Cybersecurity Coalition

Comments on the Proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive)

The Cybersecurity Coalition ("Coalition") submits this paper in response to the European Commission's release of the Revised Directive on Security of Network and Information Systems Directive ("NIS2").

The Coalition is composed of leading companies with a specialty in cybersecurity products and services, who are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[1] We seek to ensure a robust marketplace and effective policy environment that will encourage companies of all sizes to take steps to improve their cybersecurity risk management.

As leaders in the cybersecurity industry, we recognise the complexity and importance of securing critical infrastructure. We applaud the Commission's efforts to modernise the EU's approach to cybersecurity and are pleased to see that many of the recommendations we made as part of the NIS2 public consultation have been incorporated into the draft Directive. We also share the Commission's desire to promote the protection of essential services and hope that the following feedback helps you to strike the right balance between promoting security activities and avoiding the creation of non-security-enhancing 'noise', which inhibits security teams' ability to prioritise critical activities.

The Coalition was reassured to see many important issues are included in the NIS2 proposal, such as voluntary cyber threat sharing between both governments and companies, the adoption of coordinated vulnerability disclosure (CVD) policies, and restoring access to WHOIS data for security purposes. We also welcome the comprehensive risk management thrust of the revised Directive, reflecting international standards. Additionally, the Coalition welcomes efforts to increase cyber resilience across member states, and we strongly support the clarification that activities undertaken to enhance the security of cyberspace are permitted in accordance with GDPR. We believe these concepts will contribute to increased levels of cybersecurity in the EU.

As Members of the EU Council and Parliament consider the NIS2 proposal, the Coalition would like to offer some suggestions on how to make NIS2 most effective. As such, we provide comments on some of the items above and also stress the importance of including the recommendations outlined below in any continued policy development:

- Ensure that the language in the draft which affirms the legality of security activities and maintenance of the WHOIS database under GDPR remains in the final text;

---

[1] 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.

  - Adapt Recital 69 to clarify that the personal data listed is non-exhaustive
- Clearly delineate the factors that Member States should use when determining whether small- or micro-entities are designated as 'essential' or 'important', making determinations based upon empirical data and engagement with the private sector, with a mechanism for the private sector to contest their designation;
- Ensure proportionate and differentiated obligations between 'essential' and 'important' entities based upon their respective criticality;
- Effectively implement the CVD proposals by ensuring:
  - That efforts are closely aligned with existing international standards
  - That any new programs are coordinated with, and not duplicative of, widely utilised mechanisms such as the Common Vulnerabilities and Exposures (CVE) program
  - That CSIRTs are used as an intermediary for CVD only and that their use is voluntary
- Align incident notification requirements under GDPR and NIS2, by increasing from 24 to 72 hours the timeline for reporting;
- Ensure that effective incident response is prioritised over unnecessary and counterproductive incident reporting requirements, by ensuring that the threshold for reporting incidents is sufficiently high and that 'near misses' do not need to be notified;
- Align certification requirements under NIS2 with provisions of the Cyber Security Act and clarify that they apply to 'essential' or 'important' entities and not individual products, while avoiding making certifications mandatory;
- Enable essential and important entities to take a risk-based approach to the use of security capabilities such as encryption; and
- Incorporate representatives of the cybersecurity industry into the work of the NIS Cooperation Group, as appropriate.

The Coalition thanks the European Commission and Members of the European Council and Parliament for their continued open and participative process as it works with the Commission to shape the final version of NIS2. 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 NIS2 is successful in driving consistent, effective cyber risk management across the European Union.

Respectfully Submitted,

The Cybersecurity Coalition

Relevant Text	Analysis	Recommendation
Article 2: "This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.28 2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; (ii) trust service providers referred to point 8 of Annex I; (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I; (b) the entity is a public administration entity as defined in point 23 of Article 4; (c) the entity is the sole provider	As the Coalition has stated previously, we agree with the European Commission that the identification and designation of operators of essential services (OES) and digital service providers (DSPs) in Europe has been both uneven and inconsistent[2]. We observed that member states often differed in what entities they classified as OESs and vs DSPs. Given these past discrepancies, we applaud the European Commission for seeking to align the definitions across member states. Especially in today's environment with COVID19, cybersecurity plays an important role across all sectors. Because the distinction between "essential" and "important" entities may not be applied consistently across member states, however, and because organisations may need to determine for themselves a new vector for misalignment has been introduced. This may introduce further confusion among	The Coalition believes harmonization of the scope of NIS2 is of utmost importance for a clear and predictable enforcement. While we take note of the new process to define covered entities (from NIS1 to NIS2), we urge EU policymakers to make sure that any misalignment and fragmentation is avoided during the implementation phase, where Member States may still identify some additional essential or important entities. We encourage both Council Members and Members of Parliament to consider ways to close opportunities for misalignment by promoting more empirical methods for determining categorisation of "essential" vs "important" entities. Through these efforts the EU can press Member States to improve the transparency of their identification process. Additionally, a more risk based, empirical process gives ENISA and the NIS Cooperation Group an opportunity to

[2] 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.

of a service in a Member State; (d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health; (e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact; (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State; (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council29 [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive."	organisations as to what requirements they must meet. As noted in our comments on Recitals 16-18, the inclusion in the scope of cloud computing services and data centre service providers is overly broad. While certain types of cloud or data centre service providers no doubt play an important role in digital supply chains, and thus, should meet certain security requirements, it's important that smaller entities not be unnecessarily designated as an "essential" entity unless they play a truly critical role in supply chains. Moreover, given the inherently cross-border nature of these services, it's important that companies not be required to tailor their security programs to meet different requirements in different markets.	promote greater alignment across the Digital Single Market. Further, it would be useful to clarify also that a private organisation comprising multiple entities operating across different member states would be subject to NIS2 rules only in those member states where the local entity is performing an "essential" or "important" activity. Further, the scope of cloud and data centre service providers that are designated as essential or important entities should be determined according to risk and in a manner that is aligned with definitions utilized in ISO/IEC standards. Finally, in our prior submission, we noted that any extension of the scope to additional sectors should be driven by extensive evidence and empirical data. An approach that treats everything as having the same level of criticality dilutes the resources available to the most critical assets.
Article 6 (1): "Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity	Robust programmes for coordinated vulnerability disclosure (CVD) are critical to ensuring that essential and important entities receive information on potential security exposures and are able to mitigate them in a timely manner.	The Coalition supports the Commission's focus on coordinated vulnerability disclosure. For the reasons indicated in the analysis section, our top priority recommendation is for any vulnerability coordination entity to utilise the existing CVE framework for identification, tracking, and scoring of vulnerabilities.

and the manufacturer or provider of ICT products or ICT services." (2): "ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties."	Public tracking of vulnerabilities offers many benefits, including: • Notifying affected organisations of exposures so they can be mitigated quickly; • Encouraging technology providers and operators to patch security vulnerabilities in order to protect technology users; • Creating a communal body of knowledge around potential vulnerabilities and their impacts on technology and users to hopefully avoid such issues or respond to them more quickly in the future. A centralised effort to coordinate vulnerability disclosures in Europe can help build trust, responsiveness, and consistency, as well as minimising the potential disruption caused by language and cultural disconnects and timezone shifts. A European coordinator can help reduce the backlog on public notification of vulnerabilities, which has been caused by over-burdening existing systems.	Recital 31 of the NIS 2 proposal states: *"To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third country jurisdictions."* The Coalition strongly agrees with this recommendation, and further, we urge the Commission to ensure that any vulnerability coordination entity not only collaborates and aligns with its international counterparts, but also adopts international best practices and standards, including leveraging the CVE framework. One way the Commission could potentially consider doing this that would reduce complexity and overhead, and still enable ENISA to track and publish vulnerabilities in real time, would be for the entity to become a Root CVE Numbering Authority (CNA) of the global CVE registry.[3] This can be used to feed into a European-owned and operated database that leverages the existing CVE program for vulnerability identity and registration needs. We also note efforts being undertaken to enhance the European Union's position on this important

[3] https://cve.mitre.org/cve/cna.html

	Establishing an EU database can help address challenges that European organisations may face, such as by providing details on risks, impacts, and fixes in all EU languages and with focus on ICT products developed or used in the EU. However, as part of a healthy global digital economy, it is important to recognise that many technologies are made, sold, and used around the world. Further, cybersecurity threats and attacks are global. To avoid confusion around any vulnerabilities related to the security posture of these technologies, it is critical that any effort to track and score vulnerabilities be as streamlined as possible. The Common Vulnerabilities and Exposures (CVE) identification and cataloging system, and associated CVSS scoring framework, have been in place for more than 20 years and are well understood and adopted around the world. A CVE entry includes the CVE ID (in the format "CVE-2021-123456"), a brief description of the security vulnerability or exposure, and references, which can include links to vulnerability reports and	issue[4], and we both support these efforts and recommend committing additional resources to ENISA and the NIS cooperation group to continue to explore and invest in growing voluntary VDP expertise and capabilities. As Member State CSIRTs work with ENISA to build out the coordinated vulnerability disclosure process, the Coalition believes that Council Members and Members of Parliament should ensure that those policies do not require government involvement in CVD activities between private sector entities. The inclusion of government bodies should happen only when necessary to find mitigations. While a CSIRT can play an important and valuable role, it should not be mandatory for a discloser to work through them to disclose vulnerability information, but rather at their discretion.

[4] https://www.enisa.europa.eu/procurement/vulnerability-disclosure-policies-and-vulnerability-databases

	advisories. This provides security professionals with a reliable way to tell one unique security flaw from another so they can then build a mitigation and prioritisation plan. Leveraging one CVE registry benefits global cybersecurity, as companies and other stakeholders that are handling incidents have just one registry to check, and know they are talking about the same incident. As of this writing, there are 157 organizations from 26 countries participating in exchanging vulnerability information in a structured fashion. Currently organizations in Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Latvia, Netherlands, Norway, Romania, Spain, and Switzerland are successfully participating in the CVE Program. Introducing a separate European tracking and scoring framework (a new registry) will significantly increase complexity for security teams that need to prioritise and deploy patches in a timely manner in order to protect the essential function of the organisation. The increased confusion and administrative overhead will reduce efficacy of patching efforts and expose essential	

	entities - and by extension, the recipients of their services - to greater risk. Similarly, coordination and consistency is necessary across other standard practices connected with vulnerability coordination. Much work has been undertaken to mature these practices over the past 20 years, evolving to keep abreast of changing dynamics in the security and technology landscapes. Maintaining consistency with these international practices will minimise confusion and complexity for security teams, as well as ensuring that the standards being adopted are the most up-to-date. It is also important to note that current best practices acknowledge that disclosure through a coordinating body is at the discretion of the discloser and/or the technology provider. In many cases, the parties may choose to keep the disclosure private for a variety of reasons, and any European coordination entity should recognise the need for participation in the system to be voluntary.	

Cybersecurity Coalition

Article 10: "1. CSIRTs shall comply with the following requirements: (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners; (b) CSIRTs' premises and the supporting information systems shall be located in secure sites; (c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers; (d) CSIRTs shall be adequately staffed to ensure availability at all times; (e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services; (f) CSIRTs shall have the possibility to participate in international cooperation networks. 2. CSIRTs shall have the following tasks: (a) monitoring cyber threats, vulnerabilities and incidents at national level; (b) providing early warning, alerts, announcements and	The Coalition is encouraged by the efforts to improve the resources and resilience of Computer Security Incident Response Team (CSIRTs) However, the requirements and tasks attributed to CSIRTs are notable for the absence of a requirement to acquire and have access to real-time threat intelligence and to share this intelligence based on interoperable solutions using the CSIRT networks.	The coalition recommends CSIRTs be resourced to acquire state of the art global threat intelligence offerings. In addition, in the tasks assigned to CSIRTs we recommend making explicit the need to provide threat intelligence information-sharing between public and private entities based on interoperable solutions Finally the CSIRT network should prioritise the exchange of interoperable threat intelligence feeds. Interoperability enables cybersecurity communities to communicate using a common language which aids in a better understanding of cyber-attacks and improves the ability to deploy effective solutions. Improving interoperability will also improve CSIRTs ability to process and consume data.

dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents; (c) responding to incidents; (d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity; (e) providing, upon request of an entity, a proactive scanning of the network and information systems used for the provision of their services; (f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request. 3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive. 4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following: (a) incident handling procedures; (b) cybersecurity crisis management; (c) coordinated vulnerability disclosure.”		

Article 12 at large and specifically (1): "In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established."	The Coalition supports the additional guidance and direction for the NIS Cooperation Group in NIS2. The Cooperation Group has an important role to play in helping the Member States to implement the Directive.	Given the additional guidance and the list of outlined responsibilities, the Coalition recommends that the Members of the European Council and Parliament consider providing additional resources to the Cooperation Group to ensure the Group's ability to carry out its important role. Further, the Coalition recommends a more robust approach to collaboration with industry representatives. Article 12 grants the NIS Cooperation Group the ability to "invite representatives of relevant stakeholders to participate in its work," however, stronger guidance and direction is needed to ensure a robust collaboration with relevant members of industry including the ICT community and critical infrastructure entities. Additionally, guidance may also be prudent to further outline specific areas and technical methods that the Cooperation Group and the CSIRTS can share information. Additionally, Members of the European Council and Parliament should consider adding additional guidance to ensure the NIS Cooperation Group aligns any supplementation guidance with internationally recognised best practices and standards.

Article 17 (2): "Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity."	The Coalition agrees that training of the management body on cybersecurity risks is important to ensure that members of the management body are appropriately skilled and resourced to fulfill their role.	We recommend retaining Article 17 in the final text of the Directive.
Article 18 at large and specifically (5) and (6): "The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2."	NIS2 improves broad alignment by requiring member countries to adopt national risk management frameworks, in line with international best practices, to pursue supply chain security practices, to establish processes for cross border information sharing and incident response, and to develop coordinated vulnerability disclosure policies. Additionally, the NIS2 notes the need to align reporting responsibilities across member states and notes the need for consistency with requirements generated by GDPR, DORA, and other regulations.	NIS2's *Article 18* specifies seven risk management measures that must be part of all member states' risk management approaches. It then goes on to state the use of implementing acts in Article 18 (5) and delegated acts in 18 (6). We believe the document should go further and mandate the development and adoption of "implementing acts" only where they are based upon international standards and frameworks. Members of the Council and Parliament should formally recognise the role of ENISA in setting out how internationally recognised standards and certifications can be used to demonstrate compliance in lieu of setting unique EU standards, as it works with all stakeholders to identify best cybersecurity practices. The NIS2 text should also direct the Commission, when developing implementing acts, to consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.

		Effective cyber risk management should remain the ultimate objective of NIS2. It is critical, also, that the language make clear that any specifications be aligned with existing EU regulation or legislation, such as GDPR and DORA, to avoid imposing conflicting requirements on companies.
Article 19 (1): "The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non- technical risk factors."	The Coalition agrees with the emphasis on supply chain security in NIS2. The Coalition is concerned, however, about two aspects of the proposed solution. First, the Coordination Group is tasked with leading the effort, in coordination with ENISA and other relevant entities. While this was the pathway for risk assessments of the 5G networks as spelled out in EU 2019/534, the broader mandate of all supply chain ICT risk is significantly larger in scope. Without robust partnerships with the ICT companies and industry associations, the Coordination Group may have a difficult time performing the required risk assessments. Second, the Coalition is concerned about the lack of clear criteria for assessment of ICT supply chains. Without that specific criteria and focus on the	Given these concerns, the Coalition recommends that the Coordination Group work with ENISA and industry stakeholders to identify concerns or risks to be addressed with regards to sectoral supply chain assessments. Once those determinations are made, the Coordination Group can work collectively with industry to perform a thorough supply chain risk assessment.

	interdependency of ICT suppliers, the Coordination Group may make the wrong risk decisions when selecting the supply chains for assessment.	
Article 20 (1): 'Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.'	In instances where the essential entity suffers an incident or outage. the NIS 2.0 proposal does not currently offer sufficient clarity on whether the customer – or the cloud service provider - is obliged to report directly to the regulators. If the cloud service provider would be required to undertake the reporting, this would breach confidentiality and contractual obligations, for instance in a typical cloud service agreement, where incidents are notifiable to the customer. Further, essential operators often use a combination of solutions and providers to maintain an effective cyber security perimeter. In these circumstances, it is only the essential operators as the customer that can determine the exact impact of an incident.	The coalition recommends that NIS 2.0 should offer greater clarity of incident notification requirements for essential entities that provide cloud based SAAS offerings to other essential entities. One means to achieve this would be to replicate the language included in existing NIS directive at Article 16 (5) "*Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator."*
Article 20 (2): "those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or	The requirement to notify of "any significant cyber threat" is alarmingly broad. Companies could potentially have hundreds of significant cyber threats in a single day	The Coalition recommends more specific language that would require notification only for incidents that actually cause disruption or harm. If organisations want to share more on a

remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability." Article 20 (3): "An incident shall be considered significant if: (a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned; (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses."	and notification of each of those events would be both burdensome and inhibit the effectiveness of response. As written, the notification requirement has the potential to harm the efficacy of security teams, who will be flooded with unhelpful reports that do not provide any actionable intelligence, undermining confidence in the utility of the reporting system. It is important to note that a cyber threat and a report-worthy cyber incident are not the same thing. For example, North Korea may be a threat, while an attack from North Korea is a significant security incident. Organisations face a huge breadth of threats, but hopefully they will translate into far fewer incidents. The threat in and of itself may not be particularly useful information for other organisations to protect themselves, particularly if there is such a high volume of reported threats that security professionals cannot determine which threats are the most critical and should be prioritised.	voluntary basis, then they should be encouraged, but not required, to do so in order to maintain a high quality of actionable reports in the reporting system.
Article 20 (4): "Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall	24 hours is too short of a time frame to report an incident to authorities and is not in line with the requirements of GDPR, with	We recommend changing 24 hours to "72 hours, or as quick as practicable: as the time frame to

submit to the competent authorities or the CSIRT: (a) without undue delay and in any event within 24 hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action"	which many incidents may have overlapping reporting requirements. While notification about significant incidents can be helpful, the one-day timeline does not allow enough flexibility for entities to begin to understand the realistic scope or potential implications of incidents and report them. In fact, this requirement injects additional complexity at a time when entities are faced with the difficult task of responding to a cyber incident. It also greatly increases the likelihood that the entity will report inaccurate or inadequately contextualised information that will not be helpful. We also note that the full extent and impact of a cyber security incident may not be known or well understood within 24 hours of it being realised, making it difficult for an entity to determine whether it is a 'critical' or 'other' cyber security incident within the timeframes. We appreciate that Recital 55 directs Member States to ensure that the requirement to submit this initial notification "does not divert the reporting entity's resources from activities related to incident handling that should be prioritised", but the	report an incident, in order to align with GDPR (Article 33). In addition, we strongly encourage the Commission to make the scope of reportable incidents sufficiently narrow to ensure that it is manageable for both essential and important entities as well as supervisory authorities. One means to achieve this would be to focus on incidents that are truly "significant' using existing international standards and taxonomies as a basis for the definition. We also discourage the mandatory or voluntary reporting of 'near misses' whose definition is highly ambiguous. A voluntary approach based on interactions with industry-led groups such as Information Sharing and Analysis Centers (ISACs) is a more effective approach so as to avoid the reporting of irrelevant incidents. We also recommend to extend timeline to 3 months for a final report and, regarding what should be provided in one month, we suggest using the term "a more comprehensive report".

	24-hour minimum written in the law undermines that intention. Regarding (c), it is not always possible to have a "final" report in one month's time. Information about cybersecurity incidents often continues to emerge over time The definition of "any significant cyber threat", meanwhile, is alarmingly broad. Under our interpretation, organisations would constantly be reporting threats or incidents; the receiving entity would be completely overloaded; security professionals would be overwhelmed with 'noise' and unable to parse what is really critical to focus on.	
Article 21 (1): "In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be	Article 21 creates the potential for further divergence of security requirements across the Union by enabling Member States to unilaterally require the use of EU-wide certification regimes, and make them *de facto* and *de jure* mandatory in some countries, an approach that contradicts the recently adopted EU Cyber Security Act. In addition, NIS2 defines requirements that apply to entities and not the products they	If entities are mandated to adopt national (e.g. SecNum, C5) or regional (e.g. EUCS) certifications then the voluntary nature of certification, as proscribed in the CSA, is undermined. This will create a significant burden for industry without increasing cybersecurity. To preserve the single market and ensure alignment with existing regulation under CSA, we recommend that individual member states not be given the authority to implement mandatory certification requirements. Rather certification

developed by an essential or important entity or procured from third parties." (2) The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	manufacture, hence the reference to products need to be clarified. Additionally, article 21 is ambiguous, suggesting that certification could both apply to a broad scope from entities to products in paragraph (1) and entities only in paragraph (2).	requirements, where applicable, should be determined at the EU-level in a manner that is internationally aligned, grounded in risk management and voluntary. We also recommend clarifying that an EU-level certification would be applicable only to the 'essential' or 'important' entities themselves, not to their products. This could be achieved by removing Article 21(2) and amending Article 21(1) to read: "Member States may encourage essential and important entities to certify certain ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.
Article 22 (1): "In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems."	The reference to standardisation and encouragement of internationally accepted standards is welcome by the Coalition.	We recommend keeping Article 22 in the final legislation.

Cybersecurity Coalition

Article 23(1): "For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data." (4): "Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data."	The reference to top-level domain (TLD) registries is too narrow. There are many other types of organisations that provide domain name registration services such as proxy service providers, domain name resellers and brokers, and those providing "second-level" domain information (SLD) It also is important to require that information collected and maintained points to the actual owner of the domain (known as the "ultimate beneficial owner"- this person actually owns the domain, even if the domain is registered under another name). Regarding section (4), WHOIS data typically includes Name, Address, Organisation, Phone number, Email. All these fields should be available to legitimate access seekers in order to identify actual ownership of domains and enable cybersecurity efforts. This information is useful also to be able to pivot - find all other domains for that owner / email / phone / address. Any kind of domain registration anonymity effectively undermines most of the security value of this data.	The text should read "all entities providing domain name registration services shall collect and maintain accurate and complete domain name registration data for the ultimate beneficial owner of the domain in a dedicated database facility…", For section (4), reference to "not personal data" should be struck, in favor of making data "available to legitimate access seekers". A clear definition of the term "legitimate access seekers" should be provided and it must go beyond law enforcement bodies, in order to enable the continued functioning of security activities by the private sector (e.g. cybersecurity companies or researchers). An accreditation system or portal should be established for legitimate seekers.

Article 24 (1): "DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union." (2) "For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union."	Those CSPs providing services in multiple EU27 jurisdictions will be under the jurisdiction of the entity's main establishment.	We welcome subjecting these entities (such as CSPs) to the jurisdiction of their main establishment as it simplifies the notification regime.
Article 26 (1): Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise,	Regarding paragraph (1), other relevant stakeholders aside from NIS2-covered entities should be encouraged to participate in voluntary cyberthreat information sharing. Important stakeholders include the cybersecurity community, including	Member States should not set out rules about sharing platforms. They should instead point to global best practices. Any notification to governments about private-sector participation in arrangements should be voluntary.

tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing…" (3): "Member States shall set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g). Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing	companies that may have unique or specific visibility of threats that other entities (such as sector-specific groups) might not see, and can contribute that information. At the same time, cybersecurity companies would benefit from exposure to the cyberthreat data from sector-specific information-sharing arrangement. Regarding article (3), directing Member States to set rules specifying procedures and operational elements of threat information-sharing arrangements will discourage, rather than encourage, more voluntary sharing. First, it creates too much bureaucracy and red tape. Second, having Member States set these rules risks a situation where each Member State lays down separate and distinct sets of procedures, which would also be a bureaucratic nightmare and dampen efforts to share threat information across borders. Cyberthreats Mandated notification to governments (competent authorities) when organisations join or leave information-sharing arrangements is not a global best practice. A mandate to notify could create a legal risk to an organisation (and fear of punishment) that	

arrangements referred to in paragraph 2 by providing best practices and guidance."	may be greater than benefits, distracting from the operational imperative and overall goal of this legislation.	
Article 27 (1): "Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification."	A requirement to report incidents that have not occurred (a "near miss") is simply unrealistic (the Coalition notes that there is no understanding of what a 'near miss' constitutes) and will likely result in competent authorities being overwhelmed by receiving thousands of reports (if not more) per day, particularly if there is uncertainty among covered entities of their obligations to report something that has not happened.	We strongly encourage the Commission to make the scope of reportable incidents sufficiently narrow to ensure that it is manageable for both essential and important entities as well as supervisory authorities. One means to achieve this would be to focus on incidents that are truly "significant' using existing international standards and taxonomies as a basis for the definition. We strongly recommend the removal of 'near misses', given the highly ambiguous nature of the term. A voluntary approach based on interactions with industry-led groups such as Information Sharing and Analysis Centers (ISACs) is a more effective approach so as to avoid the reporting of irrelevant incidents.
Articles 28-34 on supervision and enforcement	NIS2 seeks to harmonise and streamline certain responsibilities and create a floor for approaches to cybersecurity risk	In our prior submission, we noted that any extension of the scope to additional sectors should be driven by extensive evidence and empirical data. An approach that treats everything

	management by providing consistent minimum requirements.	as having the same level of criticality dilutes the resources that are available to the most critical assets. While the ex-ante/ex-post approach to supervision seem to create a differentiation between essential and important entities, in practice, if important entities are not given a lighter approach in terms of requirements, the problem of resource allocation will be exacerbated both for supervisory authorities and for important entities. Regardless of the approach taken, enforcement needs to be clear, predictable and harmonised, in terms of commensurate administrative fines and criminal penalties.
Recitals 16-18 on the scope of cloud computing services and data centre service providers.	It is important that the definition of cloud computing services is established by ISO/IEC international standards to minimise interpretational issues but also to reflect new technologies as they become pervasive. The inclusion in the scope of cloud computing services and data centre service providers is overly broad. While certain types of cloud or data centre service providers no doubt play an important role in digital supply chains, and thus, should meet	We encourage the NIS cooperation group and ENISA to focus on aligning requirements and "essential" vs "important" thresholds as a matter of priority. Such an approach will improve both consistency of definition and breadth of competitive choice in turn improving compliance with the NIS security controls. It would be useful to clarify also that a private organisation comprising multiple entities operating across different member states would be subject to NIS2 rules only in those member

	certain security requirements, it's important that smaller entities not be unnecessarily designated as an "essential" entity unless they play a truly critical role in supply chains. Moreover, given the inherently cross-border nature of these services, it's important that companies not be required to tailor their security programs to meet different requirements in different markets.	states where the local entity is performing an "essential" or "important" activity. Further, the scope of cloud and data centre service providers that are designated as essential or important entities should be determined according to risk and in a manner that is aligned with definitions utilized in ISO/IEC standards.
Recital 29: "Member States should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy…."	Member states should be directed to ensure their national coordinated vulnerability disclosure and management policies align with existing standards for vulnerability disclosure (ISO/IEC 29147) and management (ISO/IEC 30111). These standards are referenced in Recital 28 as having value, but it is necessary to direct Member States to leverage them.These standards, developed over years through international collaboration, lay out best practices for validating, prioritising, and remediating reported vulnerabilities so that all known vulnerabilities can be addressed in a coherent and efficient manner carefully considering the nuances of vulnerability handling and disclosure. If member states	The text should clearly state that Member States should establish relevant national policies that aligns with ISO/IEC 30111 and ISO/IEC 29417.

	establish coordinated vulnerability disclosure and management policies that deviate from these ISO standards without consideration for the delicate nature of vulnerability disclosure and associated risks, they risk re-investing standards that have matured and perfected over years.	
Recital 54: "In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications,	The Coalition supports the Commission's efforts to protect and promote both the broader understanding and use of encryption as part of the risk management framework adopted by member states. As with other security tools, organisations should consider when the use of encryption is required to mitigate a particular set of risks, and respond accordingly. In a cybersecurity context, we caution against mandating encryption as the main technology to improve cybersecurity. Encryption only mitigates certain risks-namely privacy, or preventing data from being tampered with. However encryption does not provide all aspects of security. If traffic is encrypted, it is scrambled, and owners of the networks will be unaware of the presence of malware in the traffic and unable to stop it, or if data is being	As with all security-enhancing capabilities, organisations should consider the use of end-to-end encryption as part of their risk management determinations. They should not, however, be required to implement it in all circumstances. With regards to the reference to law enforcement access, we encourage the Commission to clarify its intent and note that lawful intercept solutions for E2EE will inherently undermine security.

while providing an effective response to crime.”	exfiltrated. Finally, encryption will not prevent a device from being physically compromised. In short, relying solely on encryption creates a secure “pipe” for bad actors to leverage. It is technically possible for relevant security technologies and encryption to be deployed side-by-side and complement each other. Thus, mandating use of encryption can provide a false sense of security and may impede promoting a more holistic, on-going risk-management approach to cybersecurity. At the same time, the premise that end-to-end encryption must also contain solutions for lawful access is inherently contradictory and unworkable in practice.	
Recital 59: “Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such	We are pleased that NIS2 addresses an issue stemming from ambiguity regarding GDPR enforcement, which has been raised frequently by the security community. Access to WHOIS is critical to ensuring the security and resilience of the Domain Name System. It is also one of the most critical tools used for cybersecurity research, incident response, and threat mitigation, and is particularly valuable in preventing future	Giving data processing and access to WHOIS a legal foundation in the NIS2 addresses an unintended consequence of the GDPR. This step is both privacy and security enhancing. We applaud the Commission for incorporating it into the NIS2 proposal and strongly encourage all parties to ensure that it remains intact in the final version. We would, however, encourage the final draft to clarify the definition of who qualifies as a

processing shall comply with Union data protection law."	cyber incidents once a threat has been identified. These activities are, in turn, critical to the security of personal data and critical infrastructure in the EU.	'legitimate access seeker' in order to provide greater legal certainty for companies.
Recital 69: "The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types	Tracking, analyzing and sharing critical security data is a core part of understanding and responding to threats and exposures. As such, it is critical that entities covered by the NIS 2 Directive be able to leverage all kinds of security information to ensure they are fully investigating, understanding, and maturing their security posture, and thus protecting their essential and important functions. At present, GDPR does not adequately distinguish cybersecurity activities from privacy concerns, posing unnecessary restrictions on the collection and use of data (such as IP addresses) that enable analysis of the cyber threat landscape. Hindering such activities undermines both privacy and security, making us all less secure. While it's important to provide examples of the types of personal data (IP addresses, URLs, etc.), it's important that this not be interpreted as an exhaustive list, precluding the use of similar types of data that are	We welcome the Commission's decision to address this issue and clarify the scope of legitimate security activities allowed under GDPR. However, the last sentence of the proposed Recital 69 appears to limit the types of personal data that may be processed for this purpose. An exhaustive list of the types of relevant data covered may result in unintended harms arising for the security of covered entities, as the types of data required for ensuring network and information security may change depending on the risks, threats, and future technologies. We recommend making the list of personal data non-exhaustive, for example by making the following edits indicated in **bold**: *"Such measures may require the processing of the following types of personal data* ***including, but not limited to****: IP addresses, uniform resources locators (URLs), domain names, and email addresses."*

of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.”	critical to the underlying purpose. This is particularly relevant, given the iterative nature of cybersecurity.	