-cause of the current low level of supervision identified in the Impact Assessment accompanying the proposal. As a reminder, the Commission Impact Assessment explains that the low level of ex post supervision on the Digital Service Providers was not due to the supervision and enforcement regime set forth in the NIS directive, but rather (i) the lack of a conclusive overview by the competent authorities of these services across the Member States, (ii) the lack of clarity of the jurisdiction rules and (iii) an insufficiently harmonised supervision system.[17] Similarly, the Impact Assessment noted that "during the country visits conducted in 2019-2020, the Commission observed that many Member States only make limited use of [ex ante supervision powers vis-a-vis Operators of Essential Services]."

CCIA Europe suggests that the NIS2 should be primarily an opportunity to harmonise enforcement across the EU, and calls on lawmakers to:

- Ensure that the relevant competent authority provides a **justification of the necessity of the request where the information would not be otherwise available through other means under paragraph 2 of Article 29 and 30, as well as statement of competence when other legislation apply and other competent authorities may be involved**;

- **Consider alternative measures** to physical audits, system and data access, such as the possibility to conduct third-party audits;

- Introduce **a right for the entity to seek the review of a given request before an independent body**;

- Introduce provisions governing the **cooperation between competent supervisory authorities whenever relevant EU legislation overlaps** with NIS2 (e.g. DORA, GDPR, e-Privacy Directive);

- **Remove the far-reaching personal liability of individual employees, which is disproportionate and unlikely to be effective for bad actors.** We remind lawmakers that employees' liability should be duly restricted to

[17] Section 2.2.2 of the Impact Assessment;

egregious criminal activities where the employees act in their own individual capacity, which is beyond the scope of NIS2.

4. Vulnerability Information Sharing

CCIA Europe strongly supports the Commission's efforts to facilitate vulnerability information sharing providing that they are aligned with international standards such as the common vulnerabilities and exposures program. We therefore invite lawmakers to consider the following:

- **Ensure that any vulnerability is disclosed once it has been patched by the relevant ICT provider.**
- **Support ENISA's cooperation with third country jurisdictions** who have developed or participated in vulnerability registries similar to the one described in Article 6, as per Recital 31. We consider that these efforts should not compromise EU Member States' contribution to international practices.
- **CSIRTs should be able to develop Vulnerability Disclosure Programs in future guidance and standard documents**, **based on existing international standards,** that entities may choose to deploy internally, and ensure that those programs do not require government involvement between private sector entities.
- Maintain the **voluntary nature** of Coordinated Vulnerability Disclosure programs.

***

For further information, please contact Alexandre Roure, Senior Manager, Public Policy, CCIA Europe: aroure@ccianet.org