The Information Technology Industry Council has engaged with legislators throughout the development of the NIS2 Directive. As the NIS2 Directive enters the trilogue negotiation phase, ITI has developed a set of priority recommendations on the provisions that should be included in the final NIS2 Directive. We believe that adopting these amendments will help ensure that the final NIS2 Directive uplifts cybersecurity and resiliency across the European Union.

**Legislative Interplay and Harmonization**

**Recital 12a**

*Recommended approach: Council of the EU General Approach*

ITI supports the Council’s General Approach, which indicates that in cases where an essential or important entity is subject to equivalent cybersecurity risk management and reporting obligations contained in the NIS2 Directive as well as in sector-specific legislation, that the sector-specific legislation should apply. This will help to streamline obligations that essential and important entities may be subject to.

**Recital 12ab**

*Recommended approach: Council of the EU General Approach*

ITI supports the Council’s General Approach which stresses the importance of a consistent legal interplay with DORA, and other future sector-specific frameworks, such as the eIDAS and CER Directive, to avoid unnecessary duplication and incompatibilities with NIS2. We also appreciate that the Council’s text requires coherence between reporting obligations and states that overlapping obligations should be avoided.

**Article 2(6)**

*Recommended approach: European Parliament Mandate*

There needs to be additional clarity around the interplay between NIS2 and other sector-specific legislation so that companies that fall in scope of both the NIS2 Directive and other sector-specific legislation are not subject to conflicting or overlapping regulatory frameworks such as DORA and the EECC. There should be specific direction for coordination among sector-specific competent authorities and the authorities responsible for NIS2 so as to ensure clear application of measures. ITI, therefore, welcomes the European Parliament’s provisional agreement which highlights a collaboration between the European Commission, ENISA, and the Cooperation Group.

**Article 18(5)**

*Recommended approach: Council of the EU General Approach*
ITI appreciates the clarification made by the Council that the European Commission should exchange advice with the Cooperation Group and ENISA on the draft of implementing acts and reaffirming that Member States should follow, to the greatest extent possible, international, and European standards and technical specifications.

**Article 29(9a) New**  
*Recommended approach: European Parliament Mandate*

ITI believes that it is important to establish a clear hierarchy between NIS2 and conflicting or overlapping regulatory frameworks for the companies that will fall in scope of different regulatory regimes, such as DORA and the EECC. For example, cloud providers will be subject to a horizontal supervisory regime under NIS2 and a parallel financial services oversight under DORA. With a lack of a formal mandate of the designated competent authorities under the two frameworks to cooperate on their supervisory action and recommendations, there is a concrete business risks for the providers to be presented with conflicting regulatory findings. Therefore, we support formalizing cooperation between authorities under the two laws.

**Role of CSIRTs and Technology**

**Recital 25a**  
*Recommended approach: European Parliament Mandate*

This addition would promote the ability for CSIRTs, upon request, to provide the same visibility into an entity’s Internet-accessible attack surface as the adversary. In addition to enumerating accurate and real-time inventories of these systems and assets, this capability enables more nimble discovery and remediation of critical vulnerabilities. Since entities cannot secure what they cannot see, effectively leveraging technology to provide an automated common operating picture of an entity’s attack surface is critical in today’s threat environment.

**Recital 26b**  
*Recommended approach: European Parliament Mandate*

This addition acknowledges the critical role of machine learning and AI in improving the detection of and preventing today’s sophisticated and automated cyberattacks.

**Recital 26c**  
*Recommended approach: Commission Proposal or Council of the EU General Approach*

Open-source cybersecurity tools should not be promoted over other types of software. The security of software depends on how it is developed, maintained, and deployed, regardless of type.

**Recital 45a**  
*Recommended approach: European Parliament Mandate*

This addition describes some very helpful cybersecurity hygiene best practices.

**Recital 49**
**Recommended approach: Council of the EU General Approach**

If providers of public electronic communication networks or publicly available electronic communication services are brought into the scope of NIS2, it will be important to reference and leverage the already existing work done by ENISA in developing implementing guidance for the security requirements found in Article 41 of Directive (EU) 2018/1972.

**Recital 53**

**Recommended approach: European Parliament Mandate**

This new text rounds out ways providers of public electronic communication networks or publicly available electronic communication services should secure their networks, communications, and users.

**Recital 53**

**Recommended approach: European Parliament Mandate**

The new text adds a list of important technologies that providers of public electronic communication networks or publicly available electronic communication services should be encouraged to use to secure their networks, communications, and users. Given the sophistication and automation of cyberattacks, these types of technologies, including the use of automation, are critical to today’s network defense.

**Coordinated Vulnerability Disclosure**

**Recital 28**

**Recommended approach: European Parliament Mandate and Council of the EU General Approach**

We appreciate that Recital 28 refers to international standards for coordinated vulnerability disclosure. The final text should reflect the updated standard number as proposed in the Council’s General Approach (ISO/IEC 29147). Negotiators should also adopt the text from the Compromise Agreement, which emphasizes the voluntary nature of coordinated vulnerability disclosure frameworks, and also emphasizes the importance of aligning with existing international standards and best practices.

**Recital 30**

**Recommended approach: European Parliament Mandate**

We support the European Parliament approach, which encourages ENISA to set up a European vulnerability database, as opposed to a vulnerability registry. The global cybersecurity community has been leveraging one global Common Vulnerabilities and Exposures (CVE) registry for decades. Establishing a new/additional registry would duplicate efforts, add confusion, and result in resources being unnecessarily diverted to checking multiple registries. By contrast, there are multiple databases globally that leverage the CVE, and ENISA should establish a database to better meet European entities’ needs. Establishing an EU database can address challenges that European organisations may face, such as by providing details on risks, impacts, and fixes in all EU language and with focus on ICT products developed or used in the EU.
Recital 31
Recommended approach: European Parliament Mandate

We support the European Parliament’s report, which directs ENISA to leverage the existing Common Vulnerabilities and Exposures (CVE) registry for its European vulnerability database and to explore structured agreements with registries or databases in other regions. This will ensure that the database is aligned with the global CVE registry, as well as with efforts being undertaken in third-countries.

Article 6
Recommended approach: European Parliament Mandate

For the reasons outlined above, we support changing the phrase registry to database, as proposed in the European Parliament adopted report.

Article 6(2)
Recommended approach: European Parliament Mandate

In line with the reasons we outlined above, we welcome the report of the European Parliament, which directs ENISA to leverage the existing CVE registry, rather than creating an ad hoc EU registry, which may duplicate global efforts.

EU Coordinated Risk Assessments of Critical Supply Chains

Recital 46
Recommended approach: European Parliament Mandate

In addition to undertaking coordinated risk assessments as outlined in Article 19, we appreciate that the European Parliament has proposed additional language that encourages the Cooperation Group to include information on mitigating measures or best practices for identified risks, which will offer concrete guidance as to how an organization can manage identified risks.

Article 19(2)
Recommended approach: European Parliament Mandate

We appreciate that the NIS2 Directive has an increased focus on supply chain security, as it is an undoubtedly important facet of cybersecurity. We support the fact that the NIS2 proposes undertaking coordinated supply chain risk assessments, as we more generally support a risk-based approach to supply chain security and believe such assessments will deepen policymakers’ understanding of what risks exist and how to address them. Supply chain security is a shared responsibility between government and industry, and it is our view that the NIS2 needs to further reflect that and more clearly incorporate the perspectives of industry, either via the Stakeholder Cybersecurity Certification Group or via other means. Including industry in the assessments that the Cooperation Group is directed to undertake will be valuable as they have specific insight into their
supply chains and can lend credible and relevant expertise to such risk assessments. As such, we support the inclusion of the phrase ‘and other stakeholders’ in Article 19.2.

**Reporting Obligations**

**Article 20(3)**

*Recommended approach: European Parliament Mandate*

We appreciate the approach taken by the European Parliament, which strikes references to “potential” impacts and lays out concrete criteria that should be considered in determining whether an incident is significant. A determination should be made based on actual impact of an event, as opposed to potential impact.

**Article 20(4), point a-b**

*Recommended approach: None; we continue to encourage NIS2 to allow for a 72-hour reporting window.*

We have consistently advocated for a 72-hour reporting window and continue to encourage that approach in the NIS2 Directive for significant incidents. At present, none of the approaches contemplate such a timeline. As such, we believe they will not achieve the desired objective and may instead serve to further complicate cybersecurity efforts. As we have stated in our positioning previously, a 24-hour reporting window for any type of incident is an extremely short, unworkable timescale for businesses to adhere to. During the first 24 hours following an attack, the primary focus for companies should be on identifying and responding to malicious actors/activities, rectifying the problem, and ensuring (or restoring) business continuity. In addition, exposing information about an incident before a patch is applied or operations restored makes operators and their customers vulnerable to increased attacks. This requirement also greatly increases the likelihood that the entity will report inaccurate or inadequately contextualised information that will not be helpful. A 72-hour reporting window will not preclude entities from reporting in a shorter timeframe if possible and will help ensure competent authorities can receive quality information. It will also ensure that authorities are not inundated with reports and also allow the impacted entities to focus on responding to the incident.

In laying out reporting obligations, we also urge negotiators to consider adding language that limits the reporting responsibility only to the impacted entity, in cases when one essential service provider is the user or client of another essential service provider’s service, notably by including a similar provision to Article 16(5) of the NIS Directive: “[w]here 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.” We elaborate on many of these points further in ITI’s *Global Incident Reporting Policy Principles.*

---

**Article 20(4), point c**  
*Recommended approach: European Parliament Mandate*

We support the European Parliament’s approach, which requires a *comprehensive report* no later than one month after the initial notification. It is oftentimes not possible to submit a *final report* in this time frame, because it takes a longer amount of time to conduct a thorough investigation of the incident, especially as new information is uncovered. As such, the language requiring a comprehensive approach allows for flexibility in updating the report as the entity investigates the incident.

**Article 20(4), point (ca)**  
*Recommended approach: European Parliament Mandate*

We support the European Parliament’s approach, which recognizes that an incident may still be ongoing or under investigation at the time the comprehensive report is submitted, and which allows an entity the flexibility to submit a final report only after the incident has been resolved.

**Databases of Domain Names and Registration Data (WHOIS)**

**Recital 60**  
*Recommended approach: European Parliament Mandate*

We recommend the approach in the European Parliament’s text, which recognizes the importance of making domain name registration data available to legitimate access seekers for cybersecurity purposes.

**Recital 62**  
*Recommended approach: European Parliament Mandate*

We support the European Parliament’s proposed text, which ensures that registrant databases are accurate, validated and do not hold false information.

**Article 2(6a)**  
*Recommended approach: European Parliament Mandate*

We support the European Parliament’s recommendation to create an official article to highlight processing data for security as a legitimate interest. An official provision is more impactful and makes clearer distinction between cybersecurity and privacy concerns. At present, GDPR does not make such a distinction clear, posing unnecessary restrictions on the collection and use of data (such as IP addresses) which enable analysis of the cyber threat landscape. Hindering such activities decreases security, which in turn undermines privacy.

**Article 4(15a)**  
*Recommended approach: European Parliament Mandate*

We support the European Parliament’s text, which keeps the reference of domain names broad as the reference to top-level domain (TLD) registry is too specific. 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.
Article 23(1)
Recommended approach: European Parliament Mandate

We are supportive of the European Parliament’s proposed text, which recommends the inclusion of language to ensure that registrant databases are accurate, complete, validated, and timely and do not hold false information.

Article 23(2)
Recommended approach: European Parliament Mandate and Council of the EU General Approach

We support the European Parliament’s proposed text, which directs Member States to ensure that certain information is included in domain name registration databases, including name, physical address, email address, and telephone number. This will help in confirming that the ultimate beneficial owners listed in such databases reflect real people or legitimate organisations as opposed to fake names or shell companies. In a similar vein, we also support the language proposed in the Council’s General Approach, which also directs Member States to collect similar information.

Article 23(3)
Recommended approach: European Parliament Mandate

We support European Parliament’s proposed text, which ensures that registrant databases are accurate, complete, and validated.

Article 23(4)
Recommended approach: European Parliament Mandate

We support the European Parliament’s proposed text, which makes information collected during the domain name registration publicly available after registration. This will help to facilitate access to this data by legitimate access seekers to identify actual ownership of domains and enable cybersecurity efforts.

Security as a Legitimate Interest

Recital 69
Recommended approach: European Parliament Mandate

Both the European Parliament Mandate and Council of the EU General Approach have language for Recital 69 that make clear that processing of personal information under NIS2 could be considered either a “legal obligation” and/or “legitimate interest” under the GDPR. That said, we have a slight preference for the Parliament Mandate because it uses a broader list of illustrative examples when discussing the types of personal data that could be included, e.g., time stamps, operation system or browser-related info, cookies or other modus operandi data. This helps articulate the intended scope and reach of the provision.
Article 2(6a)  
*Recommended approach: European Parliament Mandate*

We support the European Parliament’s recommendation to highlight in an Article that the processing of personal data for security purposes is covered by GDPR (and clarify in the corresponding recital (Recital 69) that processing takes place depending on the specific circumstance, in compliance with a legal obligation or legitimate interest). This will encourage Member States to clarify the relationship between GDPR and NIS2 and the distinction between the legitimate interest legal basis (used for cases that processing serves the interest of the parties (e.g., cyberthreat information sharing)) and cases where processing is conducted to fulfill the legal requirements of the NIS Directive (e.g., incident reporting, or deploying the cybersecurity measures of Article 18). At present, GDPR provides only a “legitimate interest” as the primary legal basis for cybersecurity purposes. NIS2 would require specific cybersecurity measures for which the processing of personal data is necessary. The absence of a reference to one of the existing GDPR legal bases (legitimate interest or compliance with a legal obligation) risks posing unnecessary restrictions on the collection and use of data (such as IP addresses) which enable analysis of the cyberthreat landscape. Hindering such activities decreases security, and prevents private and public sector organisations from applying, or calls into question whether they can lawfully apply, the provisions of NIS2 properly. Being able to take the needed steps to secure information systems and data will in turn improve privacy.

**Cybersecurity Certification**

**Article 21(1)**  
*Recommended approach: European Parliament, in conjunction with aspects of the Council of the EU General Approach*

We support the European Parliament’s text, which focuses on harmonisation with the EU-wide Cybersecurity Act certification schemes and uses the language “shall...encourage,” which allows for greater flexibility in how Member States choose to use certification and avoids requiring Member States to do so. We also welcome the European Parliament’s recognition that there may be existing internationally recognized certification schemes that can be leveraged. We also appreciate aspects of the Council’s text, which more appropriately shifts the burden of certification from essential and important entities to the manufacturers or developers of ICT products, systems, or services themselves.

**Article 21(2)**  
*Recommended approach: European Parliament Mandate, in conjunction with aspects of Council of the EU General Approach*

We support the European Parliament’s text, which emphasizes that certification should be used only in certain situations where insufficient cybersecurity has been identified and should be preceded by an impact assessment. We are also supportive of the implementation period proposed in the text. At the same time, we are supportive of aspects of the Council’s General Approach as well, which offers the Commission greater flexibility in choosing to adopt schemes by using the term “may adopt.” Further, we believe that the language proposed by the Council more appropriately places responsibility on the manufacturer or developer of the ICT product, system, or service to obtain a certification, as opposed to making the essential or important operator...
responsible for obtaining a certification for a product they sourced from a third-party. Of course, if the essential or important entity has developed the product, system, or service, then they should be responsible for obtaining the certification. We are similarly supportive of additional aspects proposed in the Council’s General Approach related to preparing implementing acts, including undertaking an impact assessment, carrying out an open and transparent stakeholder consultation process, and considering relevant, existing Member State laws.

Article 21(3)  
Recommended approach: European Parliament Mandate

The European Parliament’s suggestion takes into account the role of Cooperation Group and European Cybersecurity Certification Group (ECCG) before proposing a new candidate scheme.

Cybersecurity Information-Sharing Arrangements

Recital 68  
Recommended approach: European Parliament Mandate

Other relevant stakeholders aside from NIS2 entities should be encouraged to participate in voluntary cyber threat information sharing. Relevant stakeholders include cybersecurity companies (providers of cybersecurity services) that may have unique or specific visibility of threats that others (such as sector-specific groups) might not see and can contribute that information. Another relevant stakeholder is the cybersecurity research community, which might uncover valuable information on emerging threats.

Article 23 (1)  
Recommended approach: European Parliament Mandate

We provide the same comment as above: other relevant stakeholders aside from NIS2 entities should be encouraged to participate in voluntary cyber threat information sharing. The edits to the list of information recommended to be shared expands and clarifies the types of data most useful to cybersecurity practitioners and IT departments to identify cyberthreats as well as the techniques and tactics of cyber adversaries. In point b, the edits expand the description of the end goals for cyber threat information sharing, which contribute to improving the cybersecurity ecosystem.

Article 23 (2)  
Recommended approach: European Parliament Mandate

Information sharing is voluntary and based on trust. It should therefore be facilitated, but not regulated, by the Member States.

Article 23 (3)  
Recommended approach: European Parliament Mandate

Directing Member States to set rules specifying procedures and operational elements of threat information-sharing arrangements will discourage, not encourage, more voluntary sharing. Cyber threat information sharing arrangements come in various forms, and their operating procedures, including underlying ICT platforms for information exchange, should be chosen by the members to
meet their needs. We also risk a situation where each Member State has distinct procedures, which would be overly bureaucratic and dampen efforts to share information across borders.

**Jurisdiction**

**Article 24 (2)**

*Recommended approach: European Parliament Mandate, subject to additional clarification*

Although the European Parliament approach on jurisdiction allows for greater flexibility in determining where an entity’s main establishment is located, we strongly recommend that additional language is incorporated into the current text to further clarify the one-stop-shop mechanism as a precondition for effective provision of ICT services. An entity’s main establishment should be based on its headquarters as contemplated under the current NIS Directive to avoid inconsistency and confusion around jurisdiction and appropriate competent authorities.