Cybersecurity Coalition

# Submission to the European Commission consultation on Revision of the Network and Information Systems (NIS) Directive

The Cybersecurity Coalition ("Coalition") submits this paper to the European Commission on the NIS Directive revision consultation[1].

The Coalition is composed of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace that will encourage companies of all sizes to take steps to improve their cybersecurity risk management. We are supportive of efforts to identify and promote the adoption of cybersecurity best practices, information sharing, and voluntary standards throughout the global community.

As leaders in the cybersecurity industry, we recognize the complexity and importance of securing critical infrastructure. We believe that the NIS Directive could best achieve these goals through the following approach:

- Retain the current scope for designation as Digital Service Providers (DSPs);
- Promote greater alignment between DSPs' incident notification requirements under GDPR and the NIS Directive;
- Retain the current differentiation between the regulatory obligations of DSP and those of Operators of Essential Services (OES);
- Continue to review whether there is a need to expand the scope of OES. Make determinations based upon empirical data and engagement with the private sector;
- Harmonize OES security requirements across member states and align with the approach for DSPs;
- If cybersecurity certifications are necessary, utilize voluntary certification schemes and self-evaluation mechanisms based on specific criteria and aligned with international standards;
- Streamline and simplify conflicting incident reporting obligations under the NIS Directive and GDPR and provide clarity with regards to who is responsible for incident reporting;

[1] https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-commission-launches-public-consultation-nis-directive

[2] The views expressed in this comment reflect the consensus views of the Coalition and do not necessarily reflect the views of any individual Coalition member. For more information on the Coalition, see www.cybersecuritycoalition.org.

- Ensure that effective incident response is prioritized over cumbersome incident reporting requirements;
- Incorporate representatives of the cybersecurity industry into the work of the NIS Cooperation Group, as appropriate;
- Facilitate better Computer Security Incident Response Team (CSIRT) access to real-time threat intelligence;
- Clarify and drive implementation of technical measures for compliances with the NIS Directive;
- Provide liability protection for good faith reporting of cybersecurity incidents;
- Support more companies engaging in voluntary information sharing organizations;
- Encourage OES and DSP to adopt a VDP, on a voluntary basis and in a manner that aligns with international standards, as a standard component of their security programs;
- Facilitate Member State and cyber agency incorporation of VDPs in security guidance and standard documents; and
- Ensure that Member States are adequately resourced to lead VDPs, where appropriate, and support CVD led by non-government organizations.

The Coalition thanks the European Commission for its careful examination of complex issues and the open and participative process used to solicit input on NIS Directive. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that NIS Directive is successful in driving consistent, effective cyber risk management across the European Union.

Respectfully Submitted,
The Cybersecurity Coalition

October 1, 2020

CC: Ari Schwartz, Venable LLP
Alex Botting, Venable LLP

Cybersecurity Coalition

## SECTION 1 – SCOPE, OBLIGATIONS AND HARMONIZATION ISSUES

### A. Digital Service Providers (DSPs)

#### Scope of DSPs

Given wide divergences between Member States in how they define services that fall within the scope of the DSP definition, the Coalition believes it is premature to consider broadening the definition. We believe the current definition provides enough latitude to incorporate key critical digital infrastructures and services. As an example, business software services are already in scope of the existing Directive (by virtue of the Annex II I cloud computing definition), since business security software is typically managed via the cloud, according to the 'software as a service' (SaaS) principle.

Nevertheless, we strongly encourage the review process to prioritize greater consistency in the definition of DSPs across the EU and to conduct appropriate threat assessment and risk analysis when considering any expansion of the current scope.

#### Incident Notification by DSPs

The Coalition supports greater alignment between GDPR and NIS Directive incident reporting requirements for DSPs. While GDPR incidents cover confidentiality, integrity and availability incidents, incidents under the NIS Directive are focused solely on availability (loss of service). Given that many GDPR-applicable incidents will have a cybersecurity incident as its cause, there should be greater alignment between the two to avoid unnecessary complexity or confusion among DSPs when responding to cyber incidents.

#### Differentiated Obligations between DSPs and Operators of Essential Services (OES) Remain Valid

The current approach of differentiated regulatory obligations between DSPs and OES remains valid for several reasons. Firstly, on the whole DSP businesses developed during the internet revolution and have thus placed a higher emphasis on, and investment in, digital infrastructure and service cyber security protection than many more traditional players that are defined as OES. In particular, they are less likely to be encumbered by legacy systems that were developed without cyber security in mind.

Secondly, DSPs are typically multi-national companies whose businesses operate across multiple jurisdictions, making oversight by a single cyber security authority impractical.

Thirdly, it enables government to focus on the sectors needing more resources, operational support and the implementation of modern risk management frameworks where they are most needed.

Moreover, an approach that treats everything as having the same level of criticality dilutes the resources that are available to the *most* critical assets. Risk of life due to cyber incidents among DSPs is below that of infrastructure such as water, transport, energy and healthcare. Accordingly, the cyber coalition recommends the distinction – and the light touch approach for DSPs – remain in place.

## B. Operators of Essential Services (OES)

### Scope of OES

One of the many unexpected consequences of the COVID-19 global health crisis has been a sustained uptick in the number, intensity and effectiveness of malicious cyber-attacks and campaigns directed toward the digital infrastructure of essential service providers. As a result, governments are rightly re-evaluating who they consider to be operators of essential services, what cybersecurity obligations they need to comply with, and what risk management methodologies they should develop.

The Coalition sees merit in this reflection. A careful risk-based examination of whether the definition of healthcare providers should be extended to cover vaccine research facilities, healthcare product manufacturers, telemedicine providers and potentially critical pharmaceutical companies. Equally there are valid arguments for considering whether postal and food distribution hubs should have OES status as a result of the revision process.

Any extension of the scope to additional sectors should be driven, however, by extensive evidence and empirical data. This should include consultations between government and those sectors, as well as evidence and input from the security community.

### Improving OES Identification and Transparency

The Coalition agrees with the European Commission that the identification and designation of OES players in Europe is both uneven and inconsistent[3]. We also observe that a service provided in multiple Member States may be treated as an OES in one Member State, and as a DSP in another.

[3] European Commission Report in assessing the consistency of the approaches taken by the Member States. 28 October 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN found that 11 out of 28 Member States have identified additional essential services that do not fall under the original scope of Annex II.

Regardless of whether the scope of OES should be expanded to include additional sectors, it is imperative that this review place greater emphasis on convergence of OES identification as well as more clarity on what service criticality means in practice. Whilst efforts have already been undertaken by this NIS cooperation group on this front[4], consistency of definition and requirements remain absent. We encourage the NIS cooperation group and ENISA to focus on this work-stream as a matter of priority.

To ensure that the definition of OES becomes more consistent and evenly applied across the single market, this review of the Directive is an opportunity to press Member States to improve the transparency of their identification process, and for ENISA and the NIS Cooperation Group to promote greater alignment across the Digital Single Market. Such an approach will improve both consistency of definition and breadth of competitive choice in turn improving compliance with the NIS security controls.

**Harmonizing OES security requirements**

The regime for security measures for DSPs has been more effective than its counterpart for OES. Having been centrally developed and promulgated (such as by ENISA), the DSP requirements are easier to identify, more efficiently implementable, and as a result have been more effectively complied with, in terms of embedding them in product development and organizational processes. National implementations of the Directive generally refer to the EU Implementing Regulation for DSPs. More importantly, the technical guidelines for implementation of security measures for DSPs[5] are an important resource for demonstrating – in a practical and operational manner – how our members meet the requirements.

Unfortunately, there is no central resource that sets out how requirements can be met by OES, or what responsibilities vendors must absorb or share. The NIS Directive has therefore had a limited impact in influencing security measures for OES and the result is a confusing patchwork of requirements. This is despite efforts from ENISA to map requirements to the most common standards in use by OES; ISO 27001, IEC 62443 and NIST CSF. As such, any revision of the NIS Directive should harmonize the security measures applicable to OES and formally recognize the role of ENISA in setting out how internationally recognized standards and certifications can be used to demonstrate compliance, if certifications are appropriate. Effective cyber risk management should remain the ultimate objective of the NIS Directive.

[4] NIS Cooperation Group. Reference document on security measures for OES. https://ec.europa.eu/newsroom/dae//document.cfm?doc_id=53643

[5] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

Cybersecurity Coalition

### Incident Reporting Responsibilities

In situations where critical infrastructure protection is provided to an operator of an essential service by a digital service provider, members of the Coalition have experienced a lack of clarity from enforcement authorities in some markets as to the responsibility for reporting an incident. In this respect we underline the limited liability of the DSP provider and confirm that the burden of proof rests with the affected OES operator.

## SECTION 2: FUNCTIONING OF THE NIS DIRECTIVE

### Security Certification

Being able to assess security preparedness and demonstrate legal compliance to NIS requirements through certifications could be an option available for OES and DSP. Given the complexity of the current cybersecurity landscape, however, we would encourage the Commission to utilize voluntary certification schemes and self-evaluation mechanisms, based on specific criteria defined by cybersecurity authorities, to increase participation and the overall resilience of the private sector. In addition, to avoid creating unnecessary divergence from international best practices, any certifications should point to best in class international standards, such as ISO 27001, SOC 2, or IEC 62443, where relevant. In this regard, efforts by ENISA to map requirements to international standards and certifications in order to demonstrate compliance are welcome and should be formally recognized in the Directive.

### Incident Notification for DSP

Incident response notification processes and requirements are an important element of establishing an effective cyber security perimeter. In that respect, articles 14 and 16 have driven conversations around security operations controls, particularly to improve solutions and capacity building in enterprises.

The Coalition recognizes that the current mandatory incident reporting threshold – focusing on the number of users impacted rather than the size of the affected party – is the right approach and should be maintained. The objective of the revision should not be to capture more incidents, rather to focus more clearly on the most significant incidents with the greatest risk and potential impact or harm to consumers (e.g. cross border incidents would certainly fulfill that criteria).

We also observe clear overlap between the information security breach notification requirements in the GDPR, PDS2 and those required under NIS. Multiple differing reporting requirements results in uncertainty for OES and DSPs as to the right standard of intervention.

Hence NIS 2.0 should take the opportunity to streamline and simplify the obligations according to these different legislative instruments. We also encourage the designation of a single point of contact for incident reporting in Member States, to ensure that effective incident response is not inhibited by unnecessarily complex and duplicative compliance requirements.

Finally, as a general observation, the incident notification requirements would benefit from a common reporting framework (a common template for Member States to use and/or a common taxonomy of terms).

**Incident Notification for OES**

The Coalition observes that many of our incident handling customer conversations focus on establishing proactive measures, such as incident detection and response. In practice this means services such as comprehensive threat hunting, automated asset inventory, vulnerability management and configuration control delivered in the form of alerts, audit trails and automated reports.

In general, the reporting of incidents is of secondary importance to procedures and technologies for finding, responding to, and remediating an incident.

Incident response procedures are a challenge for OES players with hybrid OT/IT infrastructures, particularly in the energy and health sectors. We also note that OES operators are eager to have solutions that are interoperable with existing or other 3rd party solutions.

**The NIS Cooperation Group**

The NIS Cooperation Group has an important role to play in helping the Member States to implement the NIS Directive. The review is an opportunity to revisit the functioning of the NIS Cooperation Group and consider providing it with enhanced resources and powers to ensure effective implementation of NIS Directive related guidelines and technical measures. This may include enhanced powers/or an enhanced mandate to ensure effective implementation of its NIS-related guidelines on technical measures. It should include voluntary guidance for the development of a Vulnerability Disclosure Program (VDP) and should align with existing international approach and well-established guidelines such as ISO/IEC 29147, ISO/IEC 30111, and CERT/CC disclosure guidelines.

The Coalition would also welcome the participation of the cybersecurity industry within the NIS cooperation group, perhaps modelled on Stakeholder Cyber Certification Group (SCCG)[6], which was established by the Cybersecurity Act to advise the Commission and ENISA on strategic

[6] https://ec.europa.eu/digital-single-market/en/stakeholder-cybersecurity-certification-group

issues regarding cybersecurity certification, and assist the Commission in the preparation of the Union's rolling work program.

Participation criteria for such a new group would target cyber security vendors, operators of essential services (OES) and digital services providers (DSPs) that advise the NIS Cooperation Group on workstreams and consultations, and whose membership can provide technical input and evidence based on their experience in protecting critical infrastructure.

**Information Sharing Cooperation between CSIRTS and the NIS Cooperation Group**

Better information sharing between and amongst CSIRTs is of critical importance in the NIS review. CSIRTs need to be able to consume more threat intelligence feeds, widening the visibility, providing greater insights to their stakeholders and making their intelligence more actionable.

ENISA has played a vital role in facilitating information exchange between CSIRTs, but the review is an opportunity to direct more resources to this important task. One means to achieve this is a new work-stream dedicated to improving threat intelligence consumption through greater automation and interoperability between feeds.

CSIRTs would benefit from a common API - and which is interoperable with other commercial threat intelligence information feeds – that would allow them to improve the processes and hence the ability to consume greater threat intelligence feeds.

**Clarify and Drive Greater Implementation of Technical Measures for Compliance with the NIS Directive**

The NIS directive has contributed to a higher level of security and network requirements by many Member States and affected sectors. The Coalition has observed, however, a lack of awareness among some OES operators with respect to the NIS Directive controls, likely due to the uneven implementation of the Directive across different Member States.

We also find that for many companies covered by NIS, while awareness of the law exists, there does not appear to be a sense of awareness about what steps to take. We encourage the European Commission to develop more impactful means whereby ENISA and other relevant European and national competent authorities clearly inform businesses what steps they can take to manage their cybersecurity risks and leverage technical guidance to comply with the Directive. Many companies do not know how compliant they are, or even what criteria they should assess themselves against.

ENISA made three recommendations in its November 2019 report, "Stock taking of security requirements set by different legal frameworks on OES and DSPs" [7], on what should be done to support organizations in identifying appropriate security measures based on the provisions of the NIS Directive: 1) develop/promote a unified risk management framework; 2) develop specialized sectoral guidance; and 3) develop specialized guidance on emerging security techniques. The Coalition agrees with ENISA's recommendations, as described below.

***ENISA's 2019 recommendations:***

- *Develop/ promote a unified risk management framework.* Internationally accepted cybersecurity risk management frameworks exist that are widely understood and used in industry – such as ISO 27001, SOC 2, and the NIST Cybersecurity Framework – so a revised NIS Directive should promote existing frameworks rather than developing a new one. At the same time, while an EU-wide risk management framework is important, it might not adequately meet the needs of all sectors. As such it should be complemented by specialized sectoral guidance (see below).
- *Develop specialized sectoral guidance.* Essential services sectors differ in many ways, including their risk levels and risk tolerance, as well as their dependence on ICT. For example, in many utilities, IT is being deployed alongside long standing "operational technologies" (OT), bringing these organizations unique cybersecurity challenges. As a result, specialized sectoral guidance would be extremely helpful. Intersectoral guidance would also be helpful. Many organizations do not fall neatly in just one industry sector, and as such their ICT infrastructure spans various risk profiles. We are not sure if such intersectoral guidance already exists, which would make its development by the EU of value globally. In developing such guidance, a good place to start would be profiling case studies of organizations whose businesses span multiple sectors that have successfully implemented security throughout their disparate ICT infrastructures/systems.
- *Develop specialized guidance on emerging security techniques.* In cybersecurity, the pace of change is unrelenting. Organizations need to know about emerging security techniques to help them automatically detect and prevent rapidly evolving cyberattacks. Some breakthrough areas today, for example, are in securing containerization. ENISA, in partnership with relevant stakeholders, should issue specialized guidance on emerging techniques on a frequent basis to keep up with changing capabilities.

ENISA has a strong role to play in developing and providing NIS compliance assistance. We

[7] https://www.enisa.europa.eu/publications/stock-taking-of-security-requirements-set-by-different-legal-frameworks-on-oes-and-dsps

recommend that ENISA establish additional ad-hoc working groups chartered to produce guidance documents and to help organizations to identify and implement emerging security techniques that are "state-of-the-art"/recognized security best practice (NIS) technologies. This work could be done in collaboration with the NIS Cooperation Group and national sector supervision bodies/ competent authorities. When commencing this work, ENISA should consult and draw from existing industry efforts, and member state efforts or guidance.

***Additional recommendations:***

- *Run extensive awareness campaigns.* Specialized sectoral guidance and guidance on emerging security techniques will be useful—but only gets us halfway there. Organizations covered under the NIS Directive need to know guidance exists and how to use it. ENISA should be directed to undertake extensive campaigns around the EU to raise awareness of its guidance and help organizations to leverage it. ENISA should work with member states and industry stakeholders in this effort, which should take various formats: workshops, webinars, and even the use of hands-on cyber exercises and cyber ranges produced and held in partnership with cybersecurity vendors and national competent authorities charged with implementing the Directive.
- *Guide and empower organizations to embrace change and new technologies.* In our experience, many organizations are worried about embracing new technologies. Practical and pragmatic guidance about how early adopters have successfully integrated state-of-the-art cybersecurity technologies would be useful, for example. This could be particularly helpful for utilities or other companies reliant on industrial control/SCADA systems. We understand that some energy companies are worried about harming their operational technology (OT) environments if they move too quickly to integrate new technologies. The intense 'up time' requirements of many critical infrastructure systems also make technology upgrades and updates more challenging for them.
- *Help organizations to validate their efforts and understand where they have gaps.* Cybersecurity risk management is an ongoing process, and useful lessons will continue to be learned. ENISA should provide ongoing guidance and expertise to organizations about metrics of effective cybersecurity and how to validate their efforts.
- *Help identify outcome-based goals.* ENISA should help organizations/sectors identify intelligent goals for cybersecurity risk management that are measurable, quantifiable, and with clear timelines for execution.
- *Guide organizations to prioritize having confidence in their ICT vendors.* When evaluating procurements, how securely a vendor develops its products and services should be the focus (in other words, the practices of the vendor), not the product/service itself.

## SECTION 3: APPROACHES TO CYBERSECURITY NOT ADDRESSED BY NIS

### Liability Protection for Incident Reporting

We note that in our experience, the most positive impact on breach notification comes from national jurisdictions providing protection from self-incrimination, in effect incentivizing (by giving organizations a waiver from liability for) good faith reporting. In this respect we urge the revision to maintain these provisions in article 14.3 and 16.3 of the current Directive.

The Coalition believes that any penalties should be reserved for willful non-compliance with incident reporting obligations. Where possible, however, governments should leverage liability exemptions and safe harbor models in cyber security incident report management processes to ensure an effective and balanced approach.

### Voluntary Information Sharing between Companies

Cyberthreat information sharing is distinct from breach reporting. The former is proactive sharing of threat information to increase situational awareness and prevent attacks; the latter is reporting after an incident has occurred. While cyberthreat information sharing is extremely important, it must be voluntary. The Coalition would support the Directive encouraging (but not mandating) that companies participate in voluntary information sharing organizations, such as information sharing and analysis centers (ISACs) or industry associations that have this as their single specific purpose, for example the Cyber Threat Alliance[8] and various ISACs. These organizations have appropriate protections and governance structures for cybersecurity information sharing. Sensitive, time and mission critical intelligence is most effectively shared between competitors where there are clear controls, confidentiality and governance processes in place and where they are adhered to by all consenting parties.

### Vulnerability Disclosure Programs (VDP) and Coordinated Vulnerability Disclosure (CVD)

Just as encryption is a critical tool in ensuring the confidentiality of data, so too are effective vulnerability discovery, disclosure, and handling processes critical components of a mature security program.

VDP refers to the overarching process through which vulnerabilities in digital products can be reported, received, triaged, verified, remediated, and communicated. CVD, a component of VDP, focuses specifically on facilitating the communication and receipt of information

[8] https://www.cyberthreatalliance.org/about-cta/

regarding vulnerabilities, working with outside parties such as cybersecurity researchers, and ideally, the public communication after remediation.

By raising awareness about security vulnerabilities and adopting handling processes, users and technology manufacturers can work collaboratively to take actions, such as mitigation, to avoid risks posed by the vulnerabilities. This makes products more resilient against cyberattack, reduces the likelihood of data breach, and bolsters trust and competitiveness in digital products.

This NIS review provides an opportunity to encourage the adoption of VDPs within national vulnerability infrastructure and organizational security programs, on a voluntary basis. For VDPs to be most effective and beneficial, the NIS directive may signal to both public and private sectors to voluntarily take several actions in parallel:

- Encourage OES and DSP to adopt a VDP, on a voluntary basis and in a manner that aligns with international standards, as a standard component of their security programs;
- Facilitate Member State and cyber agency incorporation of VDPs in security guidance and standard documents; and
- Ensure that Member States are adequately resourced to lead VDPs and CVD process, where appropriate, and support CVD led by non-government organizations.

The Coalition recommends that additional resources are provided for ENISA and this NIS cooperation group to develop a voluntary program and supporting infrastructure focusing on the identification, remediation, and coordinated disclosure of discovered vulnerabilities.

The Coalition does not, however, recommend policies that would mandate the involvement of government bodies in VDP activities between private sector entities. Nor does the coalition believe that the reporting of vulnerabilities to the government should be included in the revision of the incident notification requirements, as this would create more complexity in situations in which fixes for vulnerabilities are still being developed but are not yet finalized. The inclusion of government bodies should be voluntary unless subject to sector-specific requirements (for example in the healthcare sector where connected medical devices are subject to their own cybersecurity regulations).

The Coalition recommends that any incorporation of voluntary VDP and CVD best practice guidance in the NIS review build on existing internationally agreed standards, given the global nature of such processes. This approach would enhance and complement existing efforts rather than undermine existing efforts. Fortunately, much work has already been done internationally to advance VDP and CVD. For example, ENISA[9] has produced an overview of CVD,

[9] Good Practice Guide on Vulnerability Disclosure, European Union Agency for Network and Information

identifying challenges and good practices in addition to making recommendations for improvements, a body of work that can be developed through additional funding and focus together with the NIS cooperation as set out above. International standards covering several different aspects of CVD[10] and VDP[11] already exist and can be easily referenced and/or incorporated into the NIS revision.

The NIS Directive review is a critical opportunity for the Commission to promote voluntary implementation of a VDP, which is a critical tool in driving positive cybersecurity outcomes in Europe and mitigating vulnerabilities. Ultimately this would lead to better protection for consumers, organizations, Member States and the European Union as a whole.

Security, Jan. 18, 2016, https://www.enisa.europa.eu/publications/vulnerability-disclosure.

[10] ISO/IEC 29147:2018, Information technology— Security techniques— Vulnerability disclosure, https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en. gives guidance for the disclosure of potential vulnerabilities in products and online services and details the methods a vendor should use to address issues related to vulnerability disclosure

[11] ISO/IEC 30111:2019(en), Information technology— Security techniques— Vulnerability handling processes, https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-2:v1:en. This document provides guidelines for how to process and resolve potential vulnerability information in a product or online service and is applicable to vendors involved in handling vulnerabilities. The document is related to ISO/IEC 29147. This document interfaces with elements described in ISO/IEC 29147 at the point of receiving potential vulnerability reports, and at the point of distributing vulnerability resolution information